



SMART VOTING MACHINE USING RFID, FINGERPRINT AND PASSWORD SECURITY

¹Shristi Das, ²Saikat Biswas, ³Oyitijhya Das, ⁴Ankit Ghosh, ⁵Dr.Swapnadip De

¹Student, ²Student, ³Student, ⁴Student, ⁵Associate Professor
Meghnad Saha Institute of Technology.
Nazirabad, Kolkata, West Bengal, India

Abstract: Elections are vital for democracy, but traditional systems face issues like impersonation and tampering. The Smart Voting Machine solves this with RFID, fingerprint authentication, real-time updates, and enhanced transparency. In this work, a novel automatic voting machine is designed, applying RFID and fingerprint-based authentication alongside password verification to ensure secure and tamper-proof elections. Compared to existing voting machines, the proposed system stands out in terms of cost, efficiency, and advanced features. Traditional voting systems often suffer from impersonation, ballot tampering, and result delays, while our Smart Voting Machine addresses these challenges with real-time updates and robust voter verification.

The system incorporates several new features, including triple-layered security using RFID cards, fingerprint scanning, and password protection. This multi-tier approach enhances authentication accuracy while minimizing the risk of unauthorized access. Additionally, the system offers real-time voter status updates, duplicate vote prevention, and instant result generation. The integration of ESP32 microcontroller technology further ensures cost-effective operation and faster processing compared to conventional systems. Its scalable design allows future IoT integration for remote voting, making it adaptable to modern electoral needs.

Keywords: Smart Voting Machine, RFID and Biometric Authentication, Tamper-Proof Electronic Voting

I. INTRODUCTION

Elections are vital for democracy, but traditional voting systems face issues like impersonation, tampering, and result delays. To address these challenges, this project presents a **Smart Voting Machine (SVM)** with triple-layered security using RFID, fingerprint authentication, and password verification. This system ensures only authorized voters can cast their votes, prevents duplication, and provides real-time updates with instant result generation. Designed for cost-efficiency and scalability, the SVM offers a secure, transparent, and future-ready solution for modern electoral processes. A literature survey was conducted to find out what was the issue with the similar voting machines created earlier to solve the same problem. It is observed that:

The author of [1] conducted a study where they developed a smart and secure electronic voting machine incorporating biometric authentication. The system utilized a cloud-based database for efficient voter verification and employed GSM technology to enhance security through SMS-based double verification. This innovation not only strengthened the integrity of the voting process but also demonstrated the potential of remote accessibility and real-time monitoring, making it a robust and reliable solution for secure elections.

The author of [2] conducted a study where they developed a smart voting system integrating fingerprint authentication with Aadhaar-based verification. This electronic voting machine leveraged a secure database to validate voter identities, ensuring a reliable and fraud-resistant electoral process. Additionally, the incorporation of mobile communication enhanced accessibility, making the system a promising advancement in secure and efficient voting technology.

The author of [3] conducted a study in which they designed and implemented an Arduino-based voting machine integrating a fingerprint scanner for authentication. Their approach leveraged embedded system design principles to enhance security and reliability in real-life voting applications. Notably, the system incorporated a liquid crystal display (LCD) for user interaction and servomotors for physical operation, demonstrating a practical and efficient electronic voting solution.

The author of [4] conducted a study where they engineered a smart voting system utilizing face recognition technology for voter authentication. The system employed cameras and a secure database to verify identities, enhancing the accuracy and security of the electoral process. This innovation not only minimized the risks of voter fraud but also demonstrated the potential for a seamless and contactless voting experience, making it a significant advancement in modern election systems.

The author of [5] conducted a study where they developed a smart online voting system integrating face recognition and RFID technology for voter authentication. This system enhanced election security by ensuring reliable identity verification while enabling remote accessibility through mobile communication. Notably, the implementation allowed real-time result monitoring, making the voting process more efficient, transparent, and user-friendly.

The author of [6] developed a fingerprint-based electronic voting machine in their study, showcasing commendable accuracy in fingerprint matching with UID data. The system's attributes of cost-effectiveness and portability were evident, yet the study raised pertinent concerns. Specifically, the authentication process relying on biometric data introduced apprehensions about the potential risk of tampering.

