JSRT JOURNAL

PAGES: 127-142
25/09/25

JOURNAL OF SCIENTIFIC RESEARCH AND TECHNOLOGY VOLUME-3 ISSUE-9 SEPTEMBER

IOT-Based Real-Time Security And Malfunction Detection In Electronic Voting Machines

Abhay L Holkar [1], Pooja R Marab [2]

[1]*Student, Dept. of Electronics and Communication Engineering, VTUCPGS, Kalaburagi, India.*

[2]*Assistant Professor, Dept. of Electronics and Communication Engineering, VTUCPGS, Kalaburagi, India.*

ABSTRACT

This project presents the development of a biometric-enabled smart voting and monitoring system designed to provide a secure, reliable, and user-friendly election process. The system is controlled by an Arduino UNO, interfaced with an RFID reader, R305 fingerprint sensor, user keypad, and ESP32-CAM module, offering multiple layers of authentication and real-time monitoring. A DC power supply ensures uninterrupted operation. Unlike traditional ballot papers or standard EVMs, the system allows voters to cast their votes via a touch panel interface with biometric verification, effectively preventing proxy voting and unauthorized access. Biometric information is cross-checked with the Aadhaar database, enabling eligible voters to vote from their current location without needing to travel to their native constituency. The system also includes robust data security measures, and election results can be published immediately. By combining IoT, biometrics, and smart authentication, this approach offers a time-efficient, cost-effective, and highly secure alternative to conventional voting methods, enhancing voter participation and reinforcing the democratic process.

Keywords: IOT, Security, E-voting

INTRODUCTION

Democracy has long been the foundation for giving people the power to elect their representatives, a system that traces back to ancient times. As technology has progressed, election practices have undergone major changes. For decades, countries around the world have sought to make voting more accessible, dependable, and transparent. In India, continuous efforts have been made to enhance the election process to achieve greater accuracy, flexibility, and efficiency. Originally, voting was carried out through paper ballots, requiring polling centers to be established in villages, usually within schools, colleges, or government buildings. This approach demanded extensive arrangements, such as deploying security forces and training officials, which made the process lengthy and complex. In recent years, the Indian government has upgraded the system by introducing Electronic Voting Machines (EVMs) for casting and recording votes. However, even with this advancement, strong security protocols remain essential to ensure fairness and smooth operation.

Fig1.1: ELECTRONIC VOTING MACHINE

OBJECTIVES

The key objectives of the system are

- **Time and Cost Efficiency:** Reduce the time and expenses associated with the voting process for both voters and election authorities.
- **Prevention of Proxy Voting:** Ensure voter authenticity through Aadhaar-based biometric verification.
- **Remote Voting:** Allow citizens to cast their votes from their current location without traveling to their native constituency.
- **Reduced Staff Workload:** Minimize the effort and resources required by election personnel.
- **Ease and Flexibility:** Simplify the voting process to make it accessible and user-friendly for all participants.
- **Health Safety:** Limit health risks during pandemics by ensuring the safe use of biometric devices.

LITERATURE SURVEY

Jambhulakar, Chakole, and Pradhi.,[1]

A secure web-based voting framework was developed using multiple encryption methods to safeguard votes during transmission from polling stations to the central voting server. The system incorporates cryptographic signatures to protect against denial-of-service (DoS) attacks. It employs a dual-key encryption scheme, where a public key encrypts the vote on the voter's side, and a private key decrypts it on the server side. Additionally, a digital signature mechanism ensures that the transmitted votes remain unaltered, enhancing both the confidentiality and authenticity of the election process.

Pashine, Ninave, and Kelapure.,[2]

Proposed an Android-based e-voting application designed to simplify the voting process and provide secure authentication. The system is divided into three panels: the Admin Panel (used by election authorities to manage candidate and voter records), the Candidate Panel (for candidates to communicate with voters and election officials), and the Voter Panel (for registered citizens aged 18 and above to cast their votes remotely). The approach eliminates the need for physical polling stations, thereby reducing time and resource requirements.

Khasawneh.,[3]

A biometric-enabled electronic voting system was proposed that verifies identities on both the server and user sides. Once a vote is cast, the system generates a physical copy containing a unique number and barcode for verification purposes. This copy is securely stored and used to authenticate the votes before they are recorded in the final database. Random checks of these stored copies help ensure the accuracy and reliability of the voting process.

SHRIDHARAN.,[4]

Implemented three models: the authentication model, the distributed database model, and the central server model. Voters use smart cards and biometrics for verification before being allowed to cast their vote. The system stores voter credentials in a secure database and cross-verifies them before vote counting. Mechanisms are also in place to prevent duplicate voting and ensure traceability.

E - VOTING SYSTEM

In this e-voting system, all eligible citizens of a constituency who are 18 years or older, regardless of gender, can cast their votes conveniently and securely. Voters can participate from their native constituency without facing logistical difficulties. E-voting platforms are secure digital systems that eliminate the need for paper ballots and reduce the workforce required for manual vote security. These systems ensure the integrity of the election by preventing multiple voting attempts by the same individual.

Key advantages of e-voting systems include -

- Trusted and secure voting software.
- Preservation of vote integrity and authenticity.
- Easy access and management for election administrators.
- Mechanisms to ensure each vote is unique.
- Built-in analytics and reporting tools.
- Prevention of double voting and proxy voting.
- Difficult to revert to older, manual voting methods such as in-person paper or email-based voting.
- Integration with Aadhaar-based vote management systems for smooth and authenticated voting.

- Assistance from election management experts to design, set up, and oversee successful elections.
- Efficient management of complex voting procedures.
- Increased voter turnout through simplified and accessible voting processes.

Overall, e-voting systems provide a reliable, efficient, and transparent alternative to traditional voting methods, while also supporting enhanced voter management and monitoring.

4.1 DESIGN AND TECHNOLOGY

An Electronic Voting Machine (EVM) consists of two main components: the control unit and the balloting unit, which are connected by a five-meter cable. The balloting unit allows voters to cast their vote using labeled buttons, while the control unit manages the voting process, stores vote counts, and displays results on seven-segment LED screens. The software in the control unit is permanently embedded in silicon during manufacturing, preventing any modifications, even by the manufacturer.

