International Journal of Scientific Research & Engineering Trends
Volume 12, Issue 3, May-Jun-2026, ISSN (Online): 2395-566X

Embedded System Based Smart E-Voting System Using Authentication Technologies

Kishor Ugale[1], Tushar Pandhi[2]
[1,2]Assistant Professor, MET's Institute of Engineering, Department of Electrical Engineering

Abstract: Traditional Voting plays a very important role in modern republic systems. Electronic voting (e-Voting) refers to any method of casting or recording votes through electronic technologies. Voting machines consist of the whole combination of mechanical, electromechanical, or electronic components-along with the necessary software, firmware, and documentation-used for programming, controlling, and supporting the voting process. The e-Voting system discussed here uses biological validation, notably fingerprint identification, to verify voter identity. In this method, fingerprint matching is employed to confirm the user's identity. This proposed work bears by differentiating sample fingerprint patterns to show whether the fingerprints real from the match individual. The primary objective of this system is to simplify and improve the regulation of the voting mechanism. The proposed solution is designed to encourage full participation by enabling every eligible voter to take part in elections. This is achieved through an Android application that permits human being to cast their balloting digitally. Implementing online voting across both Android and web-based platforms increases the reliability and effectiveness of the election process. The system aims to offer a convenient, user-friendly, and secure method for recording and counting votes. Online voting can reduce operational costs, boost voter turnout, and facilitate better communication in the middle of voters and candidates. The core target of the implemented system is to provide a voting mechanism that authorizes singles to submit secure and confidential ballots over a network, addressing the restrictions of traditional voting methods, which are often time-consuming and vulnerable to security issues.

Key Word: Embedded system, validation circuit, Manual voting circuit, mobile based Voting , SD card readable Module; Fingerprint sensor; Arduino UNO.

I. INTRODUCTION

Elections are a fundamental component of democracy, enabling peoples to show their priorities by choosing their leaders. In traditional, paper-based voting systems, individuals must physically visit polling stations and often stand by in extended lines to go to the polls for their votes[1]. This inconvenience leads to reduced voter turnout. Moreover, the manual voting process lacks transparency, as it is vulnerable to fraud both during voting and during the manual vote-counting stage. Errors are also more likely to occur when counting votes manually, and in minute cases, single human being may attempt to vote multiple times. These issues can create confusion, disputes, and even conflicts among people.

To accommodate these challenges, there is a growing need for a fully automated, online mobile voting system. Such a proposed work not only resolves common election-related problems but also enables real-time vote counting, ensuring that results are available promptly at the end of Election Day.

Android-based voting represents an important advancement in the democratic process. It involves the use of digital platforms to cast and record votes securely. The goal of Android-enabled voting systems is to improve speed, reduce costs, and increase the accuracy of election outcomes compared to traditional paper ballots. These systems also emphasize strong data protection measures, including confidentiality, integrity, privacy, and verifiability.

Although various voting modules already available in across the world- every person with its self-strengths and restrictions—the traditional methods are becoming less practical due to lengthy preparation times, the risk of fraudulent voting, counting mistakes, extended tabulation periods, and high operational costs. Despite these drawbacks, manual voting is still widely used in many developed and developing nations, where vote manipulation may occur to influence election results.

Android-based voting is an integrated branch system field that requires collaboration among experts in engineering, imagery security, unethical practices, law, commerce, and social sciences. It is particularly challenging from a cryptographic perspective due to the need to maintain voter anonymity while preserving isolation and safeguard throughout the election process.

Privacy

To maintain the privacy the way through which the final result is available to peoples, to maintain the security no extra data about votes or votes count will leak to the public.

Robustness:

The final outcome shows all submitted and well-organized ballots machines correctly, in unethical way some of the peoples will attack to the system in forcing way to disturb the result.

Universal verifiability

When the election is over , the result will be accessed by any one.

Scope

1. Ensures a highly secure method for casting votes.
2. Prevents ballots from being lost, stolen, or inaccurately counted.
3. Offers a reliable substitute to heritage based paper ballot systems.
4. Protects the secrecy and privacy of each voter.
5. Eliminates the possibility of proxy voting or multiple voting attempts.

Objectives

1. Lowers the total expenses incurred by election authorities in managing an election.
2. Minimizes the need for overtime work.
3. Provides faster and more dependable delivery of election outcome.
4. Makes it easier and more convenient for voters to cast their ballots.

