Anti-Fraud Mechanism Based Voting Machine With Three Stage Authentication Methods

Abstract— **A digital voting system can be the beginning of an effective, transparent, and secure voting process with the integration of technology into every aspect of our society. This study proposed a reliable and user-friendly voting system that would count votes securely using an Arduino microcontroller board. To ensure that only allowed voters can cast a ballot at a time, the system employs a three-step verification process including password, fingerprint and RFID (Radio Frequency Identification) authentication. An alert is activated in the event of unwanted access or tampering and can be silenced using the admin password. The administrator may also log in using his or her password to view the outcome of the voting. In comparison to the conventional Electronic Voting Machine (EMV), the proposed system has a number of benefits including quick and accurate vote counting, the removal of human intervention errors, increased transparency and reduced possibility of election fraud.**

Keywords—Electronic Voting Machine, Authentication, Security, RFID, Anti-Fraud.

I. INTRODUCTION

With the development of technology, routine tasks like home upkeep, traffic management, and agriculture have become automated, making them safer, more dependable, and quicker. The development of IoT-based automation is a key aspect in improving daily tasks [1]-[3]. Similarly, for democratic countries, IoT based voting systems play a pivotal role in reliable, fast and fair voting process. Traditionally voting was done with papers being marked with the stamp of the candidate's symbol and stored in a ballot box. To find out how many votes each candidate received, the ballot boxes were gathered, and the papers with stamps were counted one by one. This process would not only take a lot of time but miscounting and fraud were very common.

To stop these initial problems, EMVs were implemented as new the voting method alongside electronic record system to store data [4]. The machine consisted of a display, fingerprint scanner and push buttons to choose a candidate. An automated system like image recognition and processing technology was proposed but never implemented [5]. Though it managed to solve some of the initial problems that traditional voting had, it generated some new ones such as malfunctions and technical issues, high cost, database security, maintenance issues and risk of security breach. Due to these problems, a reliable voting system that ensures the integrity of election is difficult to establish.

To reduce attempts of fraud in voting, security and surveillance around voting system needs to be enhanced. The system that identifies voters must have multiple steps to ensure his/her identity. The process of storing the votes must be secure so that it is safe from any cyberattack or hacking attempts. The voting system cost should be reasonable as many underdeveloped and developing countries might not be able to afford them. Finally, the counting process must be transparent and precise to reduce any chance of ingenuity.

Research on authentication measures in voting systems has explored various methods, including an Arduino-based system with only one biometric verification via fingerprint sensor and GSM (Global System for Mobile) module in [6]. However, the system lacks any kind of data encryption, limited candidate choices, and no alarm system for when tempering with voting machine. In [7], authors proposed a biometric verification system using fingerprints and AADHAR numbers for Indian national voters. The disadvantage of this study was lack of security when it came to storing data. The proposed system also had no alarm system if the voting box was being tempered with. In [8], AADHAR ID-based system compares biometrics such as fingerprint and face recognition with the AADHAR database but encounters issues with a lack of proper encryption of data, no explanation on the accuracy of face recognition and no alarm. Another research has proposed an EVM system in [9] that used a fingerprint sensor to confirm the authenticity of voters by taking their biometrics into the framework. At the same time, any tempering attempts with the voting box was not answered while having limited candidate choices. In [10], the authors used a fingerprint sensor alongside two Arduinos and an external data transfer system. The data stored on the SD (Secure Digital) card can't be accessed remotely. No alarm system in case of multiple voting, limited SRAM (Static Random-Access Memory) and no registration process were the major shortcomings of this system. In [11], the authors improved the security and reliability of the system by using unimodal fingerprint biometrics and an advanced encryption standard based Wavelet Crypto-watermarking approach. Though this paper exerted itself when it came to data security, the components of this project only had a fingerprint sensor and no alarm system. The system in [12] consisted of tamper proof SD card which was used to store all information. This

system failed to describe the proper registration process and anti-tempering techniques if the voting box is attacked. Also, the use of GSM, UART (Universal Asynchronous Receiver Transmitter) and LEDs (Light Emitting Diode) were not explained. In [13], introduction to RFID-based electronic voting machine with fingerprint verification was made which suffered from not having a complete registration process, anti-tempering capabilities. The data was also stored on the microcontroller, which made it inaccessible remotely. In a case where the system was shut down, the stored data would be wiped. Finally, in [14], an RFID-based EVM that consisted of an RFID reader, buzzer and LCD had some major issues such as a lack of anti-tempering ability. The use of a microcontroller-based database which would be erased if the system was shut down made the database remotely inaccessible.

