

Fingerprint biometric voting machine using internet of things

Zakiah Mohd Yusoff¹, Yusradini Yusnoor¹, Arni Munira Markom^{1,2},
Siti Aminah Nordin¹, Nurlaila Ismail²

¹School of Electrical Engineering, College of Engineering, Universiti Teknologi MARA, Cawangan Johor, Malaysia

²School of Electrical Engineering, College of Engineering, Universiti Teknologi MARA, Shah Alam, Malaysia

Article Info

Article history:

Received Aug 16, 2022

Revised Jan 6, 2023

Accepted Jan 10, 2023

Keywords:

Arduino
Fingerprint
Internet of things
Microcontroller
Voting system

ABSTRACT

Free elections are one of democracy's principles. Elections will be used to choose the representatives of the people. It is underlined on how important it is to organize free, fair, and secret elections. Traditionally, voting used to be conducted by stamping on paper, then placing it in a ballot box with the chosen candidate. Each vote in every ballot box must be counted separately, and the votes for each contender must then be added up to determine which candidate had the most votes. Everything was done manually, it will take longer to announce the winner. Numerous errors are being made, but they will not change the outcome. In this study, a significant system that stops electoral malpractices and expedites the voting process will propose. The controller utilized in this project is the Arduino Uno. The user is authenticated using a fingerprint. Everybody's fingerprints differ from one another. The device is programmed using the Arduino IDE, and the ballot card is displayed, and the results are stored in the cloud. Only a registered voter may cast a vote, and the system alerts users to any fraud. This project protects citizens' freedom to vote and ensures an impartial election.

This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.



Corresponding Author:

Arni Munira Markom
School of Electrical Engineering, College of Engineering, Universiti Teknologi MARA
Shah Alam, Selangor, Malaysia
Email: arnimunira@uitm.edu.my

1. INTRODUCTION

Voting was traditionally done by stamping a vote for the candidate of one's choice and then dropping the paper into a ballot box [1]. To determine the number of votes cast, each vote must be counted in each ballot box, then all of the votes for each candidate must be added together, and the candidate with the most votes will be declared the winner. From this manual voting, the results can be manipulated hence it is not fair for the contesting parties since the results are fake [1]–[3].

Each citizen has the right to vote and choose their leader through voting [4]. Malaysia is a democratic country in which every citizen has the right to vote and express their preferences. Every citizen have the most important responsibilities to avoid electoral fraud [5]–[7]. People can also vote for a candidate in the forthcoming election to change the ruling party [5]. Voting is not just used to elect government leaders, but also to elect leaders in schools, colleges, and other organizations.

Biometrics is a method of identifying a person based on his bodily characteristics. Biometrics such as fingerprints, iris, face, voice, and others are commonly used to identify people [8]–[10]. The first purpose of biometrics is one-to-one matching, and the second is one-to-many matchings. The biometric sample is matched to previously stored samples in one-to-many matching. It compares with the previously saved sample in one-to-one matching [9]–[15]. The biometric approach provides a more secure and convenient means of user verification [11], [13], [15].

Biometric security is superior to password security [12]. Because each person's fingerprint is unique, it can be used as a mark of signature, verification, and authenticity [12], [13]. Systematic system is crucial in every stage of a process. This is to prevent malfunctioning of software during the simulation of the system. Next is to speed up the vote counting process. Back in the old days, votes were counted manually using human energy. As a result, the announcement of the winner took a very long time, and sometimes the results were announced the following day [15], [16]. With this voting system, results can be announced faster as they are automatically counted by the system implemented. Consequently, the cost of paying staff to count votes manually can be reduce. Paying staff uses lots of money, and sometimes the paid amount is not enough. The money can be used to actually invest in a better voting system, such as a fingerprint-based biometric voting system.

2. THEORITICAL BACKGROUND

Voting is a crucial tool in a democratic system of government for selecting the best leader out of all the qualified individuals running for the position [17]. An honest "vote" can choose an honest candidate, which will ultimately lead to effective and moral government. A strong government may raise the level of living in a democracy in any nation [18]. By casting their vote for the appropriate party, voters can select the candidate who best represents their particular party. Electronic voting devices are utilized to provide a seamless and transparent election process [19]–[21].