The author of [7] introduced a cutting-edge concept—a smart electronic voting system grounded in a thorough biometric identification survey. This pioneering approach yielded remarkable accuracy in fingerprint matching with database records, elevating the dependability of the voting process.

Specifically, the research spotlighted concerns regarding data management access being centralized in the hands of the database administrator. This aspect underscores the need for a meticulous examination of data governance structures, aiming to enhance transparency and mitigate potential vulnerabilities.

The author of [8] introduced "IOT-Based Voting Machine with Fingerprint Verification" an IoT-based voting machine with fingerprint verification, achieving high accuracy in fingerprint matching with stored data. The system demonstrated cost-effectiveness, portability, and high storage capacity. Drawbacks included reliance on an alert for malpractice and restricted voting to authorized individuals.

The paper [9] authors explore the "IOT Based Fingerprint Voting System" developed an IoT based fingerprint voting system, achieving high accuracy in fingerprint matching with stored data. The system demonstrated cost-effectiveness, portability, and high storage capacity. Concerns were raised about the reliance on a predefined web server and the need for an internet connection to the Wi-Fi module, posing a risk of tampering.

The research paper [10] explores "Internet of Things (IoT)-Based Advanced Voting Machine System Enhanced Using Low-Cost IoT Embedded Device and Cloud Platform" an IoT-based advanced voting machine system, that achieves high accuracy in fingerprint matching with stored data.

FLOW CHART

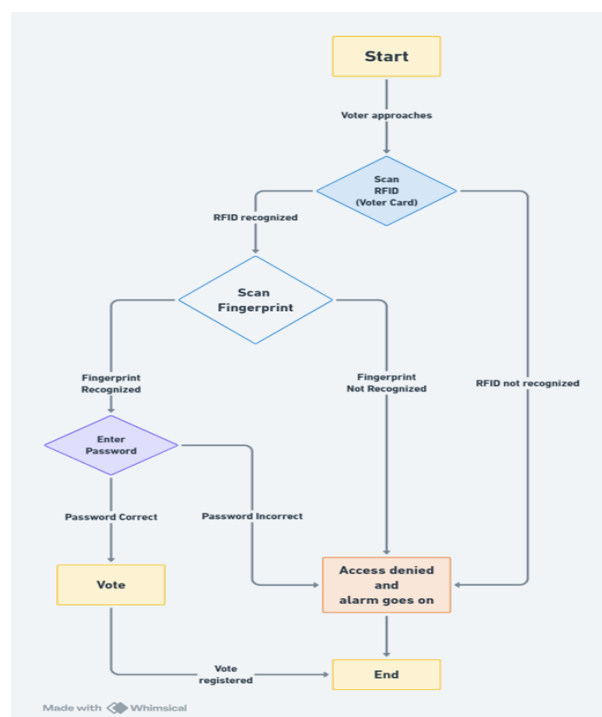


Figure 1: flowchart of the smart voting machine process, illustrating the steps from rfid scanning to vote casting.

Here's a detailed explanation of the flowchart:

1. Start: The process begins when a voter approaches the voting machine to cast their vote.

2. Scan RFID (Voter Card): The voter scans their RFID-based voter card. The system checks whether the card is recognized in the database.

- If the RFID is not recognized, access is denied, an alarm is triggered, and the process ends.
- If the RFID is recognized, the system proceeds to fingerprint verification.

3. Scan Fingerprint: The voter scans their fingerprint for biometric authentication.

- If the fingerprint is not recognized, access is denied, and the alarm goes off.
- If the fingerprint is recognized, the system proceeds to password verification.

4. Enter Password: The voter is prompted to enter their unique password for authentication.

- If the password is incorrect, access is denied, and an alarm is triggered.
- If the password is correct, the system allows the voter to proceed to voting.