From the above research it is found that most of the existing EVMs have disadvantages like having only one or two layers of security, lack of a password system and anti-tempering capabilities. These vulnerabilities render them susceptible to various forms of assaults. To overcome all these disadvantages, in this paper three-step verification has been introduced which comprises password, fingerprint, and RFID authentication. The RFID and fingerprint sensor alongside the password system ensures the authenticity of a voter. The system allows only one vote per voter and the vote counts can only be accessed with the admin password. Any attempt at tempering with the voting box will trigger an alarm letting the admin know of the security breach. A built-in timer has been set which will not let anyone change the vote counts even if the admin wants to.

The paper is organized as follows. The present section introduces the basic idea of the study. Epistemological framework is presented in section II. Section III explains experimental setup of the project. Section IV contains results and dissections including the possible outcomes of this project. Finally, conclusion is drawn in section V.

II. EPISTEMOLOGICAL FRAMEWORK

An electronic voting machine records votes in a digital storage without paper. The overall process of the voting will be conducted electrically. Here, the goal is to improve already existing electronic voting system by adding an additional layer of security as well as enhance the anti-tempering capabilities to reduce the fraudulent activities.

The machine suggested in this paper has 3 inputs. The first input is a card, second one is a password and the third one is a fingerprint. All these three are combinedly needed for voter identification. It will also make sure that no one can vote multiple times. It has a display that will also help the voters to follow the processes sequentially. As a scenario, for the very first time, the voter will be instructed to scan his or her card. If he/she provides the correct card, he/she will be instructed to provide his/ her password. If he/she also provides the correct password, he/she will be further instructed to scan his/her fingerprint. After all these personal verifications, he/she will be permitted to provide a vote just one time by pressing a single button. If anyone fails to provide any specific information, he/she will be instructed to follow instructions and provide correct information.

A. Mathematical Interpretation

The first sensor is RFID that is responsible for checking if the person is a registered voter or not. It uses radio waves to transmit signals that actives the tag. In [15], chip in the tag receives power with the equation given below:

$$P_L = P_{in} G_{tag} \lambda^2 / (4\pi R)^2 \quad (1)$$

After that, the reader portion of RFID receives power in a method described in the equation:

$$P_{rec} = P_{in} G^2{}_{reader} G^2{}_{tag} \lambda^4 / (4\pi R)^4 \quad (2)$$

where, A_s is effective scattering aperture, A_e is effective receiving aperture, P_L is power received by the chip in the tag, P_{rec} is power received by the reader (via the re-radiation), S_i is power density at *I*, G_i is Antenna *i*'s gain, σ is radar cross-section.

If there is a difference in impedance and polarization between components, the equations will be adjusted to account for this by introducing two factors: the polarization mismatch factor (p) and the reflection coefficient from the tag (Γtag). According to [15], these factors will be used to modify the equations accordingly.

$$P_L = \left(1 - |\Gamma_{tag}|^2\right).p.P_{in} G_{reader} G_{tag} \lambda^2 / (4\pi R)^2 \quad (3)$$

$$P_{rec} = p.P_{in} G^2{}_{reader} G^2{}_{tag} \lambda^4 / (4\pi R)^4 \quad (4)$$

The unique password for each voter is set in the Arduino microcontroller. During voting, the voters will provide their password using keypad sensor.

