Cloud-Based Biometric Voting Platform With Tamper-Proof Blockchain Storage

Mrs. Rashmi K T[1], Shashank D[2], Vijayalakshmi K S[3], Basavesh K[4], Shreeya V[5]
[1,2,3,4,5] *Department of Electronics and Communication Engineering Global Academy of Technology Bengaluru*

***Abstract*—Secure and voting system are fundamental in building trust and integrity in contemporary elections. The traditional electronic methods still have problems such as data tampering, unauthorized access, and voter duplication. This paper presents a cloud- based biometric Fingerprint and facial-based voting framework. Recognition for dual-factor authentication. Votes are encrypted with AES and stored in Firebase, whereas their SHA-256 hashes are recorded on a private blockchain to ensure transparency and immutability. The integration of biometric verification, encryption, and blockchain enhances security across all the stages of voting. The system, implemented with an ESP32 microcontroller and R307S fingerprint sensor provides a secure, scalable, and tamper-resistant solution adapted for digital governance and large-scale elections. Secure and verifiable voting system are fundamental to building trust and integrity in modern times election.**

***Index Terms*—ESP32, Biometric Authentication, Blockchain, AES Encryption, Cloud Storage.**

I. INTRODUCTION

Electronic voting is a guarantee of transparency, accuracy, and trust in democratic elections. However, traditional voting systems such as paper ballots and standalone electronic voting EVMs have a host of drawbacks, including the following: Voter impersonation, unauthorized access, and lack of verifiability. Centralized databases employed in traditional e-voting systems are also susceptible to hacking and tampering that can challenges which might lead to a compromise of election integrity. These are challenges that indicate the What is needed is an increasing demand by various stakeholders for the development of a safe and auditable mechanism for voting. Ensures the authenticity of the voters and confidentiality of data Biometric technologies include fingerprint and face recognition. In this case, both biometric identification and recognition mean singular, non-transferrable identifications that can be used to vet and remove duplicate voters. Meanwhile Blockchain provides immutable and transparent records. Eliminating manipulation risks. The integration of these with cloud storage and AES encryption enables a scalable voting. platform, ensuring end-to-end security, transparency, and Reliability: This paper presents the design of a cloud-based Biometric voting system with tamper-proof blockchain storage to improve the integrity of elections.

II. LITERATURE SURVEY

Electronic voting has emerged as an area of interest among researchers as It plays an important role in ensuring security and transparency, trust in democratic elections.[3] introduced a Blockchain-based voting system with increased transparency and auditability, did not include multi-factor biometric. Verification Traditional systems of voting, such as paper ballots and stand-alone electronic voting. machines, commonly face problems such as: voter impersonation, unauthorized access, data manipulation, and It lacks verifiability. The challenges have raised concerns in about election integrity and the need for more advanced tamper-resistant voting technologies [1],[3]. Conventional databases used in electronic systems are centralized, making them vulnerable to cyberattacks and unauthorized modifications. Single-factor authentication systems also Those controls based on ID cards or passwords

are prone to misuse and do not ensure that the actual registered voter is casting the vote [2].

Fingerprint and facial recognition are examples of biometric systems. provide the more reliable and unique method of verification of the voter. identity [4]. Shobana et al. [2] proposed a fingerprint-based voting system, while ensuring accurate identification, lacks end-to-end data security. Kumar et al. [3] proposed a Blockchain-powered voting system with increased transparency And auditability, did not include multi-factor biometric verification. Fatima et al. [5] designed a cloud-integrated Model of secure vote storage, but relied solely on cloud. encryption-e.g., which may still be vulnerable to insider threats. These studies indicate that isolated technologies may contribute to improved voting security, combining approaches Can offer greater protection against manipulation and fraud. Recently, researchers have highlighted that biometric integration with blockchain and encryption can offer a trusted voting. Tamper resistant environment and loss of data. To this end, a unified framework that combines these technologies is required. for complete confidentiality, integrity, and transparency in contemporary electronic elections.

Building on these, the paper proposes a novel cloud-based biometric voting platform with tamper proof blockchain storage. The system utilizes dual-factor Biometric authentication with the R307S fingerprint sensor and facial recognition for voter verification. Each verified vote is encrypted using the Advanced Encryption Standard (AES) algorithm to maintain confidentiality prior to uploading to a Firebase cloud database. To ensure data integrity and verifiability, a SHA-256 hash of the encrypted vote is recorded on a private blockchain network implemented using Ganache. The system uses an ESP32 microcontroller for Hardware control, PHP-based APIs for data transfer, and a web election management dashboard. This integrated approach provides an end-to-end, secure, transparent, and scalable Voting framework apt for government and institutional elections.