Listed below are the essential characteristics that experts in electronic voting generally agree an e-voting system must include:

Accuracy

1. No cast vote can be modified in any way.
2. No legitimate vote can be removed from the final count.
3. No invalid or unauthorized vote can be included in the final results.

Democracy

1. Only authorized or qualified voters are allowed to go to the polls.
2. It guarantees that each eligible voter can vote only a single time.

Privacy

1. Neither officials nor rest of the union can associate a ballot with the voter who submitted it.
2. No voter can demonstrate how they voted in a specific election.

Verifiability

1. Anyone can independently confirm that every vote has been accurately counted.

II. RELATED WORK

E-voting systems have been adopted in many countries worldwide. However, with the rapid advancement of technology, security challenges have also increased. Therefore, alongside the development of e-voting systems, significant research is being conducted to enhance their security. In some current e-voting systems, passwords are issued to individuals to improve security. Moreover, extensive research is focused on developing even more secure methods, one of which is the use of biometrics [3]. Biometric-based systems utilize unique human physical traits, such as fingerprints, facial features, and other characteristics, for identification and authentication purposes.

Ashwini Ashok Mandavkar proposed a system based on Mobile based face recognition employing one time

password verification for voting system 2015, Biological recognition of people voter by utilizing "face recognition" and "OTP" of every particular voter for authentication and authorization purpose.

Daniel Petcu. Dan Alexandra Stoichecu implemented a combined mobile biometric based e-voting system put in various mechanisms to spot voter between finger print scanning, verbal identification, OTP checks, phone number verification which make sure, high cryptography for voting system. This work proposes a mobile biometric-based design that deals with to these challenges during ensuring transparency, privacy, and voter anonymity, along with other essential functionalities. The system employs techniques such as Secure Sockets Layer (SSL) encryption, certificate keys, and time-limited security tokens ranging from 30 to 60 seconds. Additionally, the paper provides requirements analysis for the proposed hybrid mobile biometric e-voting system.

Thakur S. Olugbara proposed mobile voting application utilizes the dis-association potential of NFC, which also accumulates baseline voter information. This auto-coupling feature reduces the need for users to be highly familiar with the device, a common limitation in employing mobile phones for managing elections, while maintaining plainness and simplicity to use. The baseline data stored on the NFC tag serves as a local biometric reference, minimizing bandwidth usage, lowering computational demands, enabling match-on-card functionality, and ensuring that only eligible voters can cast their votes. This work identifies all the security requirements for this model and addresses potential architectural, design, and security threats and hazard aspects that may arise from implementing this approach.

Mobile technology has become extremely important in today's world. It enables the transfer and access of updated data through smartphones. These components are employing for both personal and business transactions. Moreover, the functionality of mobile phones has expanded significantly. Today, they serve a wide range of purposes, such as locating places using GPS, scanning barcodes, playing games, browsing the internet, checking weather updates, casting votes, and much more.

Among the most essential functions of mobile phones are voice calls, video calls, and the Short Messaging Service (SMS). Today, a variety of mobile phone models are accessible in the retail group, each of giving their best features and advantages. The SMS feature is particularly important, as it enables users to send messages from one device to another. Additionally, many businesses use traditional advertising methods, such as newspapers, magazines, pamphlets, and brochures, as well as radio, to encourage their goods and services.

Carlos Vegas Gonzales implemented a new Belgian E-Voting system, system was design employing a systematic LED 17 inches' touch screen system. The people will be scanned for identity identification using a barcode and biological fingerprint scanner, the people will then cast their vote using the LED and later produce the printed output to be submitted to the ballot box unit.

Maribeth Arado suggested a short messaging system voting System is about fully automated election using Short Message System (SMS). People cast individual vote through mobile phones sending SMS of their valid people those who are above threshold value and last form to the server[4]. The committee obtains the vote form through SMS and compiles the election results report.

III. IMPLEMENTATION METHOD

Hardware Description

Arduino UNO

The Arduino UNO plays a central role in many prototype Electronic Voting (E-Voting) systems, acting as the main controller that manages input/output devices, biometric authentication, acquisition, control, communication, and security logic.