After successful RFID and password match, fingerprint sensor is used to ensure RFID tag holder is the voter themselves. R307 Optical Fingerprint Reader Module sensor has been used in fingerprint authentication process. The optical fingerprint sensor that is proposed in this study has a certain working principal consists of two major processes. One is fingerprint enrollment and the other one is fingerprint matching. Enrollment process includes biometric presentation, capture and processing, feature extraction of the finger vein patterns using repeated line tracking, template generation and template storage process. Fingerprint matching process is conducted utilizing sub processes which includes biometric presentation, template creation and template comparison with the existing templates in the storage using a certain ID. Practically, to match the fingerprints, similarity score using Euclidean distance is also measured which is presented in equation (5). However, the utilized fingerprint module can register up to 127 unique fingerprint identifications.

$$\text{E.D} = \sum \left(\sqrt{\left(\left(m_{i_x} - t_{i_x}\right)^2 + (m_{i}\_y - t_{i}\_y)^2\right)}\right) \quad (5)$$

where, (m_i_x, m_i_y) are the coordinates of the extracted minutiae point, (t_i_x, t_i_y) are the corresponding coordinates in the template. Also, E.D denotes Euclidean Distance. The similarity score dictates if the fingerprint is a match or not. Fig. 1 depicts the overall voting process using the developed EVM, where three-layer security has been ensured utilizing step-by-step authentication using RFID, password and biometric fingerprint match.