III. METHODOLOGY

Block Diagram:

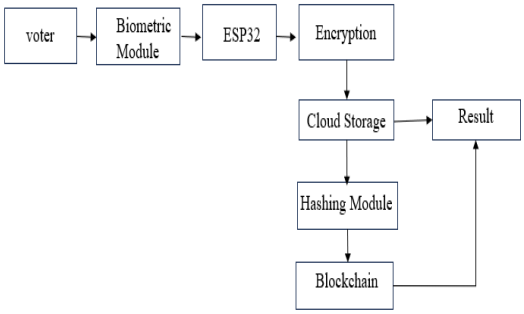


Fig.1: Block diagram of proposed solution

A. HARDWARE:

1. Control unit: ESP32 Microcontroller

Figure 2: ESP32

Figure 1 ESP32 acts as the main processing and control unit for the system. It handles the collection of biometric data, encryption using AES, and secure communication with the Firebase cloud. With Wi-Fi capability, it provides smooth real-time data transfer between the biometric module, cloud, and blockchain network. The microcontroller is also involved in the control of the authentication process so that only verified users are allowed to vote.

2. Biometric Module: Finger Print and Face Recognition

Figure 3: Finger Print

The fingerprint recognition unit which is shown in Fig. 3 is the R307S sensor-based unit. Precise and speedy fingerprint matching captures the right identification of a voter with smooth authentication. It essentially detects the unique ridge patterns of a voter's fingerprint and converts them into digital templates. The fingerprint template of each registered voter gets stored in the Firebase cloud upon registration. During authentication, the live fingerprint input is matched against the stored template for verification of identity. Serial UART communication is used to operate the R307S with ESP32 for efficient data exchange. It has an integrated image processing algorithm that. includes strong anti-spoofing protection, hence is ideal for voting applications needing high security.

Figure 4: Laptop Camera

Figure 4: The facial recognition module utilizes the web camera of the laptop to capture, in real time, an image of the voter. The captured image is then processed and matched against stored face templates in Firebase. This secondary layer of biometrics ensures that the verified fingerprint actually belongs to the rightful voter. Verification implemented by Python-based facial recognition libraries integrated with Firebase APIs, making it more secure and impersonation-free.

B. Software

1. Arduino IDE:

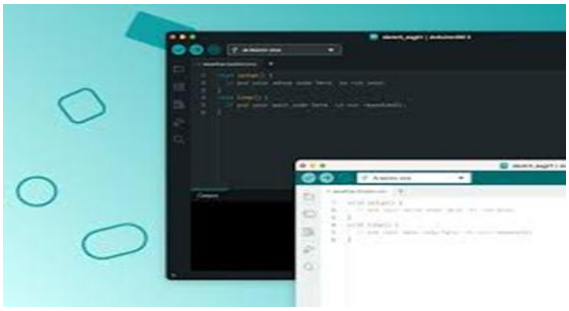


Figure 5: Arduino IDE

Figure5: Arduino IDE is used to write and upload the program into the ESP32 controller. Its major aim is to provide integration among hardware components, biometric modules, encryption logic, and Wi-Fi communication in order to perform seamless operations.

2. Firebase API Integration

The ESP32 connects to Firebase through REST APIs. During registration or voting, biometric data and encrypted votes are transmitted to Firebase using secure HTTPS connections. Firebase handles both storage and retrieval functions for authentication and result management.

3. AES Encryption and SHA-256 Hashing

The ESP32 connects to Firebase using REST APIs. Upon registration or during the process of voting, the biometric data and encrypted votes are sent to Firebase through secure channels using HTTPS. Firebase manages storage and retrieval functions for both authentication and result management

.