During elections, the control unit is operated by the polling officer, while the voter uses the balloting unit privately. The officer verifies the voter's identity, enabling the balloting unit to accept a vote. Once a vote is cast, it is displayed for the voter's confirmation and stored in the unit's memory. A local command from the control unit finalizes the vote and disables the balloting unit to prevent multiple votes. This procedure is repeated for each voter presenting a valid ID.

EVMs are powered by a 6-volt alkaline battery, allowing them to function reliably in areas with limited or inconsistent electricity. The control and balloting units depend on each other to operate. After polling ends, the units are separated and securely stored in locked premises.

Both units are manufactured with strict sealing protocols, making the hardware fixed and tamper-proof. They do not include wireless or internet components. The balloting unit contains a real-time internal clock and logs every input event with a timestamp when connected to the battery. The use of battery power prevents tampering through external electricity sources, ensuring safe and reliable operation of the EVM.

4.2 BIOMETRICS

The Indian government has implemented Aadhaar as a unique identification system (UID) across almost all sectors in the country. Once a citizen's fingerprint is recorded in the Aadhaar database, it becomes immutable. Leveraging this concept, an Aadhaar-based voting system has been designed to prevent proxy voting and minimize manual clerical work by digitizing the voting process.

This system allows citizens to cast and store their votes securely without needing to travel to their native constituency. The primary goal is to eliminate proxy voting while enabling those residing outside their constituency to vote from nearby polling booths.

The system integrates IoT devices to automate the voting process. The Internet of Things (IoT) is a network of interconnected computing devices, mechanical and digital machines, each with unique identifiers (UIDs), capable of exchanging data without direct human-to-human or human-to-computer interaction.

After voting concludes, all votes are stored in a central server database. The application can record votes according to the citizen's native constituency, and election results can be generated quickly with just a few clicks. Votes are organized in the database by constituency and ward, allowing rapid calculation of statistics and vote ratios. This automated approach ensures timely and accurate declaration of election results.

4.3 DEMOGRAPHIC INFORMATION

The Aadhaar enrollment process collects several key pieces of information, including Name, Date of Birth (or verified Age), Gender, Address, Mobile Number (optional), and Email ID (optional). Depending on the type of enrollment

- Introducer-based enrollment: Includes the introducer's name and Aadhaar number.
- Head-of-family-based enrollment: Includes the name of the head of the family, the relationship, and the head of family's Aadhaar number.
- Child enrollment: Requires the enrollment ID or Aadhaar number of one parent, along with a Proof of Relationship (POR) document.

Launched by the Government of India, the Aadhaar project is one of the world's largest national identity initiatives. It collects both biometric and demographic data of residents and stores it in a centralized database. To date, over 1.036 billion people have been enrolled, with the government investing approximately USD 890 million in the project.

Aadhaar provides a unique identification number (UID) that is consistent across all sectors. Once a person is enrolled, their Aadhaar ID remains permanent, and the risk of identity fraud or proxy use is extremely low, with biometric verification reducing the likelihood of impersonation to less than 1%.

HARDWARE AND SOFTWARE COMPONENTS

HARDWARE COMPONENTS

ARDUINO MEGA 2560 MICROCONTROLLER

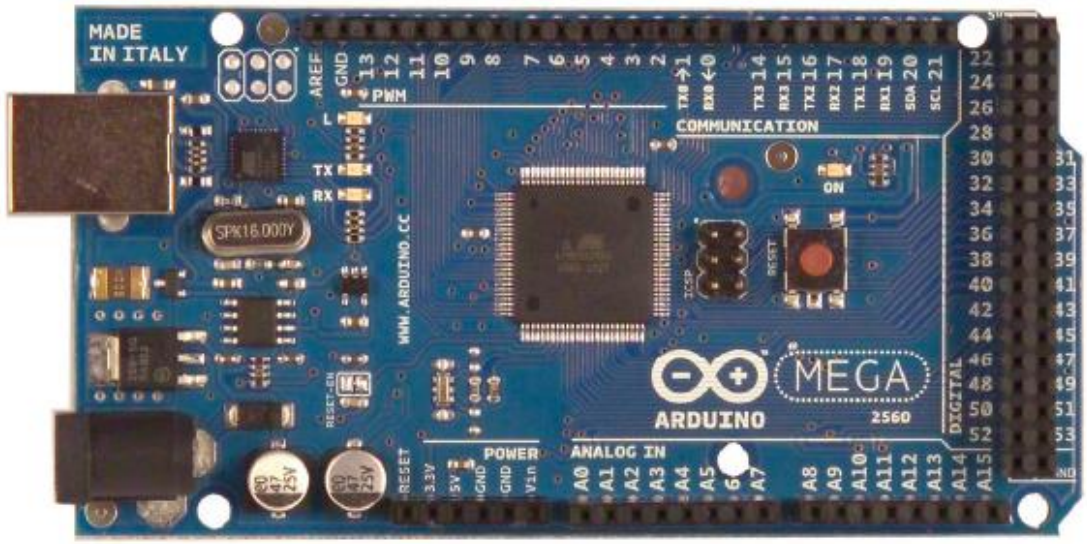
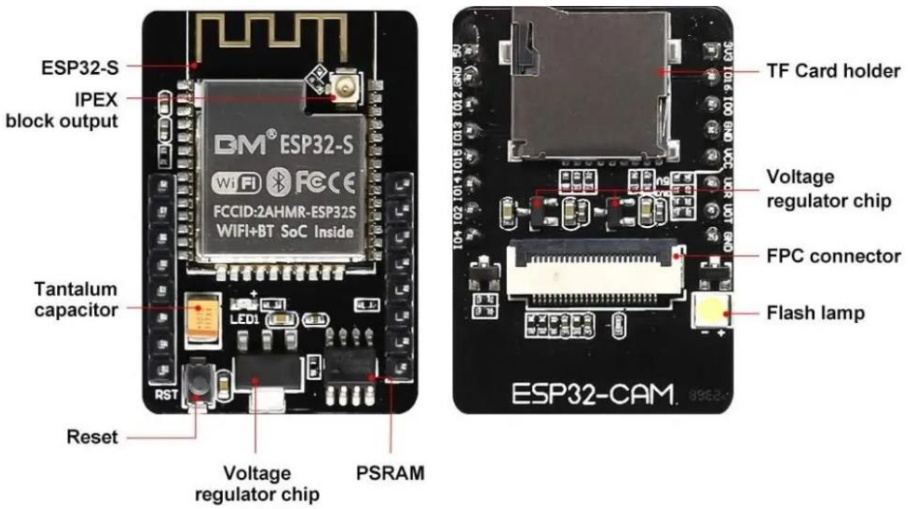


Fig 5.1.1 Arduino mega 2560 microcontroller

5.1.2 ESP32-CAMERA AI-THINKER BOARD

The world has increasingly embraced the Internet of Things (IoT), capturing the interest of hobbyists, innovators, and professionals alike. From developing smart prototypes to creating market-ready products, IoT technology has become central to modern innovation. Among the various modules available, the ESP32 series chips have gained popularity due to their intelligence, versatility, and suitability for IoT applications.