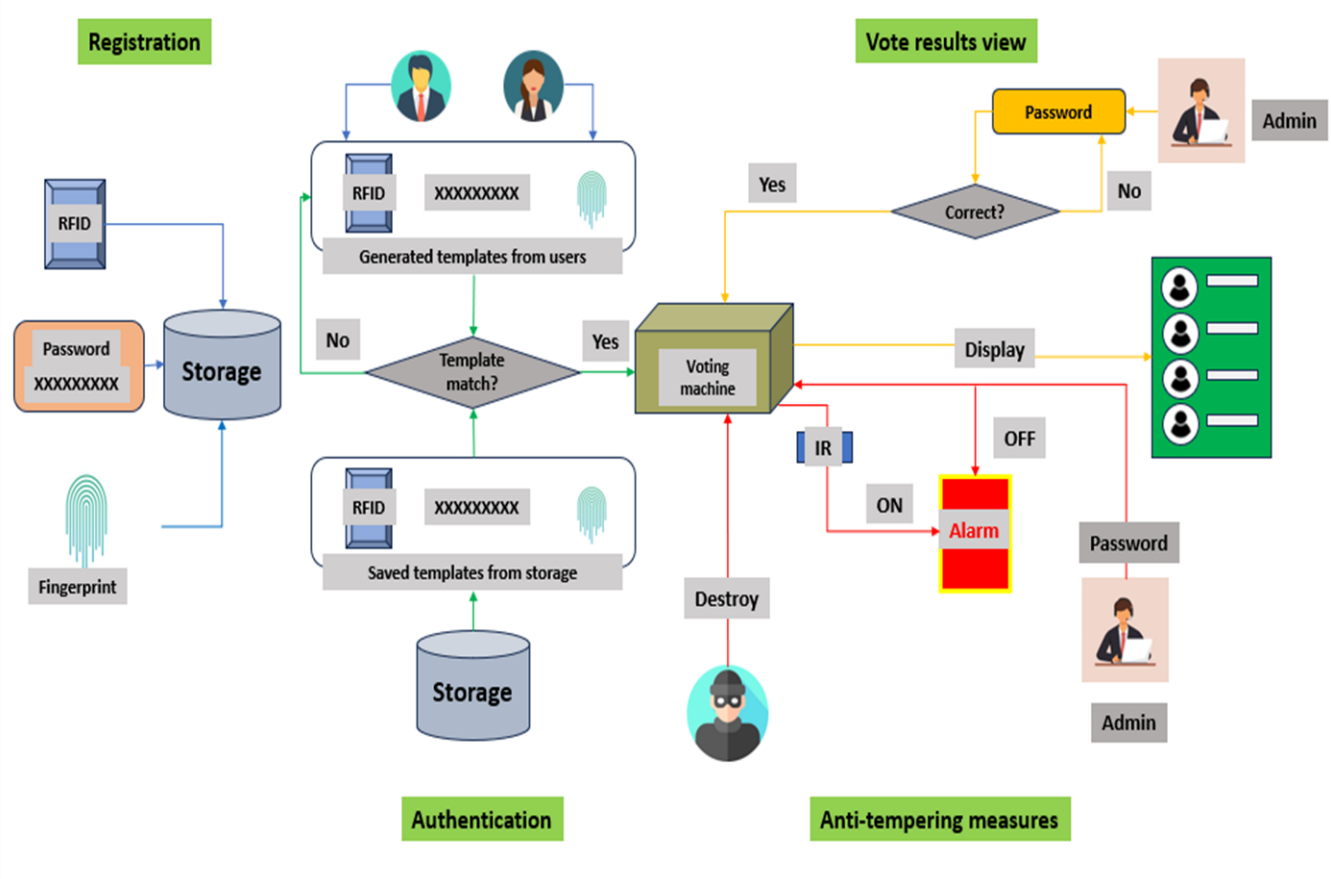

Fig. 1. Overall Working Process of Proposed Voting Machine

Admin authentication is required to view the results. Results will be stored in Arduino. To view the results, the admin needs to click a button. After clicking on that particular button, the admin needs to provide his/her password. Just after providing the correct password, the admin can view the results on the display. If the given password is incorrect, the admin will be redirected to the password section again where he/she must input the correct password.

If the voting box faces any tempering attempt or fraudulent activity, the buzzer in the voting box activates triggering an alarm that goes off in short intervals. The buzzer can only be switched off if the admin provides the Admin Password.

III. EXPERIMENTAL SETUP

The box is made out of sturdy and relatively cheap materials. On top of the box there are 5 push switches, a fingerprint scanner, a keypad, a LCD (Liquid Crystal Display) and a RFID sensor. The system along with some sensors, buttons and scanners are shown in Fig. 2. The IR (Infrared Sensor) has been configured within the voting box. It has been connected both manually and programmatically with the buzzer. So, these components are not properly visible in Fig. 2. For this study, RC522 card reader module as RFID Sensor, R307 Optical Fingerprint Reader Module as fingerprint sensor and Keypad 4*3 sensor as password provider has been used. All these three modules have been used for authentication purpose. In table I, the components that has been used for developing the EVM are listed.

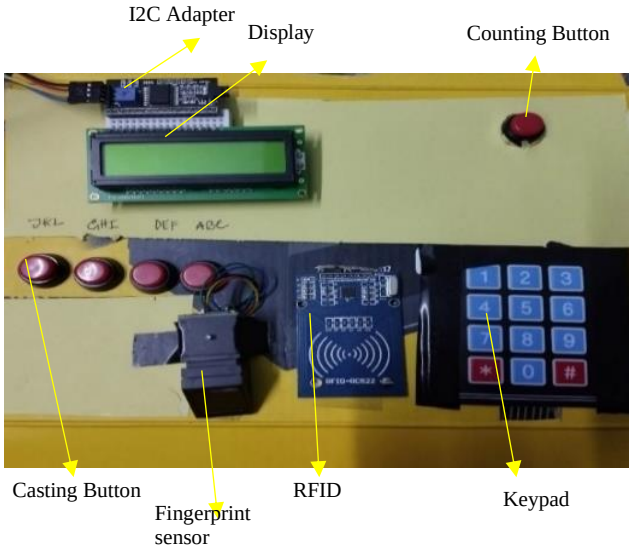

Fig. 2. Experimental Setup of Voting Machine

IV. RESULTS AND DISCUSSION

This section of the study is divided into five sub-sections. The first sub-section denotes the voting outcomes. In the next sub-section, vote counting outcomes has been described. Subsequently, safety protocol outcomes have been expressed.

Furthermore, possible cases and outcomes have been reported. Lastly, a comparison of proposed voting machine

with existing voting machines described in some renowned journals are compared.