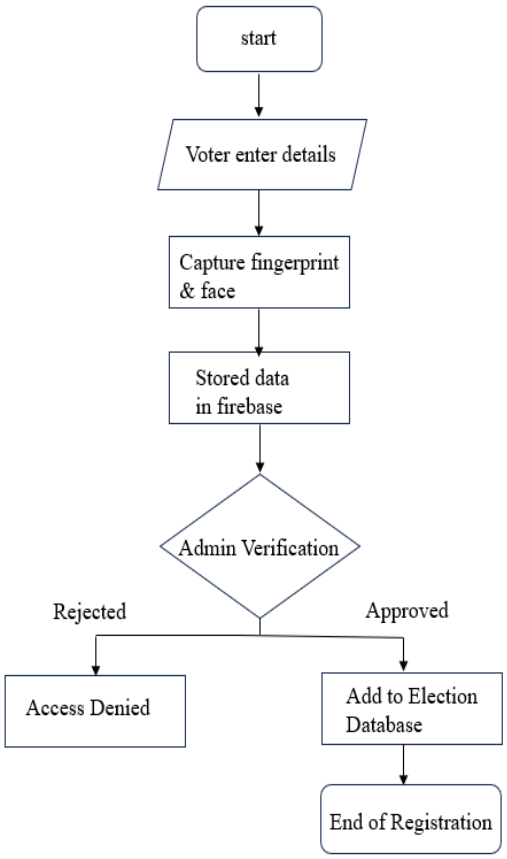
4. Blockchain Environment

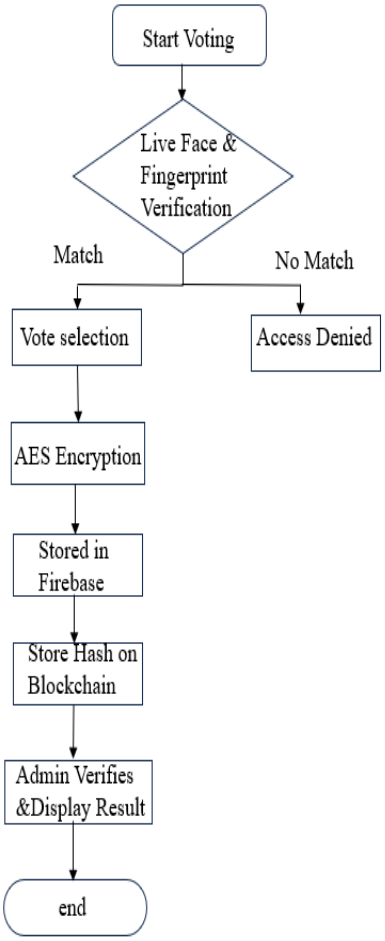
Ganache provides a local blockchain network where the SHA-256 hash of each encrypted vote is kept. This makes all votes immutable and verifiable. MetaMask provides the interface to connect the web application to the blockchain, and the admin can easily view each transaction that occurs securely

5. Web Application

The web interface is also the front-end for both voters and administrators. This will allow verified voters to log in, view the list of candidates, and ultimately cast their votes with ease. Immediately, the system encrypts the vote using AES before uploading to Firebase. The administrator dashboard shall provide a facility for authorized officials to check blockchain hashes, decrypt valid votes, and show results in real time. Its interface is designed in React and ensures ease of navigation, security of data, and transparency of the whole process.

IV . SYSTEM FLOW





Registration and Verification Phase:

1. ESP32 Setup: The ESP32 microcontroller is configured as the main controller; it captures biometric data and interfaces with the Firebase cloud for the same.
2. User Registration: The voter will fill in his or her personal information on the registration dashboard. The system captures the facial image through a webcam and the fingerprint through the R307S sensor for the purpose of biometric identification.
3. Data Storage in Firebase: Captured biometric templates in encrypted form and the details of voters will be securely uploaded to the Firebase cloud database.
4. Admin Verification: All the data of the registered voters has to be verified by the admin. The verified and approved voter record gets added to the official list, indicating that the registration phase is now complete.

Voting and Result Phase:

1. Voter Authentication: While voting, the system captures a live face image and compares it to the registered data (70–80% accuracy). After successful verification of the face, using the fingerprint with the connected R307S sensor to the ESP32 is authenticated.
2. Vote Casting: After the result of both biometric verifications comes out positive, the voter selects their candidate from the web interface. After that, the ESP32 generates a unique voter's ID to preserve one-vote-per-user integrity.
3. Encryption through AES & Storage on the Cloud: The voter's ID and candidate name are encrypted using the AES algorithm, which is then securely stored on Firebase to avoid unauthorized access.
4. Integrating Blockchain: The encrypted vote creates a SHA-256 hash stored on the Ganache blockchain via MetaMask to ensure that votes are immutable and verifiable.

