Implementation of Secure Fingerprint Voting Machine

Manasa R
Department of Electronics and communication Engineering
Dayananda Sagar College of Engineering
Bengaluru,India
manasar.87@gmail.com

Dhananjay Natani
Department of Electronics and communication Engineering
Dayananda Sagar College of Engineering
Bengaluru,India
dhananjay22natani@gmail.com

Ekta Sinha
Department of Electronics and communication Engineering
Dayananda Sagar College of Engineering
Bengaluru,India
ekta2315sinha@gmail.com

Krati Sharma
Department of Electronics and communication Engineering
Dayananda Sagar College of Engineering
Bengaluru,India
krati10sharma@gmail.com

Narayan Kumar
Department of Electronics and communication Engineering
Dayananda Sagar College of Engineering
Bengaluru, India
narayansingh717@gmail.com

Navya Holla K
Department of Electronics and communication Engineering
Dayananda Sagar College of Engineering
Bengaluru,India
hollanavya@gmail.com

***Abstract*— This study develops biometric EVM authentication. Biometric information is finger print. This article uses Arduino Uno and various peripherals like GSM modules, fingerprint modules, LCDs, etc. to allow users to scan their fingerprints to confirm their eligibility. Acknowledgement Unit, the master unit, and Voting Machine Unit make up the system. Fingerprint Modules verify the Acknowledgement Unit. The memory unit has GSM and EEPROM chips. After identifying themselves, individuals can vote using a friendly geographical interface. Only if the voter is present can their fingerprint be confirmed and the OTP issued to their mobile phone, preventing false voters and enhancing security. As noted, writing processes end after voting. Instant vote counting makes voting efficient, rapid, and secure. GSM communication creates an OTP & gives the voter feedback after they vote and alerts the perform assigned of illicit voting. Two-step verification makes the system resilient and guarantees that our votes go to our preferred candidate.**

Keywords—voting machine, secure, fingerprint

I. INTRODUCTION

Elections play a crucial role in democratic societies, providing citizens with the opportunity to choose their leaders and shape their country's future. It is vital to ensure that the electoral process is fair, transparent, and trustworthy to maintain public confidence in democracy. Electronic voting machines (EVMs) have become increasingly popular in recent years, providing a faster and more efficient way to cast and count votes [1].

One type of EVM gaining popularity is the fingerprint-based voting system. This system uses biometric data, specifically the voter's fingerprint, to verify their identity and prevent fraud. Biometric verification is an important improvement over traditional EVMs, which rely on voter identification cards and can be susceptible to vote-rigging.

The fingerprint-based voting system uses a two-step verification process to confirm the voter's identity before allowing them to cast their vote. The system first scans the voter's fingerprint to verify their identity and then enables them to cast their vote electronically. This two-step verification process ensures that only eligible voters can cast their votes and prevents multiple votes from being cast by the same person.

Moreover, the fingerprint-based voting system can store attendance information for voters, which helps prevent voter fraud and ensures that all eligible voters can cast their votes. The system's collected data can be analyzed to provide insights into voter behavior and trends, offering valuable information for political analysis.

The development of a model for the fingerprint-based voting system represents a significant step towards a more transparent, reliable, and secure election process. By using biometric technology, the system can overcome many of the challenges associated with traditional EVMs and paper ballots, such as fraud and human error [2].

However, it is essential to note that implementing an electronic voting system requires careful planning and consideration [3-4]. The system's security and integrity must be thoroughly tested and verified to prevent it from being compromised. Additionally, the system must be designed to accommodate individuals who may have difficulty with fingerprint scanning due to disabilities or other factors.

In conclusion, the development of a fingerprint-based voting system is an important improvement in the electoral process. Biometric technology enables a more secure and efficient way for voters to cast their ballots. However, it is crucial to approach the implementation of such a system with caution and careful consideration to ensure its effectiveness and accessibility for all voters[5-7].