ESP32-CAM AI-Thinker module consists of different parts. These areas described below:

ESP32-S Chip: The module is a main chip contains two high-performance 32-bit LX6 CPUs with a 7-stage pipeline architecture and used for all the processing and functioning.
IPEX block output: The printed IPEX connects GSM antennas to transmit signals.

Tantalum capacitor: The tantalum capacitor is majorly used on small size modules. They are durable and provide

ESP32-CAM AI-THINKER PINOUT

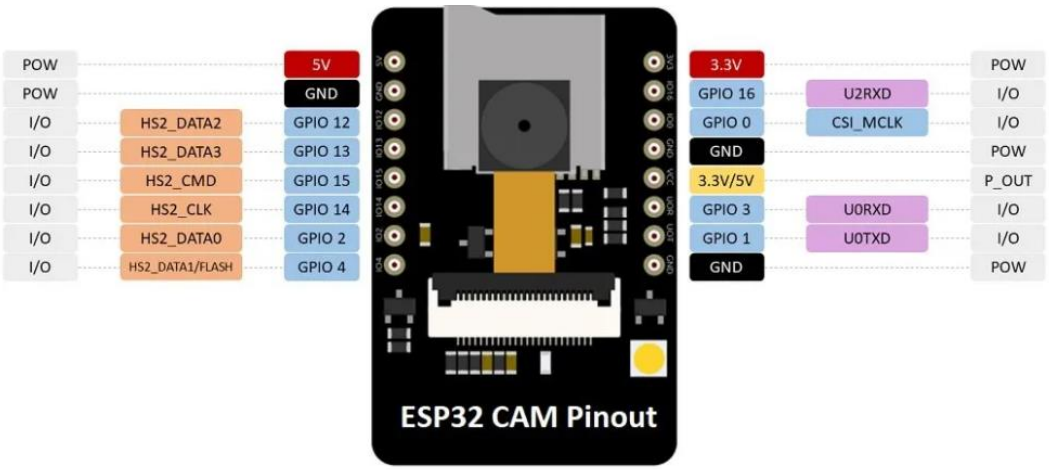


Fig 5.1.2(1) ESP32 CAM Pinout

5.1.3 R303A SERIES FINGERPRINT IDENTIFICATION MODULE

A FINGERPR

In the 21st century, the adoption of biometric-based systems has grown rapidly due to significant advancements in technology, decreasing costs, ease of use, and their versatile applications in everyday life. Biometrics has emerged as a modern standard for security systems, providing a more reliable and efficient approach compared to traditional methods.

Biometric technology is widely used to secure ATMs, smartphones, laptops, offices, vehicles, and other security-sensitive applications. It has transformed security by shifting the focus from what you know (e.g., passwords) or what you have (e.g., keys) to what you are-including fingerprints, retinal patterns, and voice recognition—offering a higher level of protection.

Fig 5.1.3(1) FINGERPRINT OVERVIEW

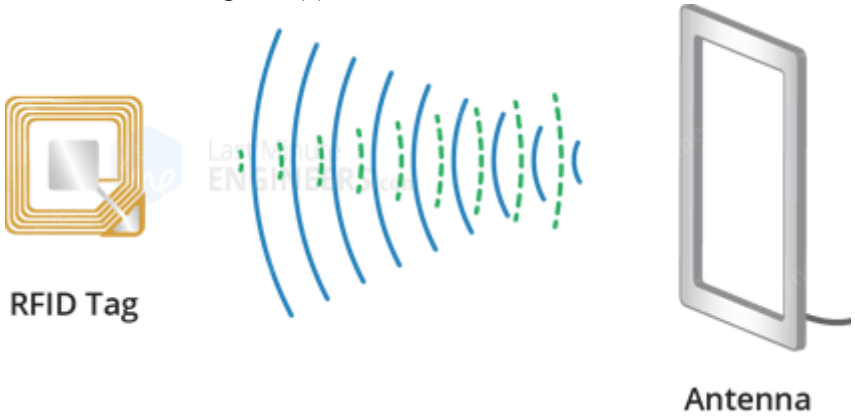
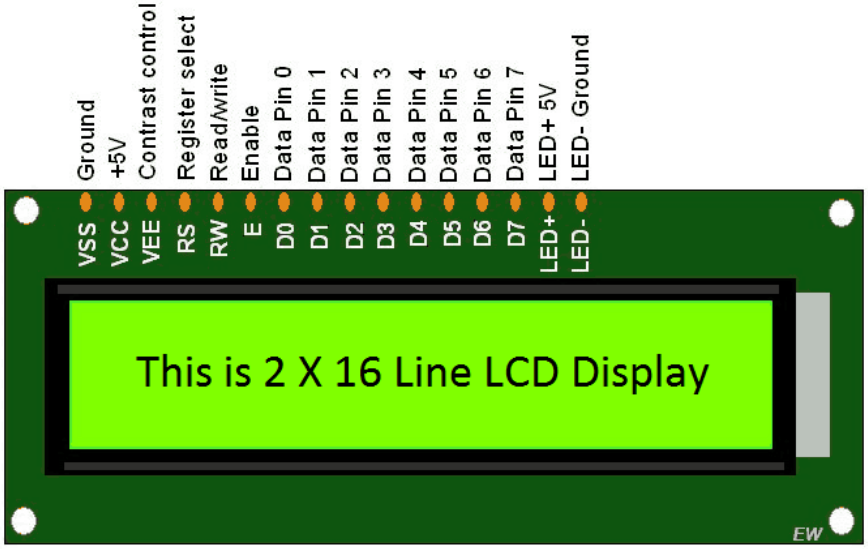


Fig 5.1.4 RC522 RFID MODULE

5.1.5 Liquid Crystal Display (LCD)

A Liquid Crystal Display (LCD) uses a special material that exhibits properties of both liquids and crystals. Within a specific temperature range, the molecules of this material can move freely like a liquid while still maintaining an ordered arrangement similar to that of a crystal. This unique property allows LCDs to control light and display images effectively in electronic devices.