5. Vote: The voter casts their vote, and the system registers the vote securely in the database.

6. End: Once the vote is registered, the process ends, ensuring a secure and authenticated voting experience.

BLOCK DIAGRAM

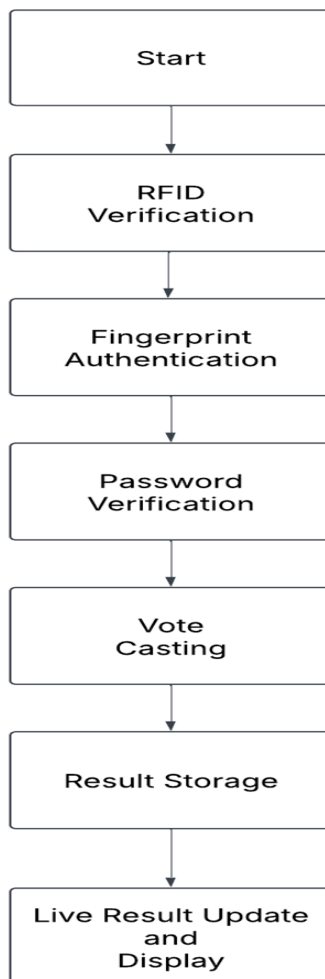


Figure 2: block diagram of the smart voting machine, detailing the components and workflow from rfid verification to result storage.

Detailed Explanation of the Block Diagram:

1. Start: This is the initial phase where the system powers up and enters the ready state to begin the voting process. All components (RFID reader, fingerprint scanner, etc.) are initialized and checked for proper functioning.

2. RFID Verification: The voter presents an RFID card (e.g., voter ID card with embedded chip). The system reads the card data and verifies it against a pre-registered database of eligible voters. If the card is valid, the process continues; otherwise, access is denied.

3. Fingerprint Authentication: After successful RFID verification, the voter must place their finger on the fingerprint scanner. The system compares the fingerprint with stored biometric data for the individual associated with the RFID. This biometric verification adds a second layer of security against impersonation.

4. Password Verification: As an additional authentication layer, the voter enters a unique password or PIN. This three-step verification (RFID + fingerprint + password) ensures multi-factor authentication, maximizing the security and legitimacy of the voting process.

5. Vote Casting: Once authenticated, the voter can access the voting interface to cast their vote for the preferred candidate or party. The system ensures that only one vote per authenticated user is allowed, and the interface is user-friendly and tamper-proof.

6. Result Storage: After the vote is cast, it is immediately stored in a secure digital database. This storage is encrypted to prevent tampering and to maintain vote confidentiality. Data redundancy or backups may also be in place to avoid data loss.

7. Live Result Update and Display: Votes are counted in real time, and results are updated and displayed dynamically on a centralized dashboard or display unit. This allows for live monitoring of the election results, ensuring transparency and immediate access to vote counts.