In the past, individuals used a manual voting system in which they had to place each party's ballot paper in a separate voting box. Officers of the election committee count each party's ballot after voting is complete. The committee members who oversaw the counting procedure named the party with the most ballots the winner. There is a possibility that the traditional voting mechanism will malfunction, leading to things like double voting, fraudulent voting, and incorrect ballot paper counting. This issue is solved by electronic voting systems since the machine will count the ballots automatically [19].

A smart voting system must be designed to address the issues with manual voting and conventional electronic voting [21]. The technology that has been proposed is a smart voting system implemented on the internet of things (IoT) platform [22], [23]. As authentication is done by scanning the voter's fingerprint, the system is getting more secure. To enable the electronic ballot reset so that voters can cast their votes and to enable sending the vote information straight to the server, fingerprint authentication is done. Therefore, the valid person is only permitted to vote for one party. The system will accept the vote if the user can be verified. Since the system is built on an IoT platform, all statistics are sent to a web server.

Existing study by [1] discuss how to log in using the Aadhar [1], [19], [24], [25] number and password. Then, it determines if that person is qualified to vote. The policy around electronic technologies and advancements in data transmission and storage are examined in this article. To vote, the user must first display their fingerprint and confirm their eligibility. The information on the voter is retrieved from the tag via a fingerprint reader. The controller receives the data from the reader and compares it to the data that has previously been stored. That person may cast a ballot or poll his vote if the information matches the data that has been stored. A notification would appear on the LCD display if the information obtained from the fingerprint reader does not match the information previously recorded.

Then, the system proposed by [2] will be employed in a nation like Bangladesh. Electronic voting machines serves as the system's foundation. The voters' fingerprints are kept in a database that was developed by them. The inserted fingerprint searches for matches in the built-in database. The technology can tell if a voter has voted more than once and is not registered. The individual can vote if it fits the database. After some time has passed, the system tallies the votes and displays the outcome.

The current voting processes are discussed by [3]. This article addresses the drawbacks of electronic voting machines. The voter will be able to get an acknowledgement after casting their ballot on the computerized voting system. The votes have been manually tallied. This study outlines a quick and safe biometric voting system. The key goals are to make the model more flexible, secure, reliable, and scalable and to reduce the amount of time needed to announce the outcome.

3. METHOD

3.1. System diagram

Figure 1 shows the block diagram of the project. The fingerprint based biometric voting machine using the IoT is a project that implements the Internet of Things. This project is about designing a system for preventing election malpractices and speeding up the vote counting process compared to the traditional voting process. In this project, the matrix keypad and push buttons are used as the inputs, whereas the outputs are light emitting diode (LED), liquid crystal display (LCD), and buzzer. When the voter inserts their identity card (IC)

number through the matrix keypad. The matrix keypad will then send the data to the microcontroller, which is the Arduino Uno, and it will check with the stored database. If the IC number is verified, the voter can move to the next stage, which is the voting stage. However, when the IC number is not matched as in the database, the voter will be disqualified as their IC number is unauthorized by the system. All three of the outputs will be triggered by the announcement of the winner of the election, where the LED will turn ON when its prescribed candidate wins, followed by the sound of the buzzer. The LCD will also display the election's winner.

In this voting system, tie results can happen or even no votes are enrolled. When that happens, the LCD has been programmed to display "TIE NO RESULTS" and "NO VOTES CASTED" where the admin can be notified through the IoT immediately, so that actions can be taken. The IoT platform will be used to send all the data to the monitoring system unit. To send the data to the internet, an Arduino Uno will be wired to an ESP8266 Wi-Fi module so that remote monitoring of the data can be monitored by the authorized admin. TINKERCAD was used in this project because it can display real-time simulation and provide clear insight during the simulation process. The function for each components as tabulated in Table 1.

