International Journal of Marketing Management

ISSN 2454 - 5007

www.ijmm.net

Email ID: editor@ijmm.net , ijmm.editor9@gmail.com

International Journal of Marketing Management

ISSN 2454-5007, www.ijmm.net
Vol. 14 Issue. 2, April 2026

AADHAR Based Voting System

[1] Dr. K. Damodar,[2] Surukunti Ashwitha Reddy,[3] Bairam Rakshith,[4] Pitla Nithinraj,[5] Nela Sandeep Kumar,

[1]Associate Professor, Department of ECE, Narsimha Reddy Engineering Collage, Maisammaguda(V), Kompally, Telangana.

[2,3,4,5] Student, Department of ECE, Narsimha Reddy Engineering Collage, Maisammaguda(V), Kompally, Telangana.

ABSTRACT

Through the integration of Aadhaar identification with voter verification, the Aadhaar-based Voting System aims to improve the legitimacy, safety, and openness of the voting process. Duplicate voter entries, impersonation, and difficulties in validating voter identification are common problems with traditional voting techniques. Each voter is individually recognized before they cast their ballot using Aadhaar's biometric and demographic data. The system's goal is to make voting more efficient and less prone to electoral fraud by automating verification and cutting down on human error. Furthermore, it lays the groundwork for potential future developments, such as internet voting, while preserving the confidentiality of personal information and the reliability of the system. Integrating Aadhaar may make current voting systems more accessible **and reliable, as this project shows.**

INTRODUCTION

Part of the democratic system is the electoral process. Regular elections are held at schools and universities to teach students about the principles of democracy and to develop good leadership skills. The biggest group of students at any given school is usually the Students' Council. Students have a platform to share their thoughts and air their complaints about the system via Students' Council. Almost every industry has been profoundly affected by technological advancements; the electoral process is no different. Technology is relied upon by people to facilitate faster, more accurate, and easier labor. The traditional paper ballot voting method is easy to use, but it lacks transparency and is prone to errors [1]. The Authenticated Voting System (AVM) was created to address the drawbacks of traditional paper ballots. There are two layers of security: Radio Frequency Identification (RFID) and biometric technology. Along with other required documentation, biometric information is captured and maintained for each student throughout the admission process. Every student is given an RFID-based identification card after the admissions process is over. In order to cast a ballot, this ID card must be shown. Voting in the election may only be done by students with current, valid identification. The student inserts their RFID card into the scanner as part of the voting procedure. By using the second level of verification, we can guarantee that the card is indeed belonging to the same student. In the second round, the voting system uses the student's biometric information, namely their fingerprint, to verify their identity. The database has a fingerprint that is compared to this one. The only person who may vote is the student if their fingerprints match. The voting equipment itself stores the votes, whereas the college database stores the essential metadata [2] [3-5]. There can be no more than three candidates for each open seat under the proposed voting procedure. If there are more than one post, then each post must have its own voting machine. When there are thousands of students to vote, the college is logically split into blocks, and the number of AVM units needed is proportional to the number of blocks. Each block has a booth-level operator (BLO) to speed up the voting process. For the college database, we will collect student fingerprints. Doing so requires access to the Internet, ideally by Wi-Fi [6]. The requirements for the pre-implementation, system-wide

International Journal of Marketing Management

ISSN 2454-5007, www.ijmm.net
Vol. 14 Issue. 2, April 2026

Problem Statement:

Voter impersonation (bogus voting), electoral fraud, and multiple votes cast by one people are serious security issues that may affect current voting systems, such as traditional ballots and conventional electronic voting machines. Delays in declaring results and public mistrust are consequences of these flaws, which damage the honesty and openness of the democratic process.

Objective

Secure and reliable voter verification utilizing Aadhaar's biometric and demographic data is the key aim of an Aadhaar-based voting system. By streamlining and improving the verification process, it hopes to do away with problems like impersonation and duplicate voting. Improved openness, less electoral fraud, and a solid foundation for future innovations like distant or online voting are all goals of the system.