TABLE I. LIST OF COMPONENTS

Components	Specification	Function
Arduino Uno	A microcontroller board used for building electronic projects that takes the decision and outputs a result [16].	The main board from where the majority of the processing is performed. It also works for the data storage of this proposed study.
Push Switch	A momentary switch which is used to make or break an electrical connection usually constructed of a strong durable material such as metal or plastic [17, 18].	These switches have been used to initiate tasks, such as, vote counting and choosing candidates.
16*2Display	Liquid crystal display (LCD) is a display screen with a digital show module that has 2 lines accompanied by 16 characters per line [18].	The main display where the instruction and the results of the voting process are shown.
Serial I2C LCD Display Adapter	A module that allows an I2C LCD display to be connected to an Arduino via serial communication [19].	The adapter that helps to connect the Arduino to the LCD.
R307 Optical Fingerprint Reader Module sensor	A biometric sensor that scans a fingerprint to verify the user's identity [20].	It has been used to collect and match the fingerprints of the voters.
RC522 card reader module or RFID Sensor	A sensor that uses radio waves to read data stored on an RFID tag [21].	RFID sensor has been used to identify the voters and to store the unique passwords.
Keypad 4*3 sensor	A set of buttons arranged in a grid used for inputting numbers, letters, or symbols [22].	It has been used so that the voters can provide the unique passwords.
Buzzer	An electronic component that makes a sound when a voltage is applied to it [23].	Buzzer has been used to alert the admin if any kind of tempering is attempted.
IR Sensor	A sensor that detects infrared radiation and is commonly used in remote controls [24].	IR sensor will detect if the voting box is being tempered with.

A. Voting Outcomes

Table II shows the possible outcomes voters might face with the voting machine.

Case 1.
When the RFID card does not match, the system shows "Wrong card" and avoids taking password and fingerprint input.

Case 2.
When the RFID card matches and wrong password is given, the system shows "Wrong password" prompt and avoids taking fingerprint input.

Case 3.
When both RFID and password match while unauthorized fingerprint is provided, the system shows "Fingerprint doesn't match" prompt.

Case 4.
When all of the mentioned inputs match, the system redirects the user to the voting process.

In Fig. 3, it is showed that whenever a wrong RFID card is used in an attempt to vote, the device will automatically redirect the user and display "Wrong Card" prompt.

TABLE II. POSSIBLE OUTCOMES OF VOTING PROCESS

Observations				Result
Cases	**RFID**	**Password**	**Fingerprint**	**-**
1	0^a	x	x^c	Wrong card
2	1	0	x	Wrong Password
3	1	1^b	0	Fingerprint doesn't match
4	1	1	1	Provide vote

0^a denotes wrong, 1^b denotes correct, X^c denotes missing

Fig.3. Wrong Card Input Prompt

B. Vote Counting Outcomes

Table III shows the possible outcomes admin can have with the voting machine.

Case 1.
If the provided admin password is incorrect, the prompt shows no output, and the vote results remain hidden.

Case 2.
If the provided admin password is correct, the admin can view the outcome of the vote.

Fig. 4 shows the overall results of the candidates to the admin after providing correct password.

TABLE III. POSSIBLE OUTCOMES OF COUNTING PROCESS

Cases	Observations	Result
1	Admin Password = 0^a	No output
2	Admin Password = 1^b	Result of votes

0^a denotes wrong, 1^b denotes correct

Fig.4. Result of Voting Process

C. *Safety Protocol Outcomes*

Table IV shows the what would happen if the buzzer was set off due to a tempering attempt.

Case 1.

If vote theft is attempted and admin password is not provided, the buzzer will buzz as an alarm.

Case 2.

If vote theft is attempted and admin password is provided correctly, the alarm will stop automatically.

TABLE IV. POSSIBLE OUTCOMES IF TEMPERING ATTEMPT HAPPENS

Cases	Observations	Admin password	Result
1	Vote theft = 1	0^a	Buzzer = 1
2	Vote theft = 1	1^b	Buzzer will stop buzzing

0^a used for successful; 1^b used for unsuccessful

D. *All possible interactions between EVM and different users*

Table V presents a comprehensive overview of the many scenarios that a voting machine may encounter, along with the corresponding results it would choose.

TABLE V. ALL POSSIBLE OUTCOMES OF THE DEVELOPED VOTING MACHINE

Cases	Outcomes
RFID matches the database	The user can give his/her password
RFID does not match the database	User have to scan a valid RFID
Password matches the database	The user can scan his/her fingerprint
The password does not match the database	User have to scan a valid RFID
Valid fingerprint	User can vote
Invalid fingerprint	User have to scan valid fingerprint
Vote given	"Thank you" message is shown and gets back to first step
Someone tries to open the voting machine	An alarm makes a sound until the admin provides admin password
Admin gives the password to check the vote	Vote details are shown in the display
Someone tries to vote for the second time.	Wrong card output will be shown

E. *Comparative Study*

In table VI, a comparison of proposed voting machine with five other existing voting machines described in some renowned journals are displayed.