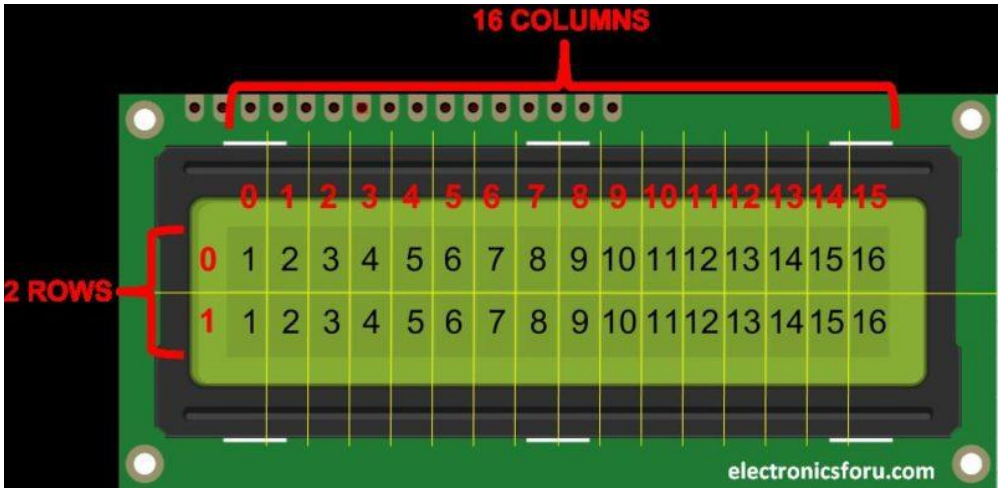


Fig 5.1.5 LCD DISPLAY

5.1.7 KEYPAD

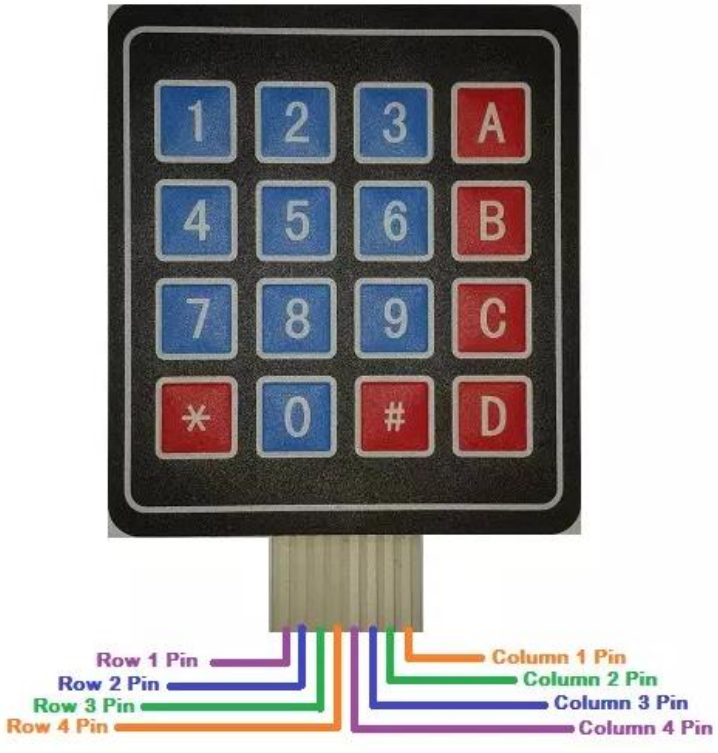


Fig 5.1.7 KEYPAD

A keypad is organized in rows and columns. A 4x4 keypad consists of 4 rows and 4 columns, with a membrane switch located beneath each key.

5.2 SOFTWARE REQUIREMENTS

- Arduino IDE

The Arduino IDE (Integrated Development Environment) is a specialized software tool designed to program and control Arduino boards as well as other compatible microcontrollers. It allows users to write code in a simplified version of C/C++, verify it through compilation, and then upload it directly to the hardware. The software features an easy-to-use editor, debugging options, and a serial monitor that helps in testing and communication with the device in real time. With its large collection of pre-built libraries and example codes, the Arduino IDE reduces the complexity of embedded programming, making it suitable for learners and experienced

developers alike. Its flexibility to support different boards such as ESP32 and ESP8266 makes it a widely adopted platform for projects in automation, robotics, and the Internet of Things (IoT).

Fig 5.2 ARDUINO IDE SOFTWARE

ESP32-CAM: Web Server Setup – For video streaming.
GSM: AT Commands For sending SMS messages.
LIBRARIES: Fingerprint library, RFID library, GSM library, ESP32 camera libraries.