V . RESULT

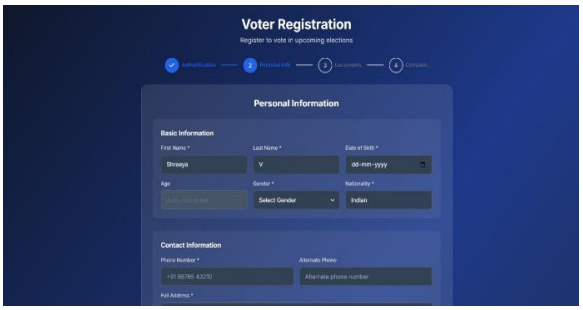


Figure 6: Voter Registration Interface

Figure 6 depicts that the voter registration module allows new users to enter their personal information and contact details for election enrollment in a secure manner. The form checks authenticity via multi-step verification; only verified persons can proceed further for biometric enrollment.

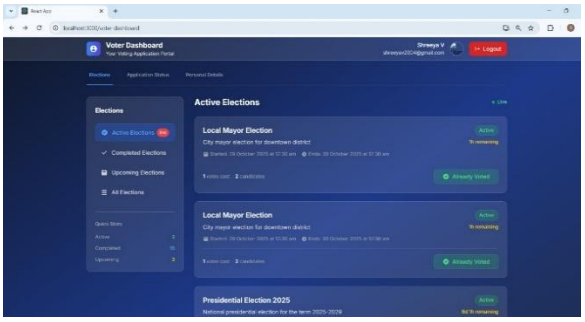


Figure 7: Voter Dashboard Interface

Figure 7 shows the Voter Dashboard, an interactive and secure interface where registered voters can view details of active, upcoming, and completed elections; they can cast their votes, while verification and monitoring access will still be limited to authorized government officials**.**

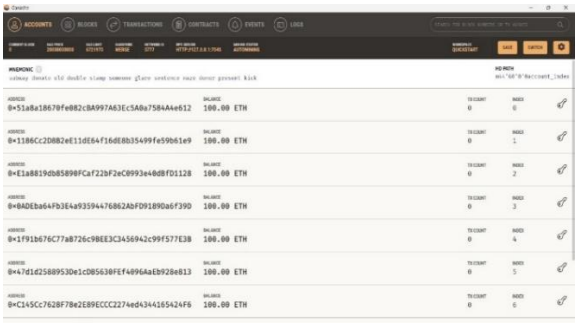


Figure 8: Blockchain Account Overview in Ganache

Figure 8: The Ganache interface displays Ethereum accounts created for vote storage and verification on the blockchain. Each account possesses a unique address and balance for the secure handling and traceability of encrypted voting data.

VI. CONCLUSION AND FUTURE ENHANCEMENT

Conclusion:

A deep understanding of biometric verification, encryption mechanisms, and distributed ledger technologies is needed to implement secure digital voting properly. Modeling the interaction between hardware modules, cryptographic algorithms, and blockchain synchronization is very important for achieving reliable and tamper-proof vote recording. Each of the technologies involved, namely, biometric sensing, cloud storage, and blockchain, introduces a different set of problems with respect to latency, consistency of data, and accuracy of authentication, making the design of a unified flexible architecture more complex and research-intensive.

Future Enhancement:

Next-generation biometric voting systems will incorporate advanced deep learning algorithms face and fingerprint recognition to improve accuracy under varied environmental conditions. Homomorphic encryption with zero-knowledge proof integration ensures complete voter privacy while allowing verifiable transparency. Future work can also leverage decentralized multi-node blockchain networks to scale up and make it fault-tolerant, together with real-time analytics dashboards for live result tracking. This work contributes toward developing a basis for intelligent, tamper-proof, and totally automated electronic election systems that are deployable on a large scale.

REFERENCES

[1] Fatima Abo-Akleek et al., “Leveraging blockchain for robust and transparent E-voting systems”, Cyber Security and Applications, vol. 3, no. –, pp. 100086, 2025

[2] Sandra Melovic et al., “Design and Implementation of an Electronic Voting System Using Blockchain Technology” 24th

International Symposium INFOTEH JAHORINA, no. 1, pp. 20 25, 2025.

[3] R. Ramyadevi and V. Priya, "Blockchain-Powered E-Voting System: A Secure and Transparent Solution with Three-Tiered OTP Security Mechanism" International Conference on Computing, Power, and Communication Technologies (IC2PCT), IEEE, pp. 728–731, 2024

[4] Abhishek Kaushik et al., "Fingerprint Based Voting System", 2023 3rd International Conference on Advancement in Electronics & Communication Engineering (AECE), pp. 51 55, 2023.

[5] Saurabh Singh et al., "Designing a Blockchain-Enabled Methodology for secure online voting system", Proceedings of the International Conference on Intelligent Data Communication Technologies and Internet of Things (IDC IoT 2023), pp. 178–184, 2023.