TABLE VI. COMPARATIVE STUDY IN BETWEEN SUGGESTED AND OTHER PREEXISTING VOTING SYSTEMS

Ref.	National ID card	GSM	Password	RFID	Alarm	Fingerprint	Single Arduino	Double Arduino	Local Database	Cloud Database/External Database
[6]	✓	✓	-	-	-	✓	✓	-	-	✓
[7]	✓	-	-	-	✓	✓	✓	-	-	✓
[9]	✓	-	-	-	✓	✓	✓	-	-	✓
[10]	-	-	-	-	-	✓	-	✓	✓	-
[13]	-	-	-	✓	✓	✓	✓	-	✓	-
Proposed	-	-	✓	✓	✓	✓	✓	-	✓	-

The parameters that have been taken for comparison are National ID Card (AADHAR), GSM module, password, RFID, alarm, fingerprint, single Arduino, double Arduino, Local database and other possible components according to database type. From this section, only one study has been found containing three-layer security but lacks of an anti-tempering system. It also has no database security as it used publicly available third-party website to store confidential information. However, the proposed study confirms three-layer security and an anti-tempering system altogether.

V. CONCLUSION

In conclusion, a possible advancement in electronic voting is the Arduino voting machine project with three-step verification. The project demonstrates the capability of utilizing open-source, low-cost technologies to create a secure and trustworthy voting machine.

The Arduino voting machine, a promising advancement in electronic voting, has several drawbacks. The primary limitation is the data storage method, which can be wiped if the Arduino is turned off. The registration process lacks an admin password, making it difficult and reducing effectiveness. Additionally, there are only four available candidates due to the lack of buttons.

Overall, the Arduino voting machine could be an innovative and affordable way to hold secure and fair elections globally. Further improvements include proper data storage and a proper registration process. GSM technology can enhance security by adding more steps to verify voter authenticity.

REFERENCES

[1] J. F. Riya, M. T. H. Chowdhury, S. A. Usha, S. Howlader, S. Ahmad and M. Z. Islam, "A Smart Helmet: Ensuring Safety of Bike Riders," *2023 3rd International Conference on Robotics, Electrical and Signal Processing Techniques (ICREST)*, Dhaka, Bangladesh, 2023, pp. 305-310.

[2] S. Niloy, F. H. Sumona, M. H. Khan, M. Z. Islam, S. Ahmad and S. Howlader, "Solar Powered Smart Irrigation System Based on Internet of Things (IoT) Using Microcontroller," *2023 3rd International Conference on Robotics, Electrical and Signal Processing Techniques (ICREST)*, Dhaka, Bangladesh, 2023, pp. 259-263.

[3] S. Ahmad, A. Saha, L. W. Chek, S. Mekhilef, T. Azam, M. Ahmed, M. Orabi, S. Ghoneim, M. Alharthi, F. Salem, B. Alamri, "Smart home automation and security system design based on iot applications", *ASEAN Engineering Journal*, vol. 9, no. 2, Dec., pp. 57-71, 2019.

[4] T. Ahmed, S. B. Sharif, T. A. Joy, M. H. Chowdhury, and M. H. Imam, "Design of a cost-effective customized Electronic Health Record system to handle patient management during Covid-19 pandemic", *AIUB Journal of Science and Engineering*, vol. 20, no. 1, Apr., pp. 41 - 46, 2021.

[5] R. Shahrear, M. A. Rahman, A. Islam, C. Dey, and M. S. R. Zishan, "An Automatic Traffic Rules Violation Detection and Number Plate Recognition System for Bangladesh", *AIUB Journal of Science and Engineering*, vol. 19, no. 2, Sep., pp. 87 - 98, 2020.

[6] V. R. Ch, M. V. P. A and B. S. S. A, "Arduino based Electronic Voting System with Biometric and GSM Features," *2022 4th International Conference on Smart Systems and Inventive Technology (ICSSIT)*, Tirunelveli, India, 2022, pp. 685-688.

[7] S. C. Venugopal and R. K. Rajan, "IoT based Voting Machine with Fingerprint Verification," *International Journal of Applied Engineering Research*, vol. 15, Nov., pp. 97–104, 2020.