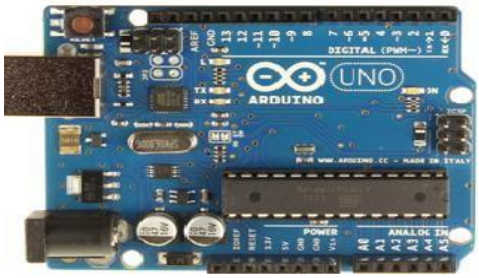


Figure 1: Arduino UNO IC

The Atmel 8-bit microcontroller has a total of 28 pins, grouped into digital and analog pins, including 14 digital and 6 analog. It requires 5-12-volt DC to operate. Among the fourteen digital pins, five can be used for PWM applications. Arduino UNO gives out 3.3 volts and 5 volts

as output. If a fingerprint sensor is used then Arduino sends commands to the sensor via Tx/Rx (UART), receives captured biometric data and verifies whether the fingerprint matches a registered template. Arduino enables the voting interface (buttons, touch keypad, RFID, etc.), detects the vote input, confirms vote selection on display and stores vote counts in internal variables or logs them to an SD card. If an SD card module is connected to the Arduino board then Arduino writes voting data to SD card, stores time stamps voter IDs, or vote counts and reads previously logged data when needed as well as provides non-volatile storage for secure data logging. Optionally, Arduino sends/receives data via: serial communication (USB) to a computer for monitoring, Wi-Fi module (NodeMCU/ESP8266) for remote tallying Bluetooth module (HC-05) for wireless data transfer as well as enables remote monitoring, result transmission, or control.

Fingerprint Sensor

Figure 2: r305 Sensor

The R305 is an optical fingerprint scanner module (sensor + processor + storage) designed for biometric authentication. It integrates image-capture, fingerprint processing, and fingerprint matching capabilities so it can enroll, store, and later verify fingerprints without needing a separate processor. It communicates via a UART (TTL serial) interface (some variants also support USB/serial adapter), making it easy to connect to microcontrollers (e.g. Arduino, Raspberry Pi) or other embedded systems. The fingerprint sensor module uses a TTL UART interface for direct communication with microcontrollers or with a PC through a MAX232 or USB-Serial adapter. Fingerprint data can be stored within the module, which supports 1:1 and 1:N identification modes. It is compatible with both 3.3 V and 5 V microcontrollers; however, interfacing with a PC serial port requires a level converter. This optical biometric reader is ideal for embedded applications such as access control systems, attendance tracking, secure storage, and vehicle locking systems. Like any optical fingerprint sensor, the quality of fingerprint acquisition depends on finger placement, cleanliness, and sensor condition — very dirty, wet, or scarred fingers may reduce reliability. Enrollment requires good-quality fingerprint images (two scans per finger). Poor-quality enrollments may lead to higher false rejections. The module's storage capacity is limited (hundreds of fingerprints), so for very large user bases you may need multiple sensors or more advanced systems. When integrating with PCs (via USB-serial), a level converter (e.g. MAX-232) may be required if using true RS232 logic rather than TTL logic.

SD card Module

An SD Card Module is a small electronic interface board that allows microcontrollers to read and write data to an SD or microSD card. It is widely used for data logging, file storage, configuration files, and recording sensor values.

Figure 3: SD card module

SD cards function exclusively at 3.3 V, requiring compatible power and I/O levels. The module is equipped with a rear-mounted MicroSD socket, which has been tested with 2 GB and 4 GB MicroSD cards. The SD card module functioned correct with the SdFAT library. An SD card module allows a microcontroller to store and retrieve data on a microSD card using the SPI communication protocol. Because SD cards operate at 3.3V logic, the module includes voltage regulation and level shifting to ensure safe operation.

Experimental Setup And Implementation

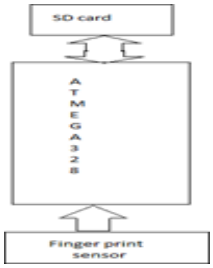


Figure 4: Authentication block diagram

The above block diagram illustrates the authentication system, which consists of an SD card, an ATmega microcontroller, and a fingerprint sensor. The SD card stores the voting database, including registered fingerprints, Aadhaar numbers, names, and mobile numbers. When a voter arrives, they scan their fingerprint [6]; if a match is found, the officer grants permission to vote. There are four candidates nominated for election as shown above in block diagram by four switches and the fifth switch will be controlling switch which will be operated by election officer. After the authentication process the officer will on the switch fifth so that voter will vote to his favorite candidate. He can vote once only if he tries again it will record first vote only (it will lock after pressing once). At a a same time, buzzer will ON. The process will be repeated and the result will be store in the SD card.

