Grenze International Journal of Engineering and Technology, June Issue

Development of Trust and Secured Voting System

Savitha A C[1], Aravind H S[2], Darshan G[3], Chidhanv K[4], Bindu R[5] and Varun C[6]
[1-6]JSS Academy of Technical Education, Bangalore, India
Email: savithaac@jssateb.ac.in

***Abstract*— The "Trust Vote: A Secure Voting System" project addresses the critical challenges of electoral fraud, duplicate voting, and unauthorized access in traditional voting systems. To enhance the integrity and transparency of the voting process, the system incorporates a multi-factor authentication approach using RFID verification, facial recognition, and fingerprint authentication. This layered security mechanism ensures that only eligible voters can cast a vote and strictly enforces the principle of "One Voter, One Vote." Additionally, the system leverages SQL-based secure data storage and incorporates a buzzer alert for unauthorized access attempts, further strengthening election security. Designed for scalability and reliability, the Trust Vote system represents a significant step toward secure, automated, and tamper-proof electronic voting, with the potential for future integration of block chain technology for added trust and immutability.**

***Index Terms*— first term, second term, third term, fourth term, fifth term and sixth term.**

I. INTRODUCTION

Elections are the foundation of any democracy, empowering citizens to choose representatives and influence governance. However, the integrity of the electoral process depends heavily on the security, transparency, and efficiency of the voting system. Traditional voting methods whether paper-based or electronic often face challenges such as voter fraud, multiple or duplicate voting, human error, and unauthorized access. To address these challenges, the work proposes *Trust Vote: A Secure Voting System*, a multi-layered authentication approach that integrates RFID verification, facial recognition, and fingerprint scanning [1]. By combining hardware like RFID modules, fingerprint scanners, and cameras with software Python-based biometric recognition and a secure database system, this system aims to provide a robust, scalable, and tamper-proof solution to ensure fair and reliable elections across various domains.

Motivation: The motivation of the work is to strengthen democratic processes by eliminating common weaknesses in existing voting systems. With the rapid advancement of biometric technologies, machine learning, and embedded systems, it has become feasible to design affordable, accurate, and real-time voter verification mechanisms. By integrating multiple layers of authentication, Trust Vote system aims to:

- Reduce the risk of voter fraud and identity theft.
- Enhance transparency and voter confidence.
- Minimize human errors and speed up the voting process.
- Provide a scalable solution adaptable to various election environments, from national polls to corporate and institutional voting

Contributions: We have developed the transparent voting system from the beginning to end. System specify the exact trusted voting platform.

Grenze ID: 01.GIJET.12.2.399_21

Earlier version of the design integrity is available in [2]. We have design and developed secure, multi-factor authentication voting system which combines RFID, face recognition, and fingerprint verification. To develop a system capable of real-time validation and alerting a buzzer is added in cases of any fraudulent or suspicious voting attempts. To store accurate data and tamper-proof result calculation MySQL is used.

II. LITERATURE REVIES

For various reasons like political occasion, crisis elections occurs. Number of voting systems are implemented, which are formal way of decision making procedure for selection of leader. General election, primary elections, municipal elections and special elections are the different types of elections occurs. Once the election is over, nomination process starts, and finally officially candidates is selected. In order to follow the voting process different kinds of methods are employed which is fixed by ACE Electoral Knowledge Network [3-5].

A. Manual Voting

Manual voting is the oldest and first method used for longer days. In this system candidate has to vote by seeking his/her name on printed ballot. After the completion of voting process, in polling station envelopes are opened, put them in files and starts voting counting for each students. The process is repeated until the final result should similar. If they found dis-similar in counting they repeat it again. The conventional methods s problematical due manual counted by hand.

B. Electronics Manual Voting

After working with conventional methods of voting system they come up with new e-voting scheme. It is a electronic technology which includes multiple mechanisms like visual vote scanning systems, voting kiosks, punched cards, transmission of ballots, voting through telephone, Internet, and computer networks. Electronic voting system increases the speed of counting process, accessible for remote location voters, disabled persons, and also gives secured reliable of elections.