II. PREVIOUS WORK

A PAPER BALLOTS

Paper ballots were one of the oldest ways for voting in an election. Each voter may write their candidate's name on a simple sheet of paper that serves as the ballot. To ensure the privacy of votes, however, pre-printed ballots are utilized in elections for general bodies and governments. Each voter uses a single ballot, which is not pooled. A voter may place their ballot in a ballot box at a polling location. The term "ballot" refers to an organization's election process, like a trade union "holding a ballot" of it's own members.

Paper ballots have the disadvantage of requiring more paper and additional time to vote. In addition, it is not suited for the blind and requires extra time for counting. Also, it needs extra personnel for security.

B LEVER VOTING MACHINES

The voter enters lever voting equipment and pushes a lever to shut the curtain and release the voting levers. The polling officials then choose the relevant candidates or measures from a list of choices. The computer is set to avoid overvoting by shutting out some other candidates when the switch of one candidate is activated. After the voter has completed their vote and pushed the lever, the curtain will open and the proper counter for every candidate and measure will be incremented. After the completion of voting, the precinct officer writes the results by hand.

Nonetheless, lever voting devices have numerous disadvantages. Their voting method is complicated, and it takes longer to vote. No recounting of votes is feasible, and testing is costly. Full tests are highly uncommon and costly to transport and keep. In addition, they are difficult to test, complicated to manage, and insecure against vote fraud.

C PUNCHED CARDS

For recording votes, punched card systems use a card (or cards) as well as a tiny clipboard-like device. Voters punch holes on the cards according to their preferred candidate or ballot issue. After casting a vote, the voter may either deposit the ballot inside a ballot box or feed it through a computerised vote-tallying system at the precinct.

Unfortunately, punch card systems have a number of shortcomings. The system does not specify candidate names, secret voting is not allowed, and further protection is necessary.

D GSM MOBILE-BASED INTELLIGENT POLLING SYSTEM

The GSM mobile-based intelligent voting system enables people to vote using their GSM mobile handsets. Each voter's vote is sent as a message to the GSM receiver module. Each individual has a mobile ID that, similar to a voter ID, identifies the voter's identification. The election committee is responsible for providing the mobile ID. At the time of the election, whenever the person casts their vote, they send a text message to a GSM including their cellphone ID as well as the candidate's ID. The GSM modem gets the votes, which originate from the mobile equipment of the voter.

The individual who may create a SIM with the same number may cast fraudulent ballots. Likewise, if a voter loses their phone number, fraudulent voting is feasible.

III. PROPOSED METHODOLOGY

Secure electronic voting machines have been developed as an alternative to traditional paper-based voting systems. One such system is an electronic voting machine developed using the Arduino Uno microcontroller. This open-source single-board microcontroller is widely used for building digital devices, and has been programmed using the C/C++ language including some hardware libraries[12-17].

The system consists of two units: an Acknowledgment Unit (AU)/Control Unit, and a Voting Machine (VM). The AU is connected to a fingerprint sensor which is used to verify the identity of the voter. The system loads the fingerprint templates, candidate numbers (per respective template), and a list of candidate numbers with values initialized to zero, from on-chip EEPROM.

The system verifies the fingerprint of a voter and checks whether it is valid, and if so, whether the voter has already cast a vote. Once the voter is verified, the AU activates the VM after a credit check and then the voter casts a single vote. The system ensures that each voter can only cast a single vote, thereby preventing fraud.

After the voter has cast their vote, the candidate count is incremented and stored in the memory. This ensures that the vote is recorded accurately and securely, and that the election results are reliable.

One of the key advantages of this system is that it is more efficient than traditional paper-based voting systems. The system eliminates the need for paper ballots, which reduces the amount of time and resources required for counting and tallying votes. It also reduces the risk of errors and fraud associated with manual counting of paper ballots.

Another advantage of this system is that it is more secure than traditional paper-based voting systems. The use of biometric authentication (fingerprint sensor) ensures that only authorized voters are able to cast a vote. Additionally, the use of digital storage (on-chip EEPROM) ensures that the votes are stored securely and are not vulnerable to tampering or manipulation.