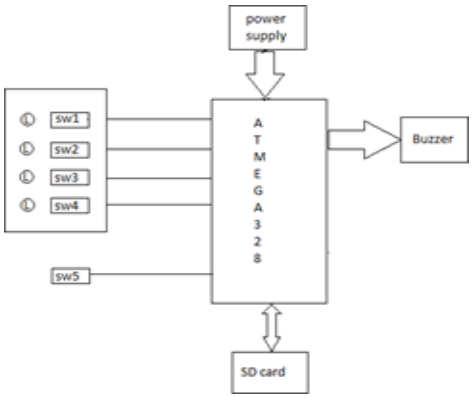


Figure 5: Proposed Block diagram of the system

Interfacing of SD card

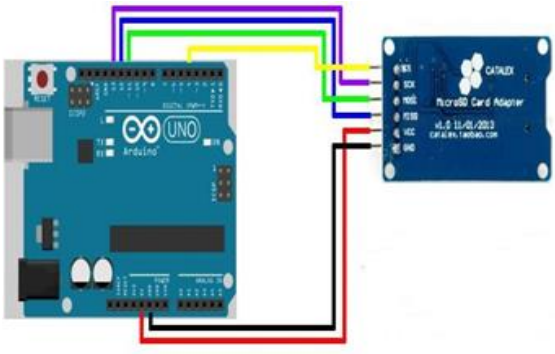
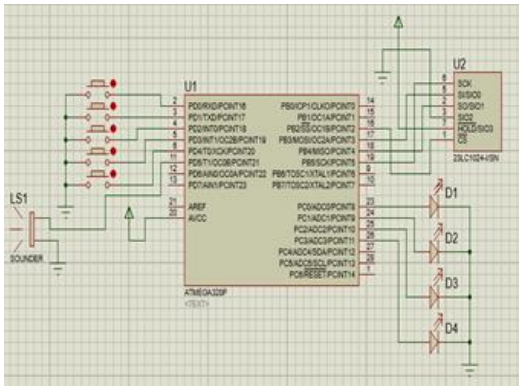
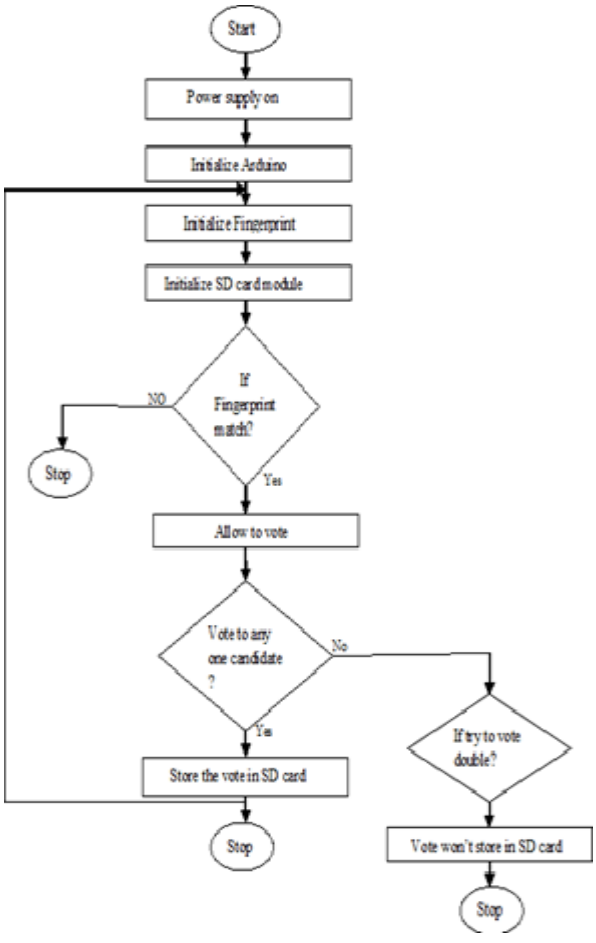


Figure 6: Interfacing of SD card with Arduino

Circuit Diagram



Flowchart



IV. CONCLUSION & FUTURE WORK

The traditional manual voting process is often slow, labor-intensive, vulnerable to electoral fraud, and expensive to run. It demands significant time and resources, turning elections into costly operations. Security is also weakened, as human limitations make it difficult to maintain the level of protection required for a reliable system. As a result, citizens are not fully empowered to exercise their democratic rights—many find it inconvenient and time-consuming to register and later wait in long lines to vote. In some regions, voters may even fear for their safety or face coercion. Furthermore, ballot counting can be manipulated, takes considerable time, and often delays the release of results.