C. Mobile Voting Systems

Mobile is one of the essential of life due to small small size, easy to use and cost effective. It give solutions to examine uniqueness of human. Bio metrics are introduced to examine uniqueness of human by considering different parameters like fingerprints, eye retinas and irises, DNA, voice patterns, and facial patterns. This approach is highly reliable for authentication purposes. If the identical authentication occurs beep is heard it stops scanning process.

In [7,8] presents a secure voting model that combines finger print authentication with IoT-based data storage. The system verifies each voter using a finger print sensor and uploads the voting data to a cloud server for real-time monitoring and faster result generation. Any mismatched fingerprint instantly triggers a fraud alert, preventing unauthorized voters from accessing the machine. By automating vote storage and reducing manual involvement, the system enhances transparency and improves accuracy when compared to traditional paper-based procedures. In [9], the author presents a dual-layer authentication model using RFID verification followed by frontal face recognition. Each voter must first scan their RFID card, after which the system captures the voter's face and compares it with the stored template. Only when both verification stages are successful does the system unlock the voting interface. This combination of RFID and facial recognition minimizes impersonation, reduces manual checking at polling booths, and provides a faster and more secure voting experience. Pradeep Katta et.al, proposes a multi-factor voting system that uses fingerprint authentication, facial recognition, and OTP verification before allowing a voter to cast their vote. Once authenticated, the vote is encrypted and stored on a block chain network, ensuring tamper-proof and transparent record-keeping. The system is designed especially for remote voters who cannot access physical polling stations. By combining biometric validation with block chain storage, the model strengthens security and prevents vote manipulation or unauthorized access [10,11]. In [12], the author uses Aadhaar -linked fingerprint and facial recognition for voter authentication. The system applies the LBPH algorithm for facial matching and cross-verifies the fingerprint to ensure the voter's identity before enabling the voting option. This dual-biometric approach prevents duplicate voting and reduces impersonation attempts. The authors also note challenges such as privacy concerns and limited digital infrastructure in rural regions, which may affect large-scale adoption. S. Ganesh Prabhu et al [13], introduces a remote voting platform that verifies users using facial recognition followed by OTP verification. After successful authentication, voters can cast their vote online through a secure interface, and the results are processed instantly. This model aims to improve voter participation, especially for individuals in remote locations or those with

mobility difficulties. The system offers convenience and real-time results but depends heavily on reliable internet connectivity and secure handling of biometric data. In paper [14], the author uses a combination of RFID verification and fingerprint authentication to validate voters before they are allowed to cast their vote. The micro controller-based system automates vote counting and eliminates human error associated with manual tallying. This dual-biometric approach enhances security by ensuring that only legitimate voters can access the machine. However, the system's scalability is limited in rural areas due to dependency on stable power and communication infrastructure. Finally, the literature collectively suggests that future e-voting systems must adopt a balanced approach, combining technical robustness, strong cyber security measures, and regulatory compliance.

III. PROPOSED SYSTEM

Secure ballot trusted voting platform is built around an Arduino Uno micro controller, which controls all operations and interfaces with input and output devices. The system ensures secure voting through multi-factor authentication using RFID, facial recognition, and fingerprint verification. The RFID module reads the voter's card, the camera module captures the face for recognition, and the fingerprint module verifies the fingerprint. The Arduino Uno processes these inputs sequentially, communicating with the database to confirm voter identity. Only voters who pass all three checks can proceed to cast their vote. The database stores voter details and vote records, blocking used IDs to prevent duplicate voting. Output devices - LCD display, buzzer, and LED - provide real-time feedback and alerts. Votes are securely stored once cast, ensuring a tamper-proof, reliable, and efficient voting process. Figure 1 shows the proposed hardware diagram.