[6] V. Anitha, Orlando Juan Marquez Caro, R. Sudharsan, S. Yoganandan, and M. Vimal, "Transparent voting system using blockchain," Measurement: Sensors, vol. 25, pp. 100620, Elsevier, 2023.

[7] Ainampudi Kumari Sirivarshitha, Kothamasu Santhi Priya, Kadavakollu Sravani, and Vasantha Bhavani, "An Approach for Face Detection and Face Recognition using OpenCV and Face Recognition Libraries in Python," Proceedings of the 2023 9th International Conference on Advanced Computing and Communication Systems (ICACCS), pp. 1274–1278, IEEE, 2023.

[8] G. Revathy, K. et al., "Investigation of E-voting System Using Face Recognition Using Convolutional Neural Network (CNN)", Theoretical Computer Science, Vol. 925, pp. 61–67, 2022 Department of Electronics and Communication, GAT Page 20 Cloud Based Biometric Voting Platform with Tamper proof Block Chain Storage

[9] Thirumal R et al., "Electronic Voting Machine with Fingerprint and Facial Recognition", 2022 2nd International Conference on Next Generation Intelligent Systems (ICNGIS), 2022. [10]

[10] Venkateswara Rao Ch et al., "Arduino-Based Electronic Voting System with Biometric and GSM Features" Proceedings of the Fourth International Conference on Smart Systems and Inventive Technology (ICSSIT-2022), pp. 685–688, 2022

[11] Thirumal R et al., "Electronic Voting Machine with Fingerprint and Facial Recognition", 2022 2nd International Conference on Next Generation Intelligent Systems (ICNGIS), 2022.

[12] Venkateswara Rao Ch et al., "Arduino-Based Electronic Voting System with Biometric and GSM Features" Proceedings of the Fourth International Conference on Smart Systems and Inventive Technology (ICSSIT-2022), pp. 685–688, 2022

[13] B. Khokher, N. Kumar, P. Saha, and M. Jharait, "Electric Voting Machine Using ATMega Microcontroller for College Election," 2024 1st International Conference on Communications and Computer Science (InCCCS), Bengaluru, India, 2024, pp. 1–6. doi: 10.1109/INCCCS60947.2024.10593639.

[14] K. V. S. Sathvika, N. Lakshmareddy, N. Karthika, K. Tarun Sai, and M. V. L. N. Raja Rao, "An Internet-Based Electronic Voting Mechanism that Utilizes Facial Recognition and Fingerprint Identification," 2024 International Conference on Distributed Computing and Optimization Techniques (ICDCOT), Andhra Pradesh, India,2024,pp.1–6.doi: 10.1109/ICDCOT61034.2024.10516068.

[15] A. Yadu and O. Chandrakar, "A Smart Voting System Combining Fingerprint and Facial Recognition for Enhanced Security," ShodhKosh: J. of Visual and Performing Arts, vol. 5, no. 1, pp. 362-366, Jun. 2024. doi:10.29121/shodhkosh.v5.i1.2024.3183.

[16] M. Satyanarayana, R. Pranam T., P. Sai Charan Reddy and S. Sai Srinivas, "Biometric Based Electronic Voting System," IJRASET J. for Res. in Applied Science & Engineering,Technology2023. doi:10.22214/ijraset.2023.50796 .

[17] H. Mittal and N. Sengar, "A Blockchain and Face Recognition Based E-Voting System," IJRASET J. for Res. in Applied Science & Engineering Technology, vol , 2025. doi:10.22214/ijraset.2025.68648.

[18] N. R. Deepak, S. Taj, S. Khizer, S. Waqeer and T. Fathima, "e-Voting System using Fingerprint and Face Recognition Authentication with

Blockchain," J. of Advances in Computational Intelligence Theory, 2025

[19] K. Vinayachandra and K. Krishna Prasad, "Cryptography and Blockchain Based E-Voting System for Secured Voting Process," J. of Electrical Systems, vol. 20, no. 3, 2024.

[20] N. Kumar, S. Kumar, A. Waqar, and C. F. Y. Ngantung,"Modernizing Comprehensive Voting Approach Using Systems: A Blockchain, Biometrics and Zero Knowledge Proofs," Int. J. Electr., Comput. and Biomed. Eng., vol. 3, no. 3, pp. 598-619, Sep. 2025. doi:10.62146/ijecbe.v3i3.116.