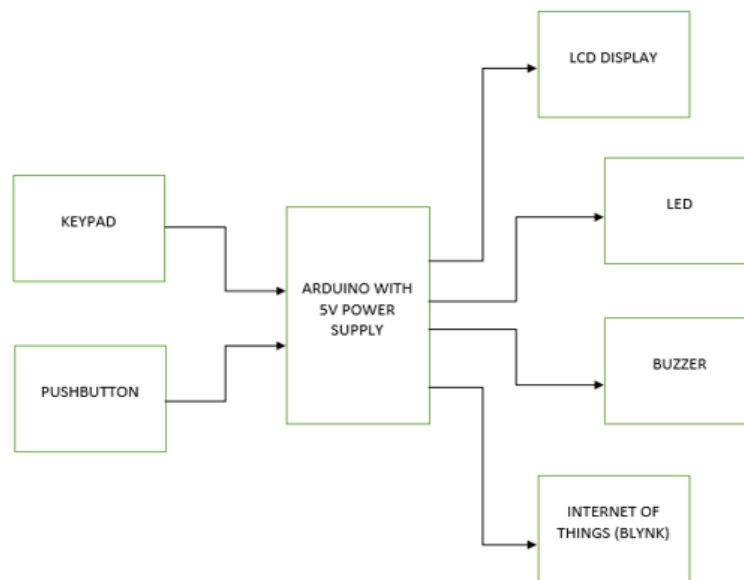


Figure 1. Block diagram of system

Table 1. Component of the project

No	Component	Function
1	Arduino Uno	The entire voting process, including reading pushbuttons, increasing vote value, producing results, and delivering vote and results to an LCD display, is controlled by Arduino
2	Pushbutton and Buzzer	Pushbuttons are utilized to choose the candidate for casting a vote while the Buzzer alerts the winner when a winner is announced.
3	LCD	The LCD is required to illustrate the system's fundamental processes as well as election results.
4	LED	Different colored LEDs are used to indicate which candidate win the election at the end of voting process when the result announcement.
5	Matrix Keypad	A matrix keypad is used in this system where it replaces the fingerprint sensor but has the same function as the fingerprint sensor. The voter will insert the IC number and if it is matched with the stored in the system, the voter will get verification to vote, or will be disqualified if the IC number is not verified.

3.2. Flowchart of the project

Figure 2 shows the flowchart of the project. Voter verification will be done using a keypad (fingerprint enrollement), where they will insert their IC number. Once verified, voter can begin to move to the next step, which is voting. However, when the inserted IC number does not match with the stored data, voter will be disqualified from voting. Verified voter can then vote for their desired candidates by pressing a specified pushbutton for each candidate. When a candidate is chosen, an LED for the specified candidate will light up. Then, the votes are sent to the system (Blynk) for counting. Lastly, the winner of the election will be displayed on the LCD and a buzzer will produce a sound.

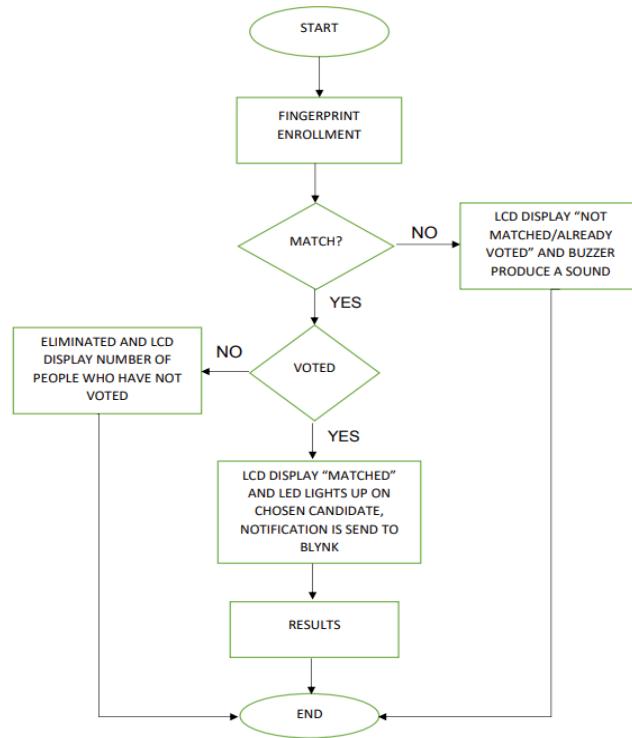


Figure 2. Flowchart of the project

3.3. System diagram

Figure 3 shows the system diagram of the project. This voting system will be utilized during election to speed up the voting process as well as the results counting process. A microcontroller is integrated into a system to operate a specific device function. It accomplishes this by analyzing data from its I/O peripherals using its core processor. The Arduino Uno will be used as a microcontroller. A matrix keypad is then used as the substitute for fingerprint sensor in the simulation to verify the voter before the voting process. Once the vote is casted, the LED for specified candidate light up and producing a sound, as well as displaying the result on the LCD.