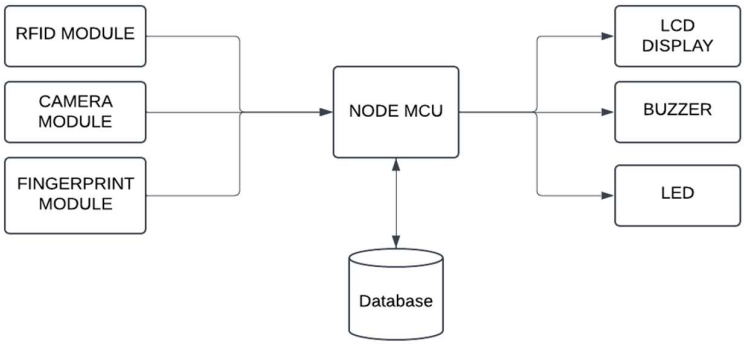

Figure 1. Block diagram of the proposed system

The workflow of the proposed system is designed to ensure secure, authenticated, and tamper-proof voting. The system follows a structured sequence of steps for voter verification, vote casting, and result generation:

- The system initializes and enters standby mode, ready for voter authentication.
- The system reads the voter's RFID card and checks it against the database.
  - If the RFID does not match, access is denied and the buzzer is triggered.
  - If the RFID matches, the system proceeds to facial recognition.
- The camera captures the voter's face and compares it with stored records.
  - Mismatch results in rejection and buzzer alert.
  - Match allows the system to proceed to fingerprint verification.
- The voter scans their fingerprint for final verification.
  - Mismatch triggers the buzzer and denies voting.
  - Match permits access to the voting interface.
- Once all authentication steps are passed, the voter is allowed to cast their vote.
- The voter selects their preferred candidate using the interface.
- An LED indicator blinks to confirm that the vote has been successfully recorded.
- The system securely stores the vote in the database and encrypts the data for safety.
- The voter's ID is marked as "voted" to prevent multiple submissions.
- The system completes the voting session for that voter.
- Vote Counting - The back end automatically counts the total number of valid votes.
- The election results are displayed securely and transparently.

This systematic workflow ensures that only authenticated voters can participate, prevents duplicate votes, and maintains the integrity and transparency of the election process. Figure 2 shows the flowchart of the voting process.