In conclusion, the development of secure electronic voting machines using microcontrollers such as the Arduino Uno has the potential to revolutionize the way elections are conducted. By improving efficiency and security, these systems can help to ensure that elections are free, fair, and transparent.

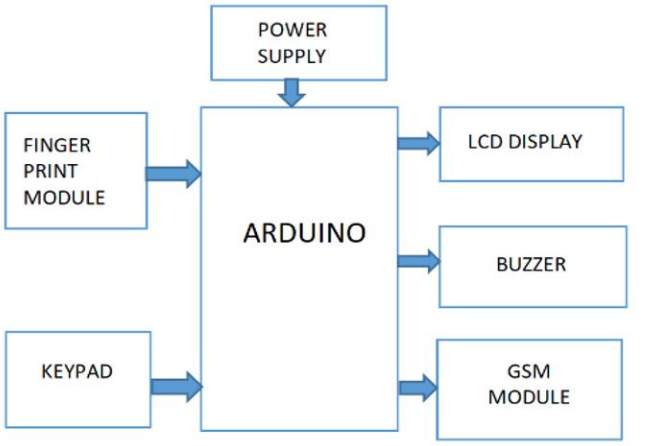

Figure1: Block – diagram of the proposed secure fingerprint voting machine

Block 1 provides the information about the connection of the Arduino board to other hardware components.

Block 2 gives the information about the connection of the fingerprint module with the Arduino board. It shows that the data is fed from the fingerprint module to the board for further processing.

Block 3 shows the connection of the Arduino board to the LCD. The data is processed on the Arduino board and the result gets displayed on the LCD.

Next, block 4 shows the connection between the keypad and the board. The OTP is entered by the user with the help of this keypad.

Block 5 gives the connection between the GSM module and the Arduino board. GSM will receive the command from the Arduino to send OTP and other notifications to the users.

Other blocks are Power Supply Unit, to provide power to the Arduino board, hence to the whole system, and a Buzzer to produce an alerting tone. It can be particularly useful in areas

where resources are limited, and high-end equipment may not be available.

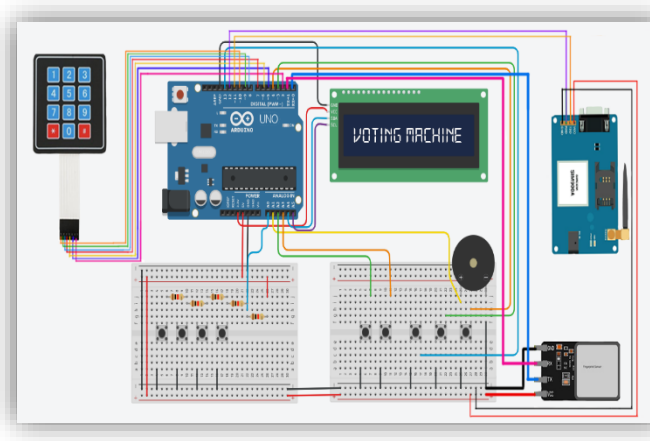

Figure 2: Circuit Diagram

IV. Working Principle

The overall working principle of proposed work is the two-step verification of a user/voter to cast his/her vote at the time of voting. The two-step verification, fingerprint matching & OTP verification, reduced the chances of duplicity and rigging of votes.

V. Algorithm: -

Step 1: The first step is to enroll the fingerprint id of the voter before the voting process starts.
Step 2: After successful enrollment, the voting process will begin. At the time of voting the first, the fingerprint of the votes will be matched with the previously stored fingerprint database created.
Step 3: Next, check if the user has already cast the vote or not. If yes, do not let them proceed, if not, then proceed to the next step.
Step 4: Now, the user should receive an OTP (using GSM) which he/she should enter correctly to be able to cast their vote.
Step 5: After both the verification steps, the voter can now cast their vote among the three candidates and after complete voting, the Result can be displayed on LCD.
NOTE: All the messages and instructions for the voter will be shown on the LCD.