System Purpose: An efficient, transparent, and highly secure electronic voting mechanism is the goal of the system. The fundamental goal is to eliminate duplicate and fraudulent votes by using the unique identification offered by the Aadhar ecosystem. This will guarantee that only genuine, verified people may vote.

Mechanism:

Using a multi-layered biometric authentication method, the system incorporates the voter's unique Aadhar identifier.

1.Identity Retrieval: The voter is required to first provide their Aadhar data, which may be done by swiping a card or scanning a QR code. Biometric Verification: The next step is for the system to take the voter's real-time biometric data (such a fingerprint) and compare it in real-time with the matching template in the Aadhar database. Third, the voter is authorized to cast their electronic vote only after authentication and a successful match. In order to stop the same person from trying to vote again, the system instantly refreshes the voting record.

Application Impact: Election security and fairness are greatly improved with the Aadhar Based Voting System. It guarantees an accurate and trustworthy election count, speeds up the tabulation process, and significantly decreases the likelihood of human error—all of which serve to fortify democracy.

BLOCKDIAGRAM:

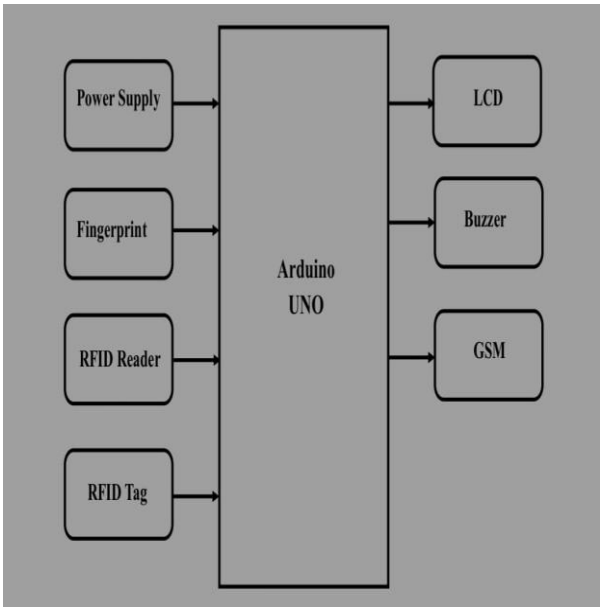
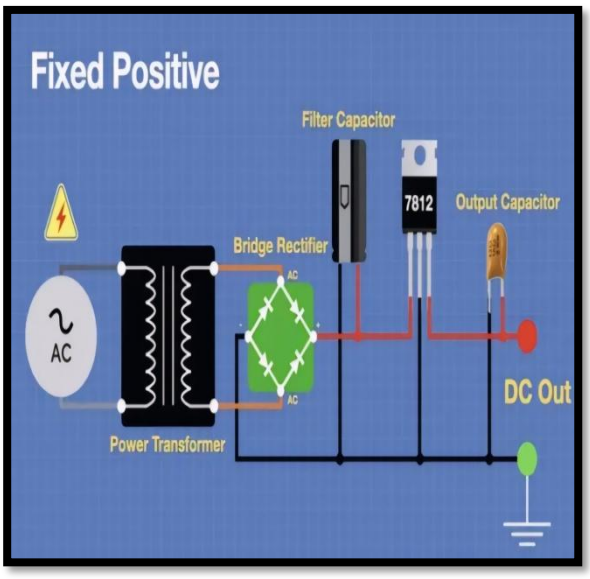


Figure 1 Block Diagram

Power Supply: After a transformer lowers the AC mains voltage, a 12V power source is ready to go. By using a bridge rectifier, the 12V AC is then transformed into DC. A voltage regulator (such as a 7812) keeps the DC voltage steady at 12V, while a filter capacitor makes the DC output more tolerable. At last, by use of suitable wiring and protective components, the regulated 12V is securely delivered to various electrical loads.