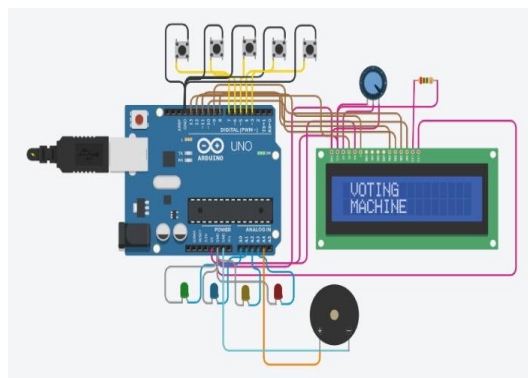


Figure 3. System diagram

In the diagram, it can be seen that the pushbuttons one to five are connected to pin 7, 6, 5, 4, and 3 of Arduino Uno respectively while all the negative legs are directly connected to the ground pin of the Arduino Uno. A potentiometer is also used to adjust the LCD's brightness level, where it is linked to VO, VCC which is the power supply and ground of the LCD, accordingly. Next, a resistor of 250 Ω is used to provide electrical resistance where it helps to lower the flow of the current.

The anode of green, blue, yellow and red LEDs is linked to the analog pins of the Arduino Uno, which are A0, A1, A2, and A3 consequently. Meanwhile the cathode of the LEDs is directly grounded to the ground pin of Arduino Uno. Each of the LEDs representing a specific candidate where it will light up when the candidate is chosen. A buzzer will also produce a sound whenever there is a winner announcement. Lastly, LCD's pin of RS, E, DB4 to DB7 is connected to the Arduino Uno's 13 to 8 pins, in descending order and the VCC to 5V and ground to GND pin of Arduino Uno.

4. RESULTS AND DISCUSSION

4.1. Voter verification

Based on Figure 4, the access is being denied because the inserted IC number did not match with the one in the stored data. Hence, the voter is disqualified to vote in the election. Figure 5 shows that the voter access to vote is granted and the LED is lighted up. This is because the voter's IC number is matched with the data, hence they can move to the stage which is the voting process.

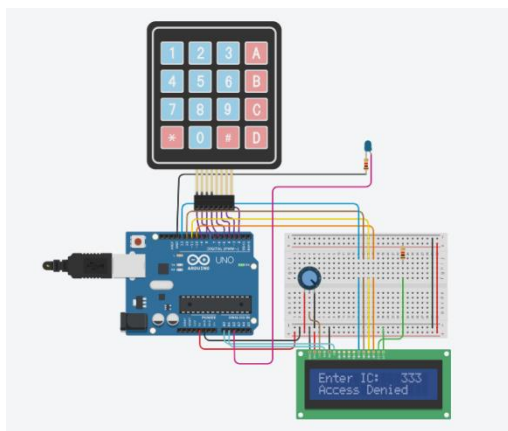


Figure 4. Access denied

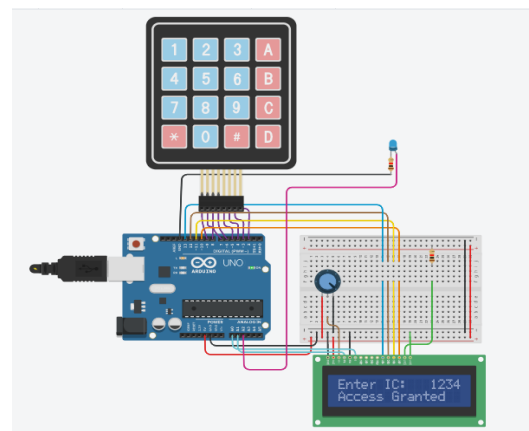


Figure 5. Access granted

4.2. Voter system

In the Figure 6, candidate A has won the election because they have the most received votes. When candidate A won, the green LED is lighted up as it is associated with candidate A. The buzzer also produced a sound to indicate a winner has been chosen for the election. Referring to Figure 7, the blue LED turned ON, indicates that candidate B has won the entire election, since they have the most votes, and triggering a sound to be produced by the buzzer.