CHAPTER 6

PROPOSED SYSTEM

6.1 BLOCK DIAGRAM

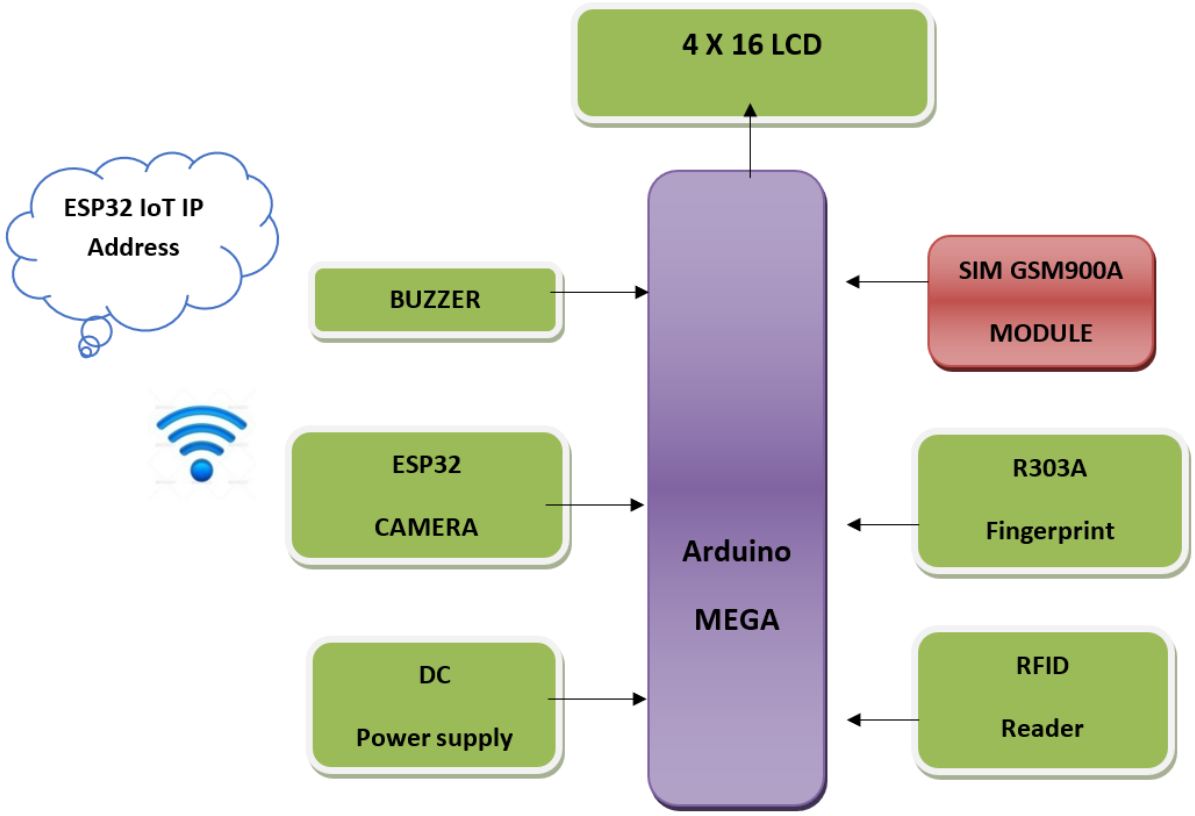


Fig 6.1 BLOCK DIAGRAM

CHAPTER 7

RESULTS AND DISCUSSION

7.1 CIRCUIT DIAGRAM

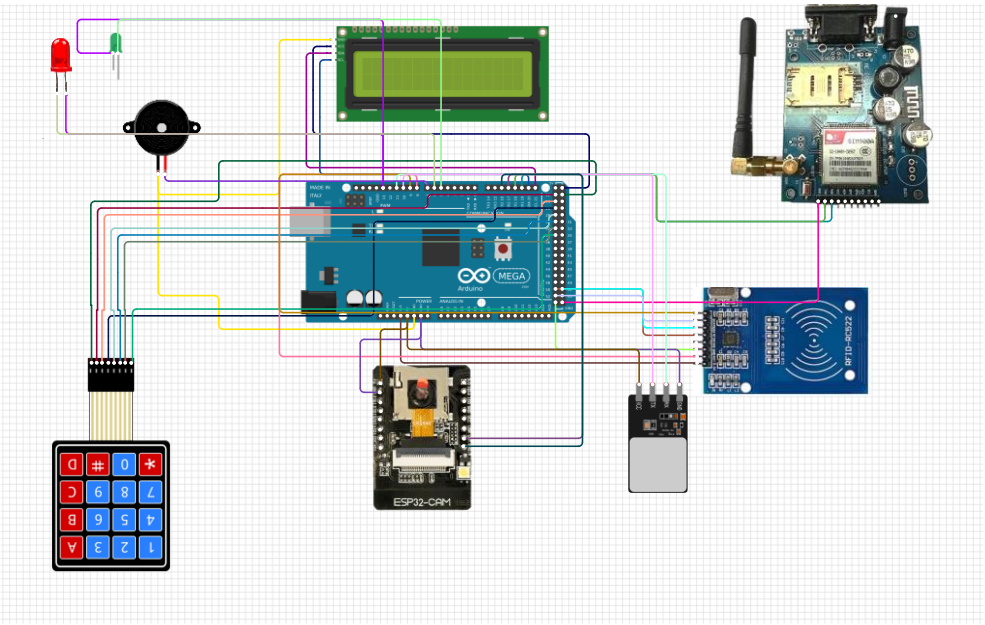


Fig 7.1 CIRCUIT DIAGRAM

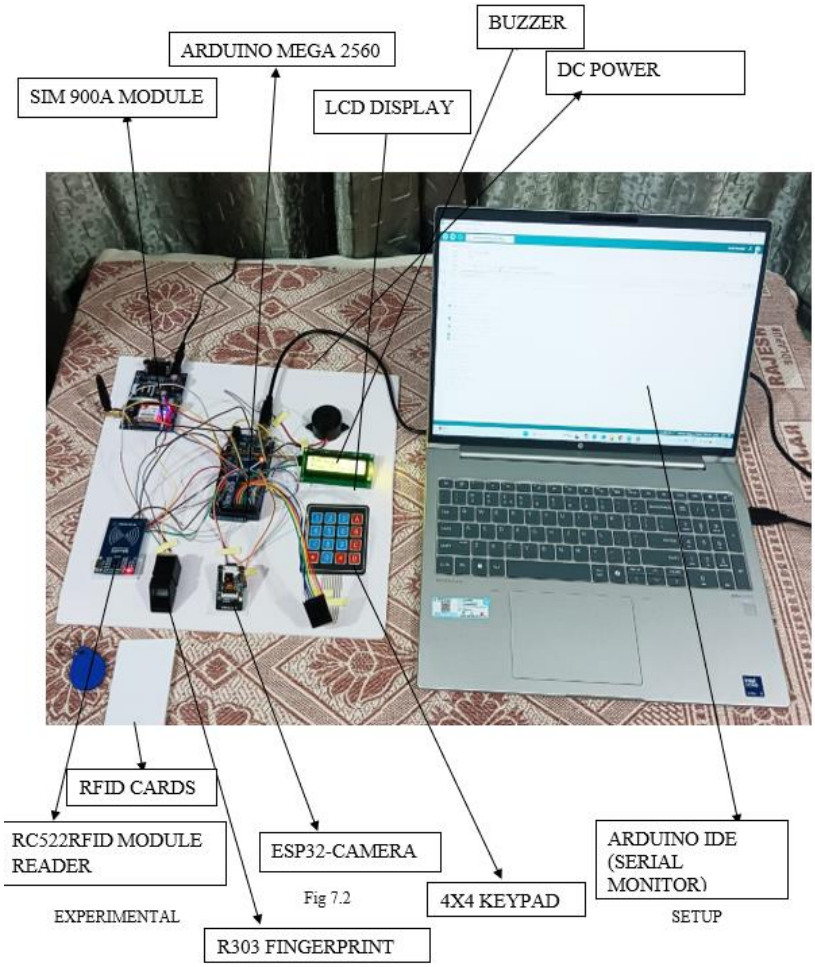


Fig 7.2

7.2 EXPERIMENTAL SETUP

7.3 RESULTS

When the EVM is powered on, it enters the pre-voting stage. Pressing the 'M' key brings up the menu on the LCD screen, as illustrated in the figure.