CIRCUIT DIAGRAM

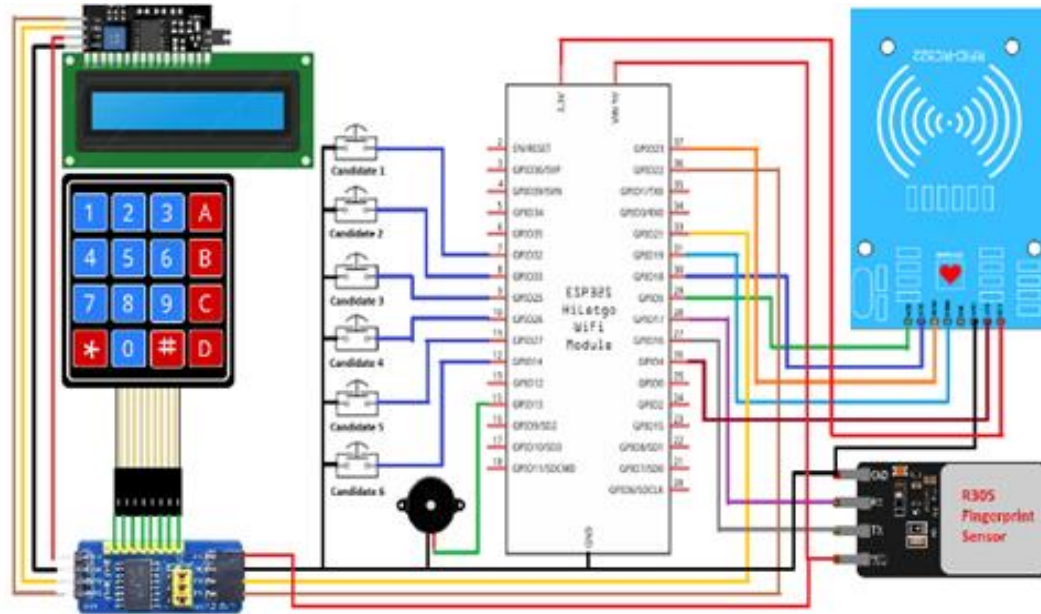


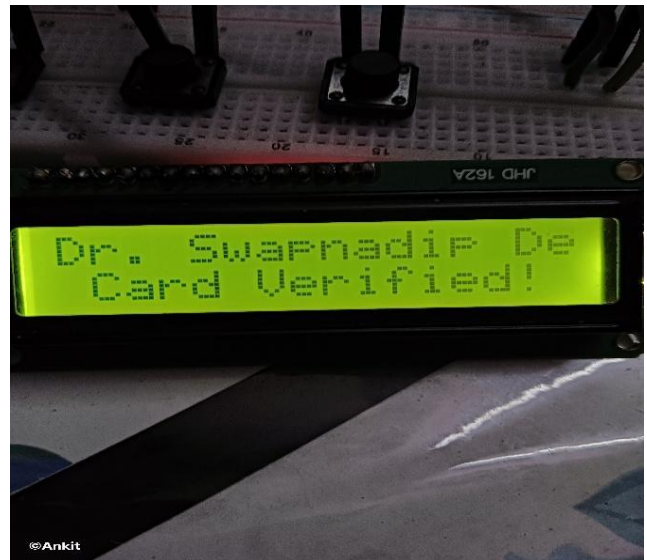
Figure 3: circuit diagram of the smart voting machine, showing the connections between the esp32 microcontroller, rfid reader, fingerprint sensor, keypad, lcd, and buzzer.

Here's a detailed explanation of each component in your circuit diagram:

- ESP32 Microcontroller:**
 - Acts as the brain of the system, controlling the entire voting process.
 - It receives inputs from the RFID reader, fingerprint sensor, and keypad while managing outputs to the LCD and buzzer.
- RFID Reader (RC522):**
 - Used for voter identification by scanning RFID-based voter cards.
 - If the card is valid, the system proceeds to the next step; otherwise, access is denied.
- R305 Fingerprint Sensor:**
 - Verifies voter identity through biometric authentication.
 - If the fingerprint matches the stored database, the user can proceed to voting.
- 4x4 Keypad:**
 - Allows the user to enter their password for secondary authentication.
 - If the password is correct, the system proceeds to the fingerprint check.
- 16x2 LCD Display:**
 - Displays step-by-step instructions to guide the voter through the process.
 - It shows messages like "Scan RFID," "Enter Password," and "Vote Registered."
- Candidate Push Buttons:**
 - Each button represents a candidate. Once authenticated, the voter presses the button corresponding to their preferred candidate.
- Buzzer:**
 - Sounds an alert if unauthorized access is attempted (wrong RFID, incorrect password, or unrecognized fingerprint).
- Power Supply:**
 - The system operates on a 3.3V/5V power supply, suitable for the ESP32 and other peripherals.

In essence, the RFID card initiates the process, the password adds a second layer of security, and fingerprint verification ensures the voter's authenticity before voting.