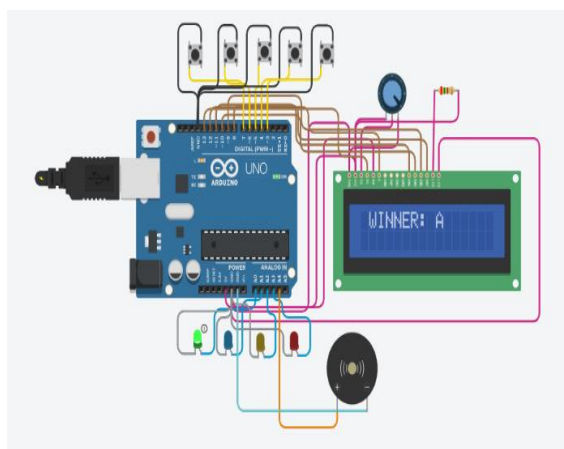


Figure 6. Candidate A won

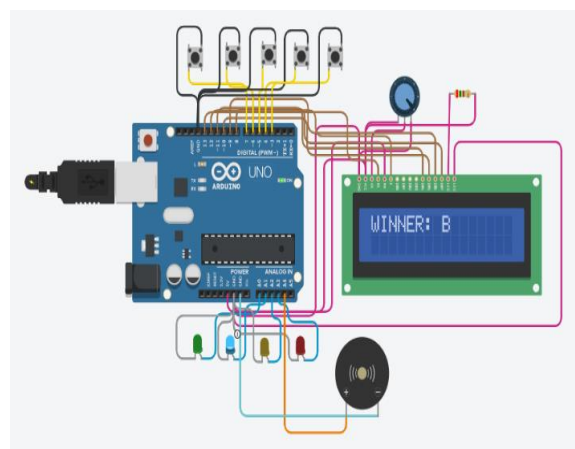


Figure 7. Candidate B won

Candidate C has won the election based on the Figure 8. This is due to the fact that it can be seen where the yellow LED is in high condition, which means that it is in ON state. The buzzer also in high state since it produced a sound. In this round of the election as shown in Figure 9, candidate D has beat other candidates since they received the most votes. Thus, it can be seen that the red LED turned ON, while the buzzer prouced a sound. Figure 10 shows that the votes between candidates are tie. This is because all the candidates received the same number of vites, hence no result of the winner during the election. Based on Figure 11, there is no vote casted for each of the candidates, which then the LCD displayed “NO VOTE CASTED”. With that, there is no results announced as there is no winner for the election.