Fig 7.2.1 EVM READY

During the pre-voting phase, the administrator can add multiple voters by entering the admin password, as demonstrated in the figure.

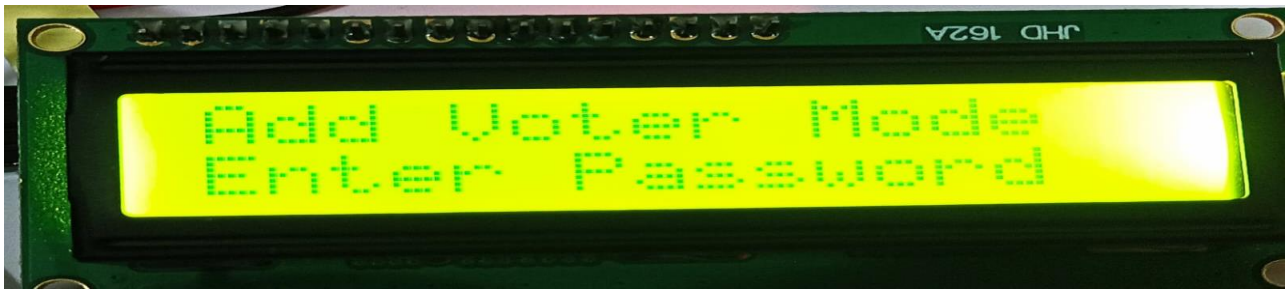


Fig 7.2.2 ADD VOTER MODE

The administrator inputs the voter's name for identification purposes when scanning the RFID card, as shown in the figure.

Fig 7.2.3 ENTER NAME MODE

The RFID card is scanned by holding it close to the reader. This step involves pre-registering the RFID cards by the administrator, as illustrated in the figure.

Fig 7.2.4 SCAN RFID CARD

Entering the fingerprint serial number for voters in serial as shown in the below figure

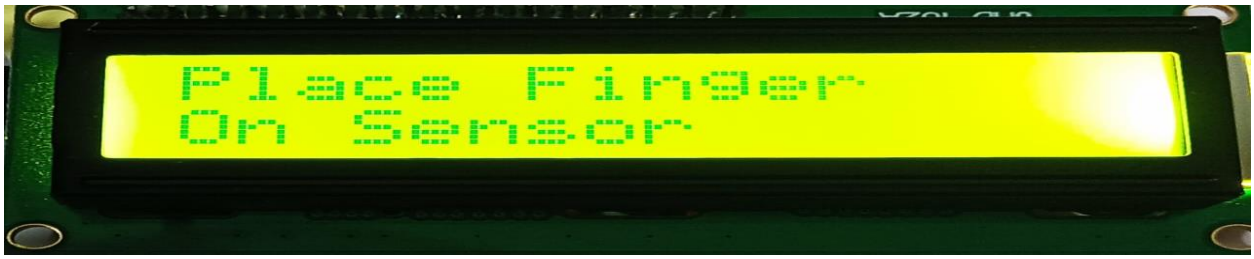


Fig 7.2.5 PLACE FINGER ON SENSOR

Fig 7.2.6 ENTER FD ID

Fig 7.2.7 PLACE FINGER

Capturing Live photo for verification process please Look at the camera as shown in the below figure

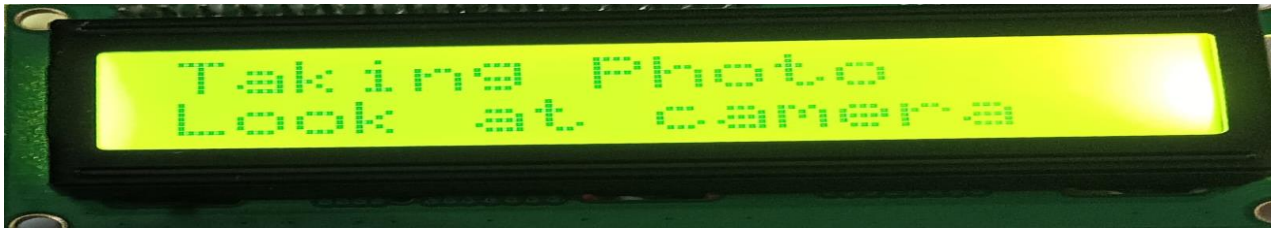


Fig 7.2.8 TAKING PHOTO

Voter Added successfully with RFID card, Fingerprint, Live Photo Captured as shown in the below figure

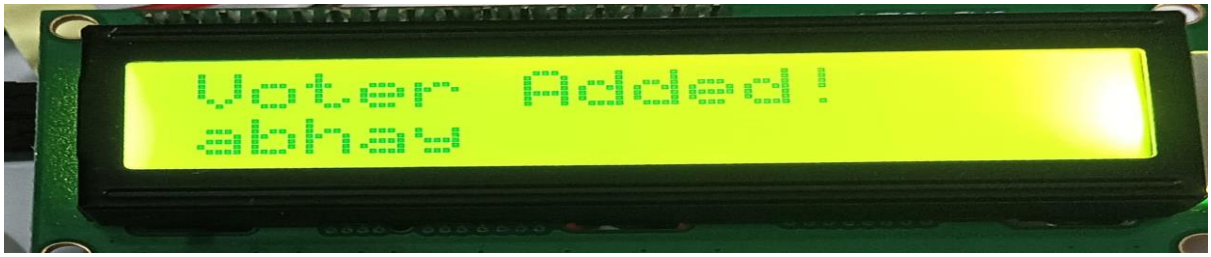


Fig 7.2.9 VOTER ADDED

Once powered on, the EVM is prepared for the voting process. Pressing the 'M' key displays the menu on the LCD screen, as shown in the figure.