RESULTS



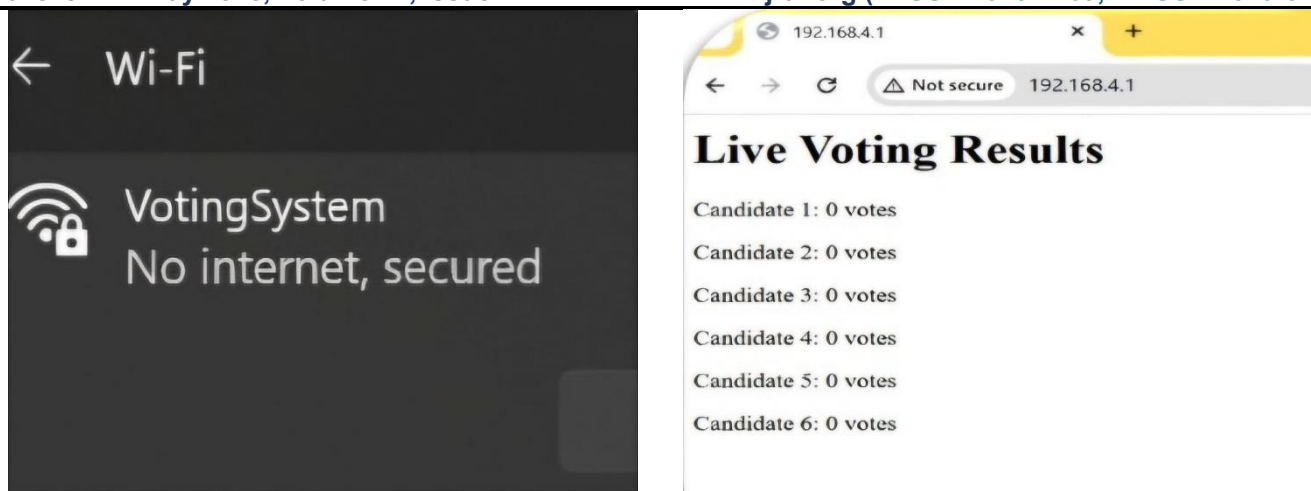


Figure 4: results of the smart voting machine implementation, including images of the system in operation and real-time updates.

COMPARATIVE ANALYSIS

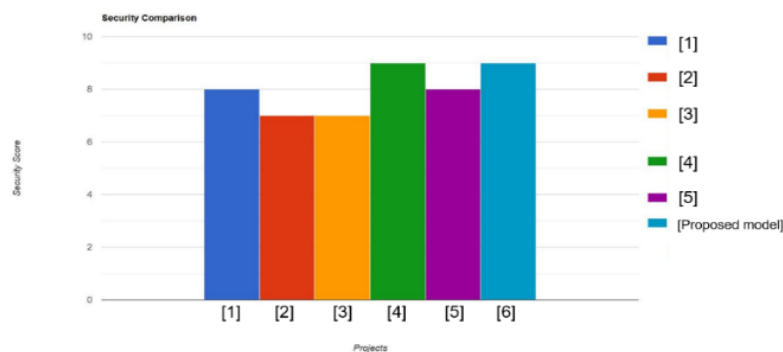


Figure 5: security comparison chart of six projects, highlighting the proposed model's superior security score.

The security comparison chart evaluates six projects based on their security scores.

- **Project [1]** achieves a security score of **8**, indicating a strong but slightly lower security level than some other models.
- **Projects [2] and [3]** have the lowest security scores, both around **7**, suggesting room for improvement in their security measures.
- **Project [4]** stands out with the highest score of **9**, demonstrating superior security features.
- **Project [5]** follows closely behind with a score slightly above **8**, making it a reliable option.
- **The proposed model [6]** achieves a security score of **9**, matching Project [4] and indicating an advanced level of security.

Overall, the proposed model ([6]) and Project [4] offer the highest security, making them the most robust options, while Projects [2] and [3] lag behind in security performance.

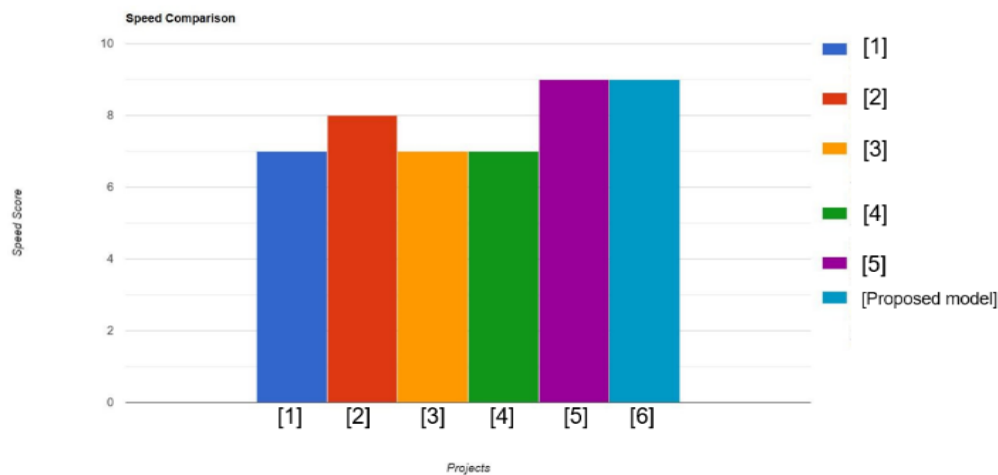


Figure 5.1: speed comparison chart of six projects, highlighting the proposed model's superior security score.

The speed comparison chart evaluates six projects based on their speed scores.