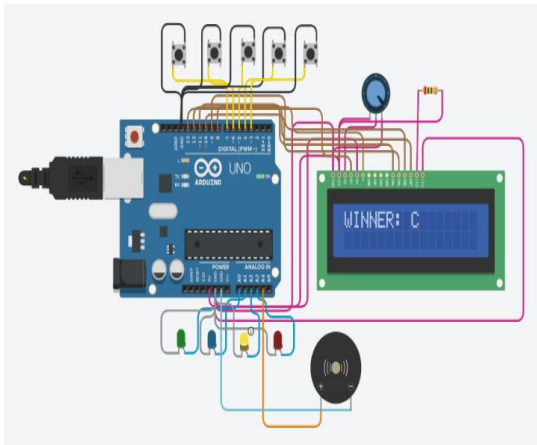


Figure 8. Candidate C won

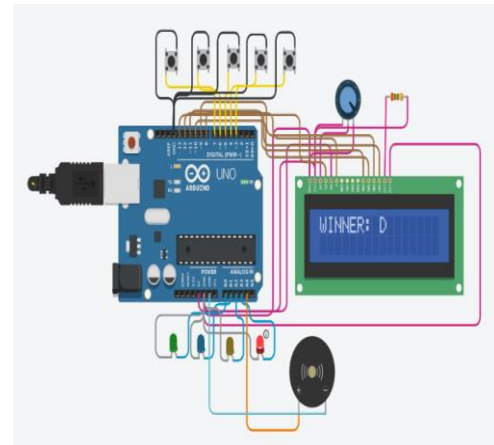


Figure 9. Candidate D won

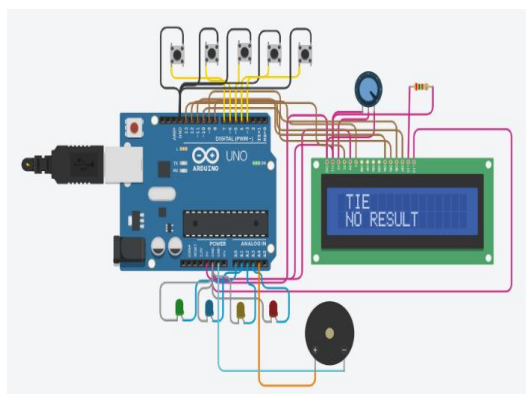


Figure 10. The And no result

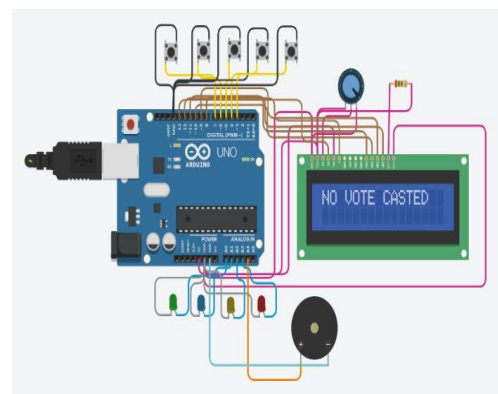


Figure 11. No vote casted

4. CONCLUSION

In conclusion, a system that solves most of the issues with the current voting system has been developed. This technique will undoubtedly offer a more secure voting procedure, which is essential for a developing country's overall development. The voting method based on fingerprints that is suggested in this research is quicker and more effective than the systems previously described in the literature. A systematic voting system has been developed in this project, where it is also speed up the vote counting process after the voting process. The cost of paying staffs to count votes manually are also reduced since the votes are counted digitally. Therefore, it is advised that the proposed method be put into place at the national level to obtain the significant benefit of making the electronic voting system completely foolproof.

ACKNOWLEDGEMENTS

This work is supported by Universiti Teknologi MARA under MyRA research grant with file no. 600-RMC/GPM ST 5/3 (027/2021). Many thanks all the staff involved: the School of Electrical Engineering,




College of Engineering, Universiti Teknologi MARA (UiTM), Cawangan Johor, Kampus Pasir Gudang, UiTM Shah Alam and Institute of Research Management and Innovation (IRMI).