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

[9] S. Agarwal, A. Haider, A. Jamwal, P. Dev and R. Chandel, "Biometric Based Secured Remote Electronic Voting System," *2020 7th International Conference on Smart Structures and Systems (ICSSS)*, Chennai, India, 2020, pp. 1-5.

[10] M. S. U. Ahmed et al., "Development of a Secured and Low-budget Biometric Electronic Voting Machine for Bangladesh," *2021 2nd International Conference on Robotics, Electrical and Signal Processing Techniques (ICREST)*, Dhaka, Bangladesh, 2021, pp. 753-757.

[11] O. M. Olaniyi, T. A. Folorunso, A. Ahmed and O. Joseph, "Design of secure electronic voting system using fingerprint biometrics and crypto-watermarking approach," *I.J. Information Engineering and Electronic Business*, vol. 5, Sep., pp. 9-17, 2016.

[12] Dr. V. V. Vegesna, Ms. M. V. Peter, Ms. V. Priya, Ms. H. Petchammal, and Dr. N. Muthukumaran, "Finger Print Based Smart Voting System," *Asian Journal of Applied Science and Technology*, vol. 2, no. 2, Apr., pp. 357–361, 2018.

[13] V. Malathy, N. Shilpa, M. Anand, and R. Elavarasi, "Radio frequency identification based electronic voting machine using Fingerprint Module," *IOP Conference Series: Materials Science and Engineering*, vol. 3, pp. 1-9, 2020.

[14] S. Pulipaka and S. Nookala, "Electronic voting machine using IOT and RFID," *International Journal of Engineering Research and Technology*, vol. 13, pp. 1-5, 2020.

[15] S. Kahng, "Design Fundamentals and Advanced Techniques of RFID Antennas," *Dev. Implement. Incheon National University*, South Korea, 2009.

[16] B Singla, S Mishra, A Singh, and S Yadav, "A study on smart irrigation system using IoT*," International Journal of Advance Research, Ideas and Innovations in Technology*, vol 5, no. 2, pp. 1416-1418, 2019.

[17] A. Mukesh, Ch. K. Varaprasad, A. J. K. Murthy, M. Rajamouli, and Dr. A. Venkataramana, "Finger print based electronic voting system," *International Journal of Progressive Research in Engineering Management and Science*, vol. 3, no. 2, Feb., pp. 250–254, 2023.

[18] T. Nagaraju, G. Vishnupriya, N. Vennela, N. Lokteja, G. M. Saifullah, and K. V. Chowdary, "Real-Time Wireless Embedded Electronics for Soldier Security", *International Research Journal of Modernization in Engineering Technology and Science*, vol. 5, no. 3, Mar., pp. 2021-2027, 2023.

[19] T. S. Lim, S. C. Sim and M. M. Mansor, "RFID based attendance system," *2009 IEEE Symposium on Industrial Electronics & Applications*, Kuala Lumpur, Malaysia, 2009, pp. 778-782.

[20] S. Namboodiri and A. P., "Fingerprint based security system for vehicles," International Journal of Advance Research, Ideas and Innovations in Technology, vol. 4, no. 4, pp. 370-372, 2018.

[21] J. B. Sy, S. M. Akele and E. B. Panganiban, "Wireless home automation with security system (WHASS)," *International Journal of Electrical Engineering and Technology*, vol. 11, no. 9, Nov., pp. 101-110, 2020.

[22] M. H. Hersyah, D. Yolanda and H. Sitohang, "Multiple Laboratory Authentication System Design Using Fingerprints Sensor and Keypad Based on Microcontroller," *2020 International Conference on Information Technology Systems and Innovation (ICITSI)*, Bandung, Indonesia, 2020, pp. 14-19.

[23] M. J. Manurung, P. Poningsi, S. R. Andani, M. Safii, and I. Irawan, "Door Security Design Using Fingerprint and Buzzer Alarm Based on Arduino," *Journal of Computer Networks, Architecture, and High-Performance Computing*, vol. 3, no. 1, Jan., pp. 42–51, 2021.

[24] M. Khairudin, G. W. Lanang, and A. Arifin, "Attadance system using infrared sensors," *Journal of Physics: Conference Series.*, vol. 1456, no. 1, p. 012012, 2020.