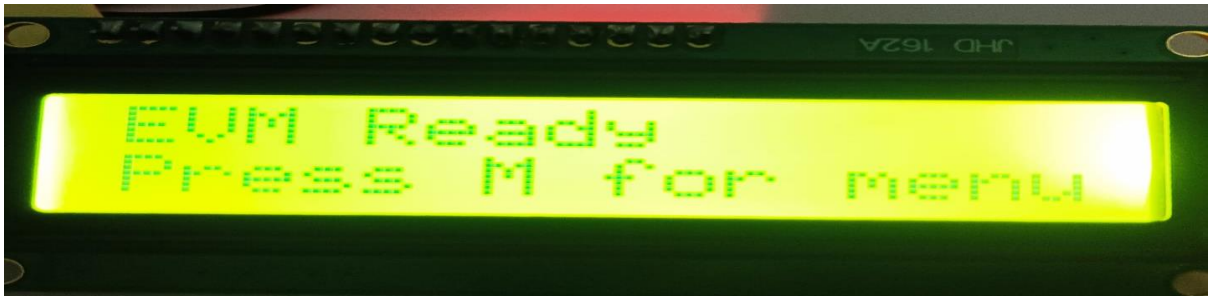


Fig 7.2.10 EVM READY FOR VOTING

The voting process begins by scanning the RFID card. Hold the card close to the reader to initiate voting, as illustrated in the figure.

Fig 7.211 SCAN RFID TO VOTE

RFID scanned successfully Please Place finger on Sensor for the Authentication process as shown in the figure

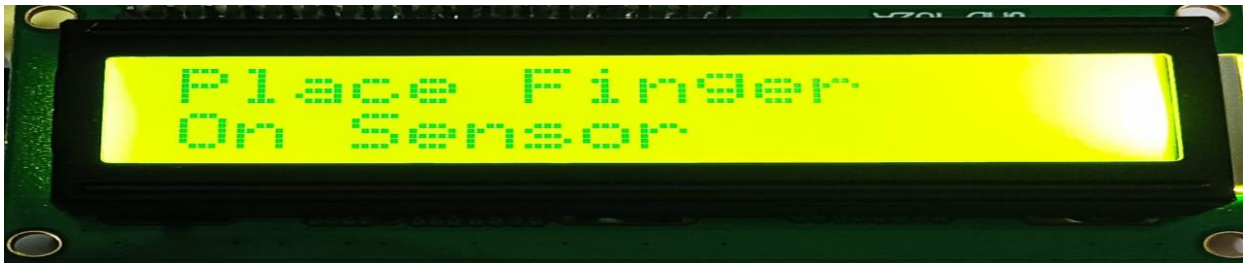


Fig 7.2.12 PLACE FINGER ON SENSOR TO VOTE AUTHENTICATION

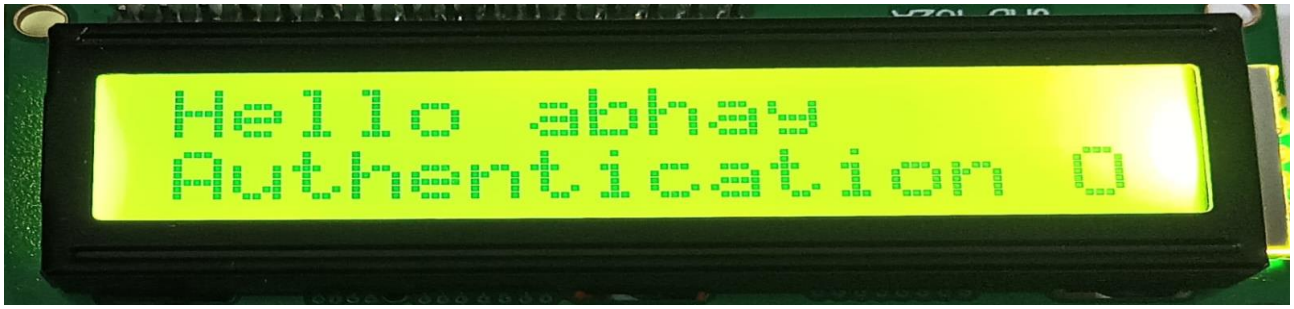


Fig 7.2.13 AUTHENTICATON SUCCESSFUL

Fingerprint scanned successfully please select party A, B, C Press 1,2,3 # to Confirm as shown in the below figure

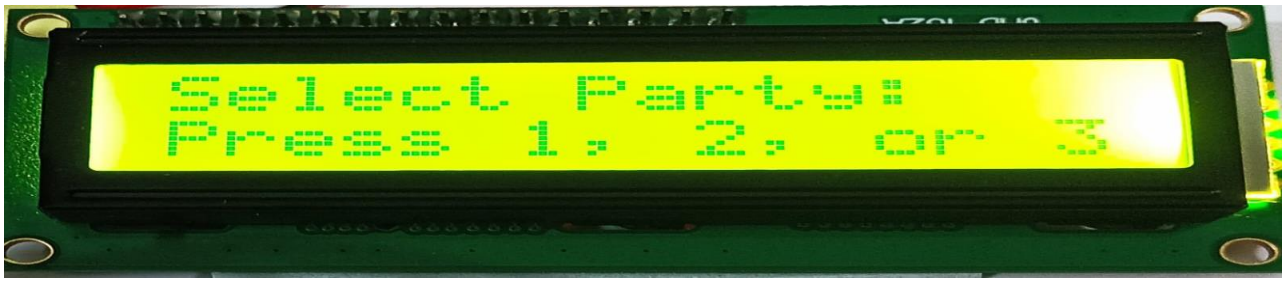


Fig 7.2.14 SELECT PARTY TO CASTE UR VOTE

Fig 7.2.15 CONFIRM PARTY PRESS # TO VOTE

Party Voted Successfully Voted Recorded Thank you as shown in the below figure

Fig 7.2.16 VOTE RECORDED THANK YOU NOTIFICATION

The system is now ready for the next voter. Please have the next voter proceed to cast their vote, as shown in the figure.