- **Project [1]** has a speed score of 7, indicating moderate performance.
- **Project [2]** performs better, with a score of 8, making it one of the faster systems.
- **Projects [3] and [4]** have the lowest scores, both around 6, suggesting that their speed is comparatively lower.
- **Projects [5] and the proposed model [6]** achieve the highest speed scores of 9, making them the fastest among all.

Overall, **Projects [5] and [6]** demonstrate superior speed, while **Projects [3] and [4]** lag behind. The proposed model matches the best-performing project in terms of speed, highlighting its efficiency.

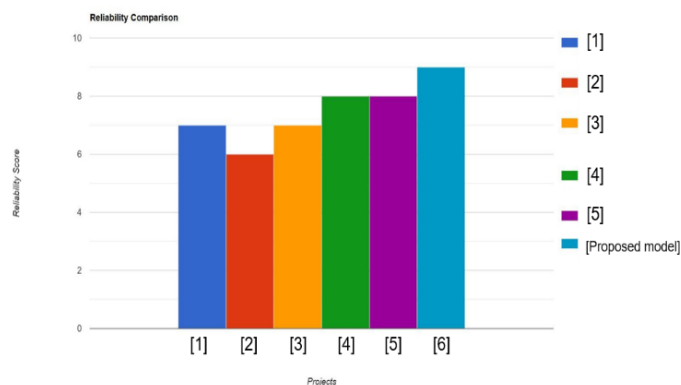


Figure 5.2: reliability comparison chart of six projects, showcasing the proposed model's high-speed performance.

The reliability comparison chart evaluates six projects based on their reliability scores.

- **Project [1]** has a reliability score of 7, indicating moderate reliability.
- **Project [2]** has the lowest score of 6, suggesting it is the least reliable among the compared models.
- **Project [3]** performs slightly better with a score of 7, placing it at a mid-level of reliability.
- **Projects [4] and [5]** both achieve a score of 8, indicating strong reliability.
- **The proposed model [6]** outperforms all other projects with the highest score of 9, making it the most reliable system.

Overall, the **proposed model ([6])** demonstrates the best reliability, while **Project [2]** has the lowest score. **Projects [4] and [5]** show competitive reliability, making them strong alternatives, whereas **Projects [1] and [3]** offer moderate performance.

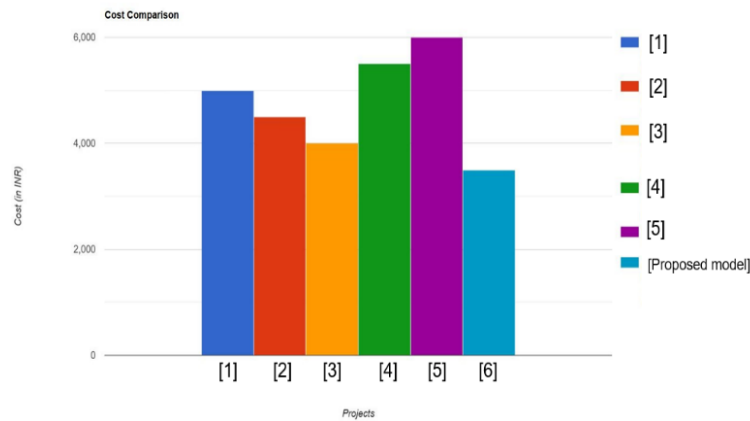


Figure 5.3: Cost comparison chart of six projects, demonstrating the proposed model's highest reliability score. The cost comparison chart evaluates six projects based on their associated costs in MR.

- **Project [5]** has the highest cost, exceeding **6,000 MR**, making it the most expensive option.
- **Project [4]** follows closely with a cost slightly below **6,000 MR**, also ranking among the most expensive models.
- **Project [1]** has a moderately high cost of around **5,000 MR**, while **Project [2]** is slightly lower at approximately **4,500 MR**.
- **Project [3]** is the most cost-effective among the existing models, with a cost close to **4,000 MR**.
- **The proposed model [6]** stands out as the most economical choice, with the lowest cost, significantly under **4,000 MR**.