VI. Flow-chart

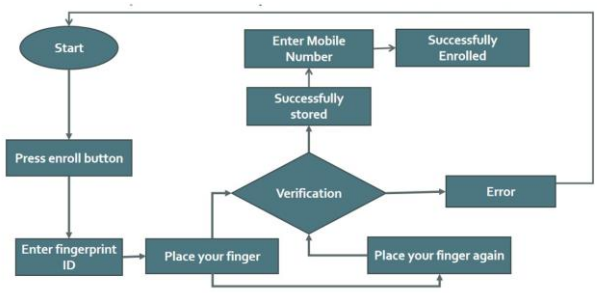

Figure 3 Flow-chart for Enrollment

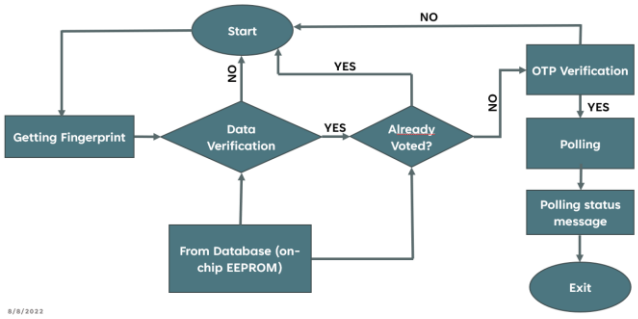

Figure 4 Flow-chart for System (Methodology)

Firstly, after starting the system the voter would have to scan his fingerprint on the fingerprint sensor.
The fingerprint scanned will be matched with the fingerprints stored in the enrollment process (done before the voting process) at the data verification stage. If the fingerprint matches then the user will be allowed to move on to the next stage. Otherwise, if the voter's fingerprint does not match, the system will go into an Exit state.
Next, after successful verification of the fingerprint, the system will check whether the voter has already cast his/her vote or not. If yes, the system will go into the Exit state. Otherwise, the voter will move on to the OTP verification stage.
After the verifications mentioned above, the voter will now receive a 5-digit OTP on his registered mobile number which he would have to enter correctly in the system using the keypad. If the voter has entered the correct OTP, he will now be able to cast his vote for one of the candidates of his choice. Otherwise, the system will go into an Exit state.
After all the voting has been done, the results will be displayed on the LCD and the voters will receive a message for the same.

VII. Hardware

A. *Hardware Used: -*

Arduino UNO — Arduino UNO is an ATmega328P-based microcontroller board. It contains 14 digital input/output pins (six of which can be utilized as PWM outputs), 6 analogue input, a 16 MHz ceramics resonator, a USB port, a power connector, an ICSP header, and a reset button. It includes everything required to operate the microcontroller; just connect it to a PC through USB or power it with an AC-to-DC converter or batteries to get started. You can tamper with a UNO without excessive concern about making a mistake; in the worst case situation, you may replace the chips for a few bucks and start again.