International Journal of Marketing Management

ISSN 2454-5007, www.ijmm.net
Vol. 14 Issue. 2, April 2026

Figure 2 Power supply

Finger Print: The voter's fingerprint is photographed by a fingerprint sensor, which then digitizes the picture. • The elector presses their index finger on the optical sensor. • The fingerprint's ridges and valleys are scanned by the sensor. • The picture is transformed into a digital template using the inbuilt DSP. • The Arduino checks it against files that have templates associated with Aadhar information. The voter's identity is confirmed upon matching.

Figure 3 Finger Print

RFID Reader

When an RFID tag gets close to a reader, the reader powers the tag using electromagnetic waves. • The RFID tag has a unique identifier that the reader can read. • The serial transmission allows the Arduino to receive this ID. • The Aadhar-linked identity of the voter is represented by this ID. RFID adds another level of security to the voting process by verifying the voter's identification.

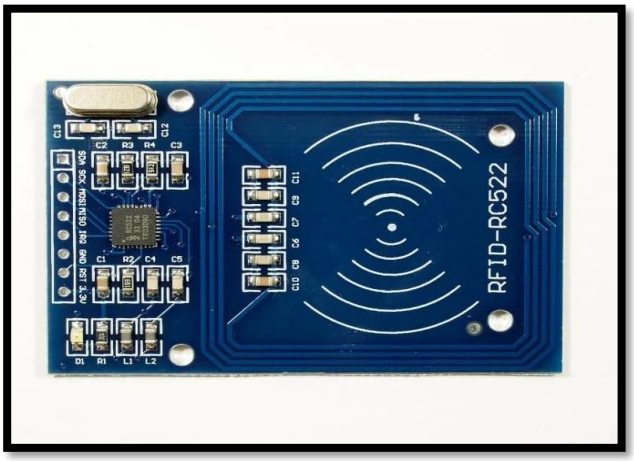


Figure 4 RFID Reader

RFID Tag

Embedded in an RFID tag is a microchip that may be uniquely identified. For optimal viewing: • It draws strength from the field of the reader. • The reader receives the ID that was saved by it. Before the fingerprint module can be enabled, this one-of-a-kind ID is used for voter verification.

Figure 5 RFID Tag

16x2 LCD

The molecules of liquid crystal sandwiched between two transparent electrodes allow an LCD to regulate the light that passes through them. The crystals twist and untwist in response to an electric signal, allowing or blocking light, respectively. Graphics or characters are rendered on the screen as a result of this. The screen may be seen more clearly with the aid of a backlight or natural light.

International Journal of Marketing Management

ISSN 2454-5007, www.ijmm.net
Vol. 14 Issue. 2, April 2026

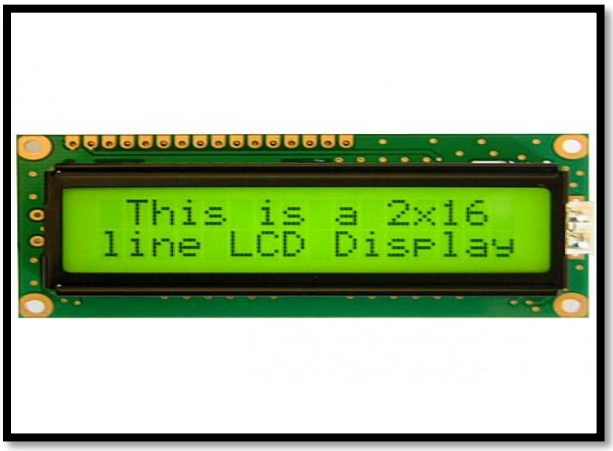


Figure 6 16x2 LCD

Buzzer

By use of a vibrating diaphragm, a buzzer is able to transform electrical energy into audible sound. The internal electromagnet or piezo element vibrates quickly in response to applied voltage. Waves of audible sound are produced by these vibrations. Whether it's a tone, alarm, or beep depends on the vibration frequency.