REFERENCES




- [1] R. Murali, P. Bojja, and M. Nakirekanti, "AADHAR based electronic voting machine using Arduino," *International Journal of Computer Applications*, vol. 145, no. 12, pp. 39–42, Jul. 2016, doi: 10.5120/ijca2016910786.
- [2] R. Rezwan, H. Ahmed, M. R. N. Biplob, S. M. Shuvo, and M. A. Rahman, "Biometrically secured electronic voting machine," in *2017 IEEE Region 10 Humanitarian Technology Conference (R10-HTC)*, Dec. 2017, pp. 510–512, doi: 10.1109/R10-HTC.2017.8289010.
- [3] S. Anandaraj, R. Anish, and P.V. Devakumar, "Secured electronic voting machine using biometric," in *2015 International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS)*, Mar. 2015, pp. 1–5, doi: 10.1109/ICIIECS.2015.7192976.
- [4] B. U. Umar, O. M. Olaniyi, A. B. Olatunde, A. A. Isah, A. K. Haq, and I. T. Ajayi, "A bi-factor biometric authentication system for secure electronic voting system," in *2022 IEEE Nigeria 4th International Conference on Disruptive Technologies for Sustainable Development (NIGERCON)*, Apr. 2022, pp. 1–5, doi: 10.1109/NIGERCON54645.2022.9803174.
- [5] N. B. Kintu and I. Z. Mohamed, "A secure e-voting system using biometric fingerprint and crypt-watermark methodology," in *ASCENT International Conference Proceedings – Information Systems and Engineering*, 2018, pp. 1–18.
- [6] M. K. Alhasnawi and A. S. Alkhalid, "Secure online voting using steganography and biometrics," *International Journal of Current Engineering and Technology*, vol. 7, no. 3, pp. 1097–1104, 2017.
- [7] N. P. Narayanan, C. S. Pradeep, P. Gulati, G. R. Bharath, and S. Nivash, "Design of highly secured biometric voting system," *International Journal of Engineering and Advanced Technology*, vol. 8, no. 5 Special Issue 3, pp. 111–114, Sep. 2019, doi: 10.35940/ijeat.E1028.0785S319.
- [8] B. U. Umar, O. M. Olaniyi, L. A. Ajao, D. Maliki, and I. C. Okeke, "Development of a fingerprint biometric authentication system for secure electronic voting machines," *Kinetik: Game Technology, Information System, Computer Network, Computing, Electronics, and Control*, pp. 115–126, Mar. 2019, doi: 10.22219/kinetik.v4i2.734.
- [9] D. G. Nair, V. P. Binu, and G. S. Kumar, "An improved e-voting scheme using secret sharing based secure multi-party computation," Feb. 2015, [Online]. Available: <http://arxiv.org/abs/1502.07469>.
- [10] N. R. Paulraj, G. Rajagopalan, M. Rajesh, S. V. Kiruthika, and I. Jasmine, "Smart voting machine based on fingerprints and face recognition," *International Journal of Engineering Research & Technology (IJERT)*, vol. 5, no. 9, pp. 1–4, 2018, doi: 10.17577/IJERTCONV5IS09009.
- [11] M. A. Zamir, D. A. Khan, and M. S. Umar, "Secure electronic voting machine using biometric authentication," in *2022 9th International Conference on Computing for Sustainable Global Development (INDIACom)*, Mar. 2022, pp. 511–516, doi: 10.23919/INDIACom54597.2022.9763202.
- [12] J. P. Thomas, K. R. S. N. Kumar, V. Addanki, A. Gupta, and N. Chaturvedi, "Hardware implementation of a biometric fingerprint identification system with embedded MATLAB," in *2010 International Conference on Advances in Recent Technologies in Communication and Computing*, Oct. 2010, pp. 155–157, doi: 10.1109/ARTCom.2010.79.
- [13] M. R. M. Isa, Y. H. Yahaya, M. H. M. Halip, M. A. Khairuddin, and K. Maskat, "The design of fingerprint biometric authentication on smart card for PULAPOT main entrance system," in *2010 International Symposium on Information Technology*, Jun. 2010, pp. 1–4, doi: 10.1109/ITSIM.2010.5561969.
- [14] A. M. Jagtap, V. Kesarkar, and A. Supekar, "Electronic voting system using biometrics, raspberry pi and TFT module," in *2019 3rd International Conference on Trends in Electronics and Informatics (ICOEI)*, Apr. 2019, pp. 977–982, doi: 10.1109/ICOEI.2019.8862671.
- [15] G. Deepa et al., "Biometric based voting system using aadhar database," in *2022 Second International Conference on Artificial Intelligence and Smart Energy (ICAIS)*, Feb. 2022, pp. 1071–1075, doi: 10.1109/ICAIS53314.2022.9743138.
- [16] N. Kate and J. V. Katti, "Security of remote voting system based on visual cryptography and SHA," in *2016 International Conference on Computing Communication Control and automation (ICCUBEA)*, Aug. 2016, pp. 1–6, doi: 10.1109/ICCUBEA.2016.7860071.
- [17] S. Ajish and K. S. AnilKumar, "Secure I-voting system using QR code and biometric authentication," *Information Security Journal: A Global Perspective*, vol. 31, no. 1, pp. 83–104, Jan. 2022, doi: 10.1080/19393555.2020.1867261.
- [18] J. I. Pegorini, A. C. C. Souza, A. R. Ortoncelli, R. T. Pagno, and N. C. Will, "Security and threats in the Brazilian e-voting system: a documentary case study based on public security tests," in *14th International Conference on Theory and Practice of Electronic Governance*, Oct. 2021, pp. 157–164, doi: 10.1145/3494193.3494301.
- [19] V. R. Ch, M. V. P. A, and B. S. S. A, "Arduino based electronic voting system with biometric and GSM features," in *2022 4th International Conference on Smart Systems and Inventive Technology (ICSSIT)*, Jan. 2022, pp. 685–688, doi: 10.1109/ICSSIT53264.2022.9716452.
- [20] F. Hazzaa and S. Kadry, "New system of e-voting using fingerprint," *International Journal of Emerging Technology and Advanced Engineering*, vol. 2, no. 10, p. 9, 2012.
- [21] N. Ashok, B. B. Teja, and A. Balakrishna, "RFID and fingerprint recognition based electronic voting system for real time application," *International Journal of Engineering Development and Research (IJEDR)*, vol. 2, no. 4, pp. 3850–3854, 2014.
- [22] S. K. Shaw, S. Poddar, V. Singh, and S. Dogra, "Design and implementation of Arduino based voting machine," in *2018 IEEE Electron Devices Kolkata Conference (EDKCON)*, Nov. 2018, pp. 450–454, doi: 10.1109/EDKCON.2018.8770474.
- [23] J. S. Manoharan, "A novel user layer cloud security model based on chaotic arnold transformation using fingerprint biometric traits," *Journal of Innovative Image Processing*, vol. 3, no. 1, pp. 36–51, Apr. 2021, doi: 10.36548/jiip.2021.1.004.
- [24] R. Patel, V. Ghorpade, V. Jain, and M. Kambli, "Fingerprint based e voting system using aadhar database," *International Journal for Research in Emerging Science and Technology (IJREST)*, vol. 2, no. 3, pp. 87–90, 2015.
- [25] S. Agarwal, A. Haider, A. Jamwal, P. Dev, and R. Chandel, "Biometric based secured remote electronic voting system," in *2020 7th International Conference on Smart Structures and Systems (ICSSS)*, Jul. 2020, pp. 1–5, doi: 10.1109/ICSSS49621.2020.9202212.