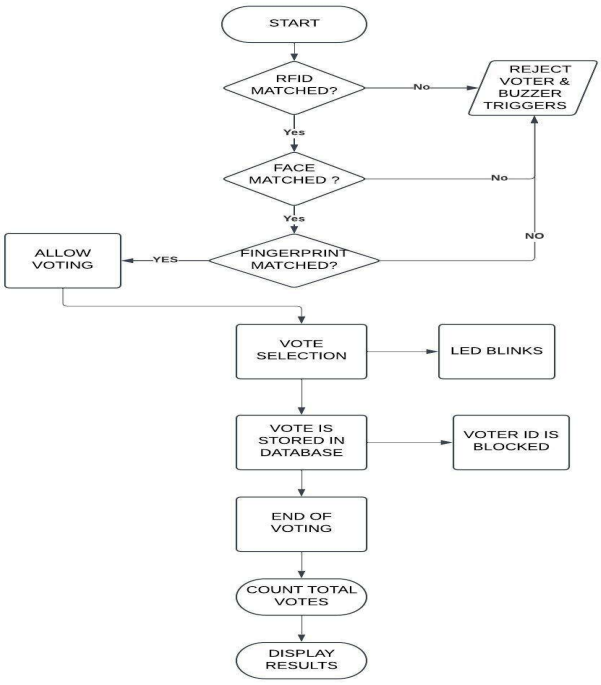

Figure 2. Flow chart of voting process

IV. RESULTS AND DISCUSSION

The work was successfully implemented and tested to validate its efficiency, accuracy, and security in the voting process. The main motto of our work is to free from fraud voting, and it should be fair and transparent. From the results we can make sure that proposed voting system operates more reliable, effective and trusted. In the testing process each module is evaluated and tested. After integration full functionality of the voting machine is verified. Through RFID module registered voters accurately are identified. If any unregistered person comes for voting it will show right away denied access. Immediately it triggers the buzzer alert, for stop for voting. From the face recognition module, it compares the faces of registered voting person through camera connected in the voting system. If any mismatch found in the image immediately it stop for further processing. The app was implemented by using Python and Open CV. Further enhanced voting system is implemented by using fingerprint authentication module. Comparison of each voter's fingerprint is done with the previously stored biometric data. If the finger prints matches then only allow for voting. Hence in this way all three authentications RFID, face, and fingerprint are successfully developed which ensures trusted and secured vote. The LCD outputs illustrated in Figure 3(a), (b) and (c). show case the operational performance of the developed secured voting platform.These snapshots represent real-time data captured during system testing and demonstrate the effectiveness of the model in verifying voter identity through RFID scanning, voter ID confirmation, and fingerprint authentication. The outputs confirm that each authentication module functions correctly and that the system can securely identify and validate eligible voters before allowing them to cast their vote. In Figure 3(a), the RFID module reads the voter's RFID card when it is brought near the scanner. The LCD display shows the message "RFID Success", indicating that the RFID tag has been successfully read and matched with a valid entry in the database. This step verifies the voter's unique identification number and ensures that only registered voters can proceed to the next authentication phase. If an unregistered card is scanned, the system would display an error message and deny further access. This output confirms that the RFID module is functioning correctly and acts as the first layer of security in the voting system. Moving on to Figure 3(b), once the RFID verification is completed, the system retrieves the corresponding voter details from the database. The LCD screen displays

"Voter ID Verified" followed by the voter's name, indicating that the system has recognized the voter's unique identity associated with the scanned RFID card. This output proves that the communication between the RFID module, the micro controller, and the database is successful. By displaying the voter's name, it also helps election officials verify the authenticity of the voter before proceeding to the next step of authentication, enhancing transparency in the process. Figure 3 (c) shows the final authentication step followed. From overall we successfully completed multi layered verification in real-time world.

Figure 3(a). RFID reads voter ID

Figure 3(b). Verification of RFID

Figure 3(c). Final authentication verification

A. Benefits

- It reduces the cost of election like ballot's printing, employing staff.
- It reduces the human errors for final result counting.
- Encourage for more participation.
- It speed up the voting process.

B. Application

- Used for student council elections, class representative selection, or department-level voting to eliminate manual counting and ensure one-student-one-vote fairness.
- Companies can use it for internal decision-making, employee representative elections, policy voting, or annual general meetings.
- Can be used in official government or local body elections as a secure and tamper-proof alternative to traditional EVMs.
- Residential associations, gated communities, and local groups can conduct transparent voting on rules, budgets, or facility usage.
- Higher education bodies like the Senate, Board of Studies, or Faculty Council can conduct confidential and authenticated voting on academic regulations, curriculum approval, and policy decisions.
- Board of directors can vote securely on high-level decisions, ensuring strict authentication and preventing unauthorized participation.
- Used in technical fests, cultural events, hackathons, or competitions where judges cast votes securely. Multi-layer authentication avoids bias or duplicate scoring.
- Helps societies elect presidents, treasurers, and committee members transparently, reducing disputes and increasing trust among members.
- Departments that need internal voting for tender approvals, project approval committees, or welfare scheme selections can use it for secure decision-making.

- Sports clubs, NGOs, religious organizations, and membership groups can conduct internal elections smoothly and securely.
- Startups with multiple founders or investors can conduct voting on equity decisions, policy changes, or funding approvals with full security.

V. Conclusion and Future Scope

The work successfully demonstrates a modern, efficient, and reliable approach to conducting elections with enhanced security, transparency, and accuracy. In addition, the system can be developed into a portable and wireless voting terminal using IoT modules to enable secure remote or mobile voting. The inclusion of a user-friendly graphical interface and multilingual support will make the system accessible to a wider range of users. With these enhancements, "A SECURE BALLOT: TRUSTED VOTING PLATFORM" has the potential to evolve into a large-scale, fully automated, and highly secure voting platform—revolutionizing the way elections are conducted and strengthening the foundation of democratic governance.In furure work Block chain can be used to store votes in an immutable ledger, ensuring that voting records cannot be altered, deleted, or tampered with. This increases transparency and makes the system fully audit-proof. Multiple voting terminals across different locations can be linked to a secure cloud server. This allows real-time monitoring, centralized data management, and immediate result generation for large-scale elections.