Figure 7 Buzzer

GSM Module

The ability to communicate over a mobile network is made possible by a GSM module. Through UART, the Arduino transmits AT instructions. • "Vote Recorded Successfully" is one example of an SMS notification sent using GSM. • If linked to a web-based database, it may also update distant servers.

Figure 8 GSM Module

Arduino Uno

An external adapter (7-12V) or a USB cable (5V) may power an Arduino. Users program the ATmega328P microcontroller by writing code in the Arduino IDE and then uploading it. Processing: Sensor inputs are read by the microcontroller using digital and analog pins. Controlling Output: Actuators like motors, relays, or LEDs get signals from the software. It has connectors for serial, I2C, and SPI communication, so it can talk to other devices.

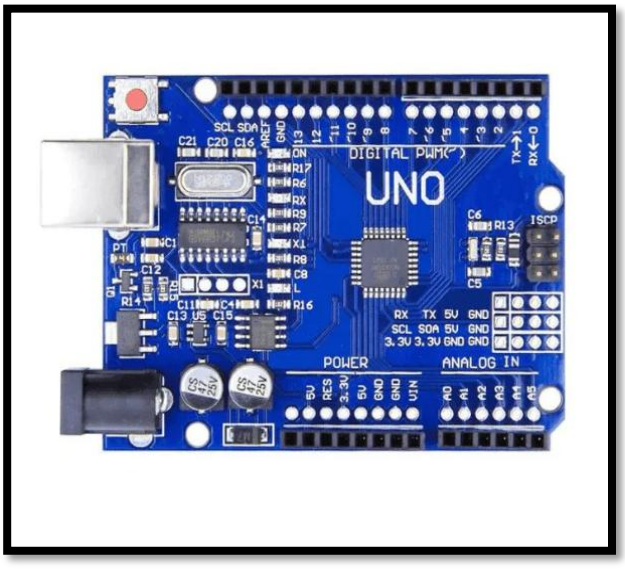


Figure 9 Arduino UNO

Interface Design

Figure 3 shows the layout of the AVM system's user interface. "Student" and "Elections Commission" are

International Journal of Marketing Management

ISSN 2454-5007, www.ijmm.net
Vol. 14 Issue. 2, April 2026

the only primary sections. The authority to form a BLO and enroll candidates for the election lies with the EC. It consists of two primary modules, EC and BLO. EC comprises two sub-modules, one for managing students and another for managing BLOs. The records of BLOs may be added to, deleted from, or updated by EC. The EC sub-module under the manage students module allows users to see student information as well as election results. Since the information about students is taken from the college database, EC does not have the authority to change student records. Two sub-modules make up the BLOs module: managing candidates and council positions. Using the add post sub-module, BLO posts all election-related information. Using the add post module, BLO publishes various dates, such as the final date for submitting nominations and withdrawals, among others. It is also within BLO's rights to remove a post. Nominations may be submitted and withdrawn using the manage candidate sub-module.

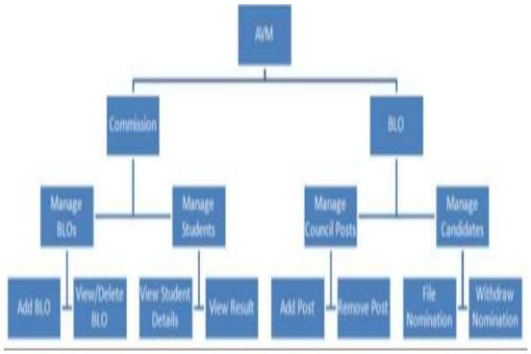


Figure 10. Structure chart of AVM system

In terms of interfaces, the AVM system offers two distinct kinds. Two interfaces are available: one on the computer that is connected to the AVM unit, and the other on the AVM unit itself. The system's graphical user interface (GUI) is accessible exclusively to administrators, EC members, and BLOs. The computer's graphical user interface (GUI) allows the administrator to add BLOs and applicants, and it also allows BLOs to alter their passwords. The GUI is not given to the students. After they've finished both authentication procedures, they need to push a voting button on the AVM device. The AVM system's main screen is shown in Figure-n. The administrator, who is also the head of EC, uses it to construct BLOs. After the BLOs are formed, each one has the ability to change their own password. The specifics of all BLOs may be seen using Fig-n, the GUI [16,19].