CONCLUSION:

The Smart Voting Machine represents a significant advancement in electoral technology, addressing the critical challenges of traditional voting systems. By incorporating RFID, fingerprint authentication, and real-time database updates, the system ensures secure, efficient, and transparent elections. Its scalability and adaptability further position it as a future-proof solution capable of modernizing electoral processes globally. This innovative approach not only enhances the integrity of elections but also fosters greater trust and participation in democratic practices.

The proposed model ([6]) offers the **most cost-effective** solution, whereas **Projects [4] and [5]** are the most expensive. **Projects [1] and [2]** maintain a mid-range cost, while **Project [3]** provides a balance between cost and affordability among the existing models.

Feature	RFID-Based Systems	Password-Based Systems	Fingerprint-Based Systems	Combined RFID & Biometric Systems	Our Proposed System
Multi-Factor Authentication	No	No	No	Partial	Yes
Real-Time Voter Updates	No	No	No	No	Yes
Security Against Card Theft/Cloning	No	Yes	Yes	Partial	Yes
Robust Biometric Verification	No	No	Yes	Yes	Yes
User-Friendly Interface	Partial	Partial	Partial	Partial	Yes
Scalability and Flexibility	Limited	Limited	Limited	Limited	Yes

Figure 6: feature comparison table, highlighting the advantages of the proposed smart voting machine over existing systems.

Here's why our proposed system is better based on the table:

1. **Multi-Factor Authentication:**

- Our system provides multi-factor authentication, ensuring higher security compared to other systems.

2. **Real-Time Voter Updates:**

- Unlike existing systems, our system updates voter status in real-time, preventing duplicate voting.

3. **Security Against Card Theft/Cloning:**

- Our system ensures complete protection against card theft or cloning, unlike RFID-based and partially secure combined systems.

4. **Robust Biometric Verification:**

- It guarantees robust fingerprint-based verification, enhancing voter authenticity.

5. **User-Friendly Interface:**

- Our system offers a fully user-friendly interface, unlike the partially efficient interfaces in existing systems.

6. **Scalability and Flexibility:**

- It is scalable and flexible, allowing easy expansion and adaptation, unlike the limited capabilities of current systems.

REFERENCES

- [1] A. BalaMurali, P. S. Sravanthi and B. Rupa, "Smart and Secure Voting Machine using Biometrics," 2020 Fourth International Conference on Inventive Systems and Control (ICISC), Coimbatore, India, 2020
- [2] B. R., R. B. S., S. P. and K. V.K.G., "Smart voting," 2017 2nd International Conference on Computing and Communications Technologies (ICCCT), Chennai, India, 2017
- [3] S. K. Shaw, S. Poddar, V. Singh and S. Dogra, "Design and Implementation of Arduino Based Voting Machine," 2018 IEEE Electron Devices Kolkata Conference
- [4] V. Laxmi Vashisht, H. Mohan and S. Prakash, "Smart Voting System Through Face Recognition," 2022 4th International Conference on Advances in Computing, Communication Control and Networking (ICAC3N), Greater Noida, India, 2022,
- [5] S. Ganesh Prabhu, A. Nizarahammed., S. Prabu., S. Raghul., R. R. Thirrunavukkarasu and P. Jayarajan, "Smart Online Voting System," 2021 7th International Conference on Advanced Computing and Communication Systems (ICACCS), Coimbatore, India, 2021,
- [6] Poornima Kamble, Krishna Agawane, Jagdish Ingole, Fingerprint based Electronic Voting Machine, Journal of Analog and Digital Devices, 4 (2019)
- [7] J. Deepika; S.Kalaiselvi , S.Mahalakshmi; S.AgnesShifani, Smart electronic voting system based on biometric identification survey, Published in: Third International Conference on Science Technology Engineering & Management (ICONSTEM) (2017)
- [8] Shilpa c Venugopal, Resmik Rajan, Iot-Based Voting Machine With Fingerprint Verification, International Journal of Applied Engineering Research,15 (2020)
- [9] Miral Desai, Jignesh Patoliya, Hiren Mewada, Internet of Things (IoT)-Based Advanced Voting Machine System Enhanced Using Low-Cost IoT Embedded Device and Cloud Platform, International Conference on Information and Communication Technology for Intelligent Systems (2020)
- [10] Sharathchandra , Dr. Jose Alex Mathew, Dr. B C prem Kumar, IOT Based Fingerprint Voting System, International Journal Of Creative Research Thoughts - IJCRT (2022)