An electronic voting system that incorporates biometrics allows individuals to vote both online and in person. It eliminates the possibility of proxy voting or casting multiple votes. By using fingerprint authentication through a mobile device, voters can support the candidate or party of their choice from any location. Registration can also be completed online via mobile devices, except for fingerprint enrollment, which still requires a visit to the electoral office.

In the future, the software could be enhanced to verify whether the scanned fingerprint is of sufficient quality for encryption, especially when low-cost scanners are used. It should also be able to detect false positives and false negatives during the real-time voting process to ensure that only authorized individuals are allowed to vote, even when mobile identity verification is used as an additional security layer. The database could be decentralized with additional layers to reduce server load and improve security, especially regarding access to government records.

Moreover, both fingerprint registration and address verification should eventually be fully automated online, eliminating the need for voters to visit electoral offices. It would also be beneficial to develop a platform-independent application that can run on various mobile devices equipped with fingerprint scanners, or that can connect to external scanners via USB. This approach would prevent users from having to purchase specialized, potentially costly devices. Finally, voters' fingerprints should be re-registered every five years to account for changes such as aging, new wrinkles, and variations in blood circulation.

REFERENCES

1. Electronic Voting (2009), Available from http://www.hwskioskprinter.com/terminology electronic voting.pdf
2. Electoral office of Jamaica (2007), Available from www.jis.gov.jm/special_sections/election_2007/index.html
3. Jain, A et al (1997) "On-Line Fingerprint Verification." IEEE Transactions on Pattern Analysis and Machine Intelligence Vol. 19, No. 4, 1997: 302-305
4. Gentles, D (2011). "Application of Biometrics for Mobile Voting", M.Sc. Computer Science Dissertation, Department of Computing, University of West Indies, Jamaica.
5. Okediran O. O., Omidiora E. O., Olabiyisi S. O., Ganiyu R. A., Alo O.O., "a framework for a multifaceted electronic voting system", International Journal of Applied Science and Technology Vol. 1 No.4; July 2011
6. Ravi. J, K. B. Raja, Venugopal K. R, "fingerprint recognition using minutia scorematching", International Journal of Engineering Science and Technology Vol.1(2), 2009
7. "adaptive filtering and neural Networks", American University of Beirut Faculty of Engineering and Architecture Department of Electrical and Computer Engineering, Vol. 1 No.4; July 2011
8. Andrew Ackerman, Professor Rafail Ostrovsky "Fingerprint Recognition", 2002
9. Ms. Kavya Ramesh Naidu, Mr. Ankush Dinesh Ingale, Ms. Pratiksha Sukhadeo Gaikwad, Mr. Hitesh Rajendra Thakare, Mr. Sujal Sunil Chavan, Prof. Yogeshk Sharma," Online Voting System",International Research Journal of Modernization in Engineering Technology and Science, Volume:05/Issue:05/May-2023.
10. Beulah Jayakumari a,Lilly Sheeba b, Maya Eapen c, Jani Anbarasi d, Vinayakumar Ravi e, A. Suganya a, Malathy Jawahar ," E-voting system using cloud-based hybrid blockchain technology", Journal of Safety Science and Resilience, Volume 5, Issue 1, March 2024, Pages 102-109
11. Yuvi Darmayunata1 , Febrizal Alfarasy Syam, Afriansyah," Implementation And Development Of E-Voting System For Election Of Student Council Chairperson Of Smp Negeri 10 Pekanbaru", Journal

of Applied Engineering and Technological Science, Vol 1(2) 2020 : 150-161

12. Y Tolegen Aidynov, Nikolaj Goranin, Dina Satybaldina and Assel Nurusheva, ”A Systematic Literature Review of Current Trends in Electronic Voting System Protection Using Modern Cryptography”,MDPI,2024.
13. Ankit Kumar , Deepanshu Kumar , Dewanshu Kumar , Naman Singh , Yogesh Sharma, ”E-Voting Website” International Journal of Novel Research and Development, Volume 9, Issue 5 May 2024.
14. Amirul Asyraf Khairul Salleh , Harlinawati Abdul Kadir, Aslimariah Ahmad , and Mohd Azahari Mohd Yusof, ”The Implementation of Electronic Voting System for Student Representation Council using reCAPTCHA”, IOP Conference Series: Materials Science and Engineering, International Colloquium on Computational & Experimental Mechanics (ICCEM 2020).