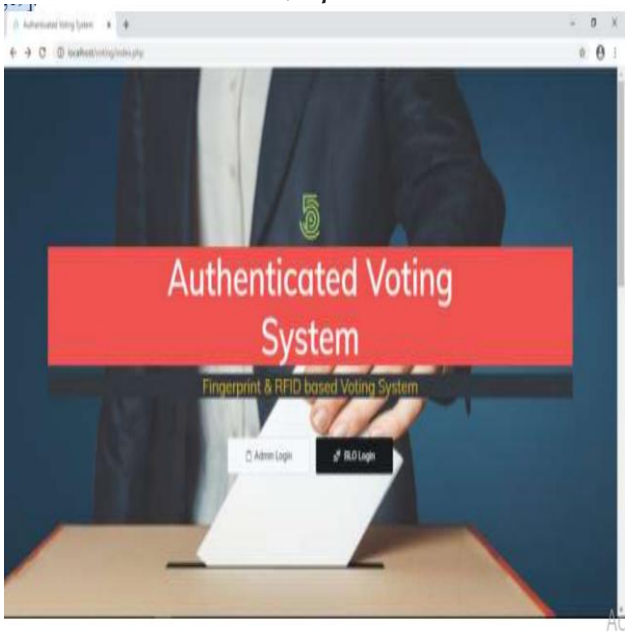


Figure 11. Home Screen

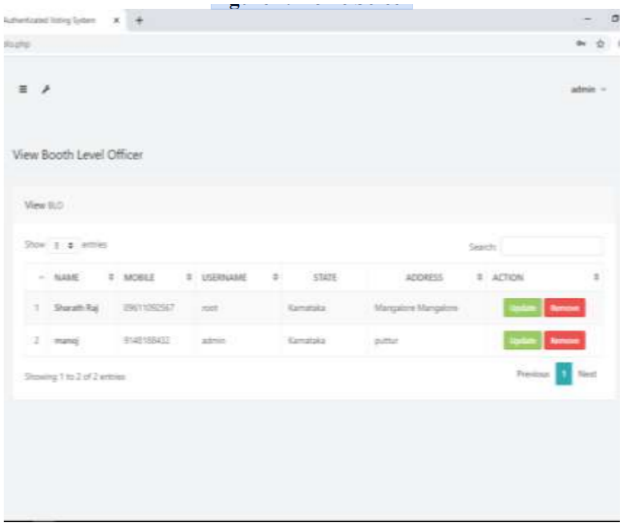


Figure 12. View BLO

The user interface that BLOs utilize to add individual candidates is seen in Figure 5. The AVM's LCD will show the appropriate message when the system is prepared to conduct the voting procedures. Every student is required to swipe their own RFID card. After this verification process is complete, pupils are instructed to retain their fingerprints on the reader. Next, the data collected from the input is compared to the student records that were retrieved from the college database. A student's right to vote is forfeited in the event of a dispute. The student will be able to

International Journal of Marketing Management

ISSN 2454-5007, www.ijmm.net
Vol. 14 Issue. 2, April 2026

cast a ballot after passing the second round of validation. The results may be seen by the EC after the election procedure is finished [20].