BIOGRAPHIES OF AUTHORS






Zakiah Mohd Yusoff    is a senior lecturer who is currently working at UiTM Pasir Gudang. She received the B.Eng. in Electrical Engineering and Ph.D. in Electrical Engineering from UiTM Shah Alam, in 2009 and 2014, respectively. In May 2014, she joined UiTM Pasir Gudang as a teaching staff. Her major interests include process control, system identification, and essential oil extraction system. She can be contacted at email: zakiah9018@uitm.edu.my.






Yusradini Yusnoor    was born in Malaysia who is currently pursue her studies as a undergraduate student majoring in Electrical Engineering at UiTM Cawangan Johor, Kampus Pasir Gudang. She can be contacted at email: yusradiniyusnoor@gmail.com.






Arni Munira Markom    is Senior Lecturer at the School of Electrical Engineering, College of Engineering, Universiti Teknologi MARA, 81750 Masai, Johor, Malaysia. She received her Ph.D. in Electronics (Photonics Engineering) from Universiti Malaya, Malaysia in 2016. She previously had a Masters in Microelectronics from Universiti Kebangsaan Malaysia and a Bachelor of Electronics (Computer Engineering) from Universiti Teknikal Malaysia Melaka, Malaysia. Her research areas are photonics technology, fiber lasers, fiber sensors and electrical engineering including microcontrollers and IoT devices. She can be contacted email: arnimunira@uitm.edu.my.



Siti Aminah Nordin    is a lecturer who is currently working at UiTM Pasir Gudang. She received her B. Eng. (Hons) of Electronic Engineering and Master's in electrical engineering from Universiti Teknologi MARA (UiTM) Shah Alam, in 2010 and 2014, respectively. In May 2014, she joined UiTM Pasir Gudang as a teaching staff. She is currently working towards the Ph.D. degree on microwave and radio frequency at Universiti Teknologi MARA Shah Alam, Malaysia. Her research interests include microwave filter, antenna, and electromagnetic wave. She can be contacted email: sitia181@uitm.edu.my.



Nurlaila Ismail    received her Ph.D. in Electrical Engineering from Universiti Teknologi MARA, Malaysia. She is currently a senior lecturer at School of Electrical Engineering, College of Engineering, Universiti Teknologi MARA, Malaysia. Her research interests include advanced signal processing and artificial intelligence. She can be contacted at email: nurlaila0583@uitm.edu.my.