Fig 7.2.17 NEXT VOTER PLEASE COME INTERFACE

Voting Process stopped successfully and Voting responses are recorded successfully as shown in the below figure

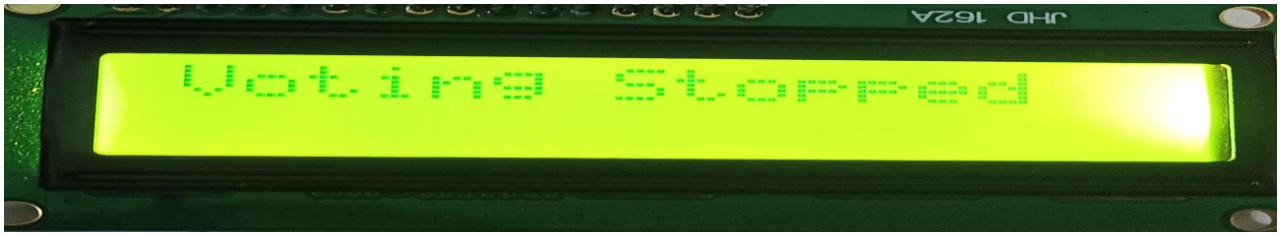


Fig 7.2.18 VOTING DONE SUCESSFULLY AND VOTING STOPPED

If any stage of authentication like fake RFID, fake Fingerprint an SMS Alert is sent to the concerned security person in the election commission office instantly he will get the alert like RFID cad number and Fingerprint mismatch alert will be sent.

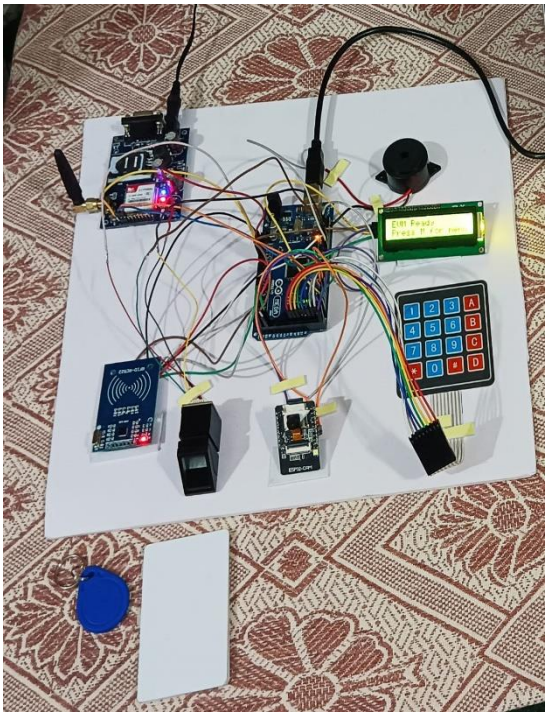


Fig 7.2.19 MALFUNCTION DETECTED AND SENT VIA SMS ALERT THROUGH GSM

APPLICATIONS

1] NATIONAL AND STATE ELECTIONS -

This system can be implemented in government elections to provide a secure, efficient, and dependable voting process.

2] ORGANIZATIONAL VOTING –

Companies, clubs, and institutions can use this EVM for internal elections or decision-making processes.

3] UNIVERSITY AND COLLEGE ELECTIONS –

Student councils and campus organizations can implement the system to conduct fair and transparent elections.

4] REMOTE VOTING LOCATIONS –

Thanks to its portability and GSM connectivity, the system can be effectively utilized in remote or rural areas where deploying traditional EVMs is challenging.

5] COMMUNITY OR LOCAL GOVERNANCE ELECTIONS –

The system can help small communities or local government bodies conduct efficient and tamper-proof elections.

6] SECURE POLLING IN PRIVATE EVENTS –

Any event requiring confidential and verified voting, such as awards selection or surveys, can use this system.

7] SMART CITY GOVERNANCE –

Integration with IoT and GSM allows city authorities to monitor and manage civic voting processes efficiently.

8] ELECTION MONITORING IN DISASTER ZONES –

The portable and GSM-enabled system can facilitate voting in areas affected by natural disasters where conventional EVMs may be difficult to deploy.

9] MOBILE VOTING BOOTHS –

Can be used in mobile or temporary booths for door-to-door voting in rural or inaccessible regions.

10] CORPORATE DECISION-MAKING –

Large corporations can use it for board member elections, shareholder voting, or confidential internal polls.

CHAPTER 10

CONCLUSION

The developed Electronic Voting Machine (EVM) integrates fingerprint authentication, RFID-based voter verification, ESP32-CAM monitoring, and GSM-enabled malfunction reporting to deliver a secure, reliable, and user-friendly voting system. This layered approach ensures that only authorized voters can cast their votes while enabling real-time monitoring of the polling environment. Automating vote recording and result transmission minimizes human errors and reduces the likelihood of fraud or manipulation. Overall, this project highlights how modern technology can improve transparency, efficiency, and public trust in the electoral process

REFERENCES

1] Jambhulkar, S. M., Chakole, J. B., & Pardhi, P. R. (2014). Secure design for internet-based voting using multi-layer encryption. Proceedings of the International Conference on Electronic Systems, Signal Processing and Computing Technologies.

2] Pashine, P. R., Ninave, D. P., Kelapure, M. R., Raut, S. L., Rangari, R. S., & Hajari, K. O. (2013). Android-enabled secure e-voting and social governance solution. International Journal of Engineering Trends and Technology (IJETT), 9(13), March 2.

3] Khasawneh, M., Malkawi, M., & Al-Jarrah, O. (2008). Biometric-based secure electronic voting approach for election procedures. Proceedings of the 5th International Symposium on Mechatronics and its Applications (ISMA08). Amman, Jordan.

4] Sridharan, S. (2013). Development of a verified and secure online voting framework. Fourth International Conference on Computing, Communication and Networking Technologies (ICCCNT). Tiruchengode, India, July, IEEE – 31661.

5] Hazzaa, F. I., Kadry, S., & Zein, O. K. (2012). Web-oriented fingerprint-assisted voting system: design and execution. International Journal, 2(4), December.

6] Katiyar, S., Meka, K. R., Barbhuiya, F. A., & Nandi, S. (2011). Online voting protected with biometrics and steganography techniques. Second International Conference on Emerging Applications of Information Technology.

7] Agarwal, H., & Pandey, G. N. (2013). Online voting framework for India utilizing Aadhaar authentication. Eleventh International Conference on ICT and Knowledge Engineering.

8] Kaliyamurthie, K. P., Udayakumar, R., Parameswari, D., & Mugunthan, S. N. (2013). Network-oriented highly secured e-voting system. Indian Journal of Science and Technology, 6(6S). Print ISSN: 0974-6846 | Online ISSN: 0974-5645.