References

[1] Acemyan, C.Z., Kortum, P. and Oswald, F.L., 2022. The trust in voting systems (TVS) measure. International Journal of Technology and Human Interaction (IJTHI), 18(1), pp.1-23.

[2] Robertson, S. (2005). Voter-centered design: Toward a voter decision support system. ACM Transactions on Computer-Human Interaction, 12(2), 263–292. doi:10.1145/1067860.1067866.

[3] Savitha, A.C. and Reddy, M.D.B., 2023. Women safety detection and alerting system using facial expression: a survey.

[4] Joint EC-UNDP Task Force. (2012, April 17). Biometric Voter Registration: Skills required and problems encountered? Retrieved August 16, 2012, from Aceproject Web site: http://aceproject.org/

[5] AC, D.S., 2025. Modern Circuits and Systems Technologies (MOCAST) on Machine Learning Applications in Communications and Electronics. Published in Zhongguo kongjian kexue jishu/Chinese Space Science and Technology, Web of Science (ESCI) Indexed Journal, 21(11).

[6] AC, D.S., KM, M.K., DH, J., Bedre, K. and DS, M., 2025. Biometric Attendance System Based on Fingerprints. Journal of Scholastic Engineering Science and Management (JSESM), A Peer Reviewed Universities Refereed Multidisciplinary Research Journal, 4(5), pp.69-73.

[7] Yusoff, Z.M., Yusnoor, Y., Markom, A.M., Nordin, S.A. and Ismail, N., 2023. Fingerprint biometric voting machine using internet of things. Indonesian Journal of Electrical Engineering and Computer Science, 30(2), p.699.

[8] AC, D. S., KM, M. K., & MS, P. (2025). Implementation of Color Detection Tool for Blind People. Journal of Scholastic Engineering Science and Management (JSESM), A Peer Reviewed Refereed Multidisciplinary Research Journal, 4(5), 19-23.

[9] Priyadarshini, R., Shangamithra, D., Swathi, T., Subhaharini, G., & Sreenivasan, L. (2020). Design and realization of RFID based smart voting system with frontal face recognition technique. International journal of innovative research in technology, 6(12), 338-343.

[10] Amato, G., Falchi, F., Gennaro, C., Massoli, F.V., Passalis, N., Tefas, A., Trivilini, A. and Vairo, C., 2019, June. Face verification and recognition for digital forensics and information security. In 2019 7th International Symposium on Digital Forensics and Security (ISDFS) (pp. 1-6). IEEE.

[11] Bhuvaneswary, N., Reddy, C.V., Aravind, C. and Prasad, K.H., 2022, May. Smart Voting Machine using Fingerprint Sensor and Face Recognition. In 2022 International Conference on Applied Artificial Intelligence and Computing (ICAAIC) (pp. 1159-1166). IEEE.

[12] Prabhu, S.G., Nizarahammed, A., Prabu, S., Raghul, S., Thirrunavukkarasu, R.R. and Jayarajan, P., 2021, March. Smart online voting system. In 2021 7th International conference on advanced computing and communication systems (ICACCS) (Vol. 1, pp. 632-634). IEEE.

[13] BalaMurali, A., Sravanthi, P.S. and Rupa, B., 2020, January. Smart and secure voting machine using biometrics. In 2020 Fourth International Conference on Inventive Systems and Control (ICISC) (pp. 127-132). IEEE.

[14] Sridharan, S., 2013, July. Implementation of authenticated and secure online voting system. In 2013 Fourth International Conference on Computing, Communications and Networking Technologies (ICCCNT) (pp. 1-7). IEEE.