7. Conclusion & Future Work

An intelligent and safe authenticated voting system for college elections was described in this research. It is built on Arduino flat-form IoT technology. A two-layer security technique is used to guarantee voter security and maintain the method's integrity. We take it as a given that this approach helps schools hold transparent and fair elections for the Student Council. The system is not flawless, but it does achieve the desired results in terms of efficiency and performance. We have discovered a few system restrictions. Since there are only three voting switches, the system can only back three candidates simultaneously. We can take care of this in our next projects. Plus, the system only lets you vote for one position at a time. The system may be designed to accommodate elections for any number of offices simultaneously. Furthermore, the memory capacity of the Arduino Mega board is somewhat low. Our next project will make use of an AVM board based on the Raspberry Pi. This project's integrated devices are upgradable, data is saved in the cloud, and automated voting may expedite the voting process. More development is required to make the system flexible and versatile as it is still in its early stages. It is still in beta, but in future work we will deliver a device that is improved, reliable, error-free, and scalable.

References

1.Arduino Documentation. (2024). Arduino UNO Technical Specifications. Retrieved from https://www.arduino.cc/en/Main/ArduinoBoardUno

2.Adafruit Industries. (2023). Optical Fingerprint Sensor – Product Guide and Technical Details. Retrieved from https://learn.adafruit.com/

3.RFID Journal. (2024). Introduction to RFID Technology and Applications. Retrieved from https://www.rfidjournal.com/

4.SIMCOM Wireless Solutions. (2023). SIM800 GSM Module – AT Command Manual and Hardware Design Guide. Retrieved from https://www.simcom.com

5.Microchip Technology Inc. (2024). ATmega328P 8-bit AVR Microcontroller – Datasheet. Retrieved from https://www.microchip.com

6.UIDAI – Unique Identification Authority of India. (2024). Aadhaar Authentication Overview and Security Features. Retrieved from https://uidai.gov.in

[7] Lavanya, S, 2011, Trusted secure electronic voting machine. *Proceedings of the International Conference on Nanoscience, Engineering and Technology, ICONSET 2011*, 505–507.

[8] Matharu, G. S., Mishra, A., & Chhikara, P, 2015, CIEVS: A cloud-based framework to modernize the Indian election voting system. *2014 IEEE International Conference on Computational Intelligence and Computing Research, IEEE ICCIC 2014*, 1-6

[9] Elhoseny, M., Ramírez-González, G., Abu-Elnasr, O. M., Shawkat, S. A., Arunkumar, N., & Farouk, A, 2018, Secure Medical Data Transmission Model for IoT-Based Healthcare Systems. *IEEE Access*, *6*(c), 20596–20608.

[10] Kiruthika Priya, V., Vimaladevi, V., Pandimeenal, B., & Dhivya, T, 2018, Arduino based smart electronic voting machine. *Proceedings - International Conference on Trends in Electronics and Informatics, ICEI 2017*, *2018-Janua*, 641–644.

[11] Kadbe, A., Balgujar, S., & Chimote, S, 2013, Biometric and RFID Secured Centralised Voting System. *(IJCSIT) International Journal of Computer Science and Information Technologies*, *4*(2), 255–258.

[12] Reddy, B. M. M., & Srihari, D, 2015, RFID Based Biometric Voting Machine Linked To Aadhaar For Safe And Secure Voting. *International Journal of Science, Engineering and Technology Research (IJSETR)*. *4*(4), 995–1001

[13] Mansingh, P. M. B., Titus, T. J., & Devi, V. S. S, 2020, A Secured Biometric Voting System Using RFID Linked with the Aadhar Database. *2020 6th International Conference on Advanced Computing and Communication Systems (ICACCS), Coimbatore, India, 2020.* 1116–1119.

[14] Prabhakaran, G., Dharshini, T., Janani, N., Deepan, R., & Elavarasan, P. Electronic voting machine based on fingerprint and iris authentication. *International Journal of Intellectual Advancements and Research in Engineering Computations.* 6 (1). 135-139

ISSN 2454-5007, www.ijmm.net
Vol. 14 Issue. 2, April 2026

[15] Naveenraj, M., Arun, A. C., Gowtham, A., Laleth, T. R., & Naveen Kumar, G, 2019, Biometric based electronic voting system using aadhar. *International Journal of Innovative Technology and Exploring Engineering*, *8*(6), 196–199.