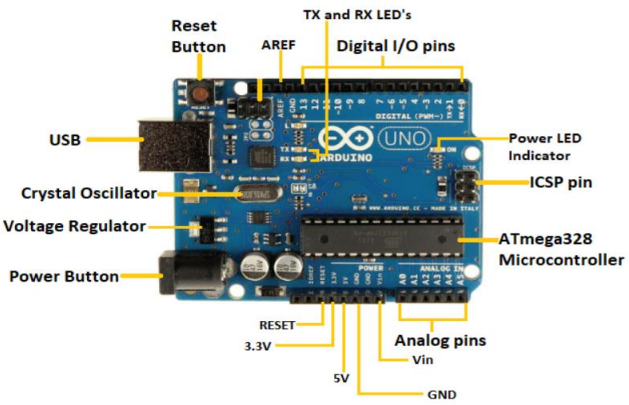

Fig. 5 Arduino UNO

Table 1: Arduino Uno Specifications

Board	Name	Arduino UNO R3
	SKU	A000066
Microcontroller	ATmega328P	
USB connector	USB-B	
Pins	Built-in LED Pin	13
	Digital I/O Pins	14
	Analog input pins	6
	PWM pins	6
Communication	UART	Yes
	I2C	Yes
	SPI	Yes
Power	I/O Voltage	5V
	Input voltage (nominal)	7-12V
	DC Current per I/O Pin	20 mA
	Power Supply Connector	Barrel Plug
Clock speed	Main Processor	ATmega328P 16 MHz
	USB-Serial Processor	ATmega16U2 16 MHz
Memory	ATmega328P	2KB SRAM, 32KB FLASH, 1KB EEPROM
Dimensions	Weight	25 g
	Width	53.4 mm
	Length	68.6 mm

Fingerprint Module (R307) - R307 Fingerprint Module consists of an optical fingerprint sensor, a high-speed DSP processor, a high-performance fingerprint alignment method, high-capacity FLASH chips, and certain other hardware and software components, has stable performance and a simple structure, and is equipped with fingerprint entering, image processing, matching, search, and template storage, among other capabilities[18-21].

Figure 6 Fingerprint Sensor

Table 2: Fingerprint Sensor Specifications

Operating voltage (v)	4.2 ~ 6 VDC
Current consumption	≤75mA
Verification Speed	0.2 sec
Scanning Speed	0.3 sec
Character file size	256 bytes
Template size	512 bytes
False Acceptance Rate (FAR)	≤0.0001%
False Rejection Rate (FRR)	≤0.1%
Resolution	500 DPI
Operating Temperature	-20 ~ +50 °C
Length (mm)	46
Width (mm)	21
Height (mm)	23.5
Weight (gm)	20
Shipment Weight	0.022 kg
Shipment Dimensions	13 × 11 × 6 cm

16x2 LCD Display (WH1602B1) - Winstar WH1602B is among the most widely used varieties of 16x2 character LCD modules on the market. The default interface of the WH1602B 16x2 LCD type is a 6800 4/8-bit parallel

connection. Model no. WH1602B1 has a 4-line SPI interface, whereas model no. WH1602B3 has an I2C interface.

Table 3: LCD Specifications

Backlight Type/Color	Transmissive/white
Character Display Format (Chars. x Lines)	16 x 2
Character or Graphic Display	Character
Graphic Display Format	N/A
LCD Type	VATN
Operating Mode	Negative mod

Figure 7 LCD Module

GSM SIM 900A - SIM900A It is constructed using SIMCOM's Double Band GSM-based SIM900A modem. It operates on 900MHz frequencies. SIM900A can automatically scan these two bands. AT Commands may also be used to set the frequency bands. The baud rate is changeable through AT command between 1200 and 115200. SIM900A is a wireless, ultracompact module. Interface for connecting a PC together with a controller using RS232 Chip (MAX232)is forthcoming.

Figure 8 GSM Module

Table 4: GSM Module Specifications

GSM/GPRS Specification	
GSM/GPRS Module	SIM900A
Frequency	900MHz/1800MHz
Modem Interface	RS232 Serial Interface
Baud Rate(Default factory)	9600bps
Power requirement	4.5V to 12V
Current requirement	<590mA
SIM900A module operating temperature	-40°C to +85°C
Weight	40g

Other Hardware Components Used: -
LEDs
Push Buttons
On/Off Switch
Piezo Speaker/Buzzer
Wires and 9V batteries
Resistors

B. Software: C++ on the Arduino - The proposed work is built using the Arduino IDE which requires the code to be written in C++ programming.

VIII. WORKING

- Firstly, a database will be created for all the voters which will include their respective fingerprints and mobile number.
- The process of registering the users is done by pressing the enroll button and then entering the voter id.
- The voter will be prompted to place his/her finger on the fingerprint sensor 2 times for accuracy.
- After successfully storing the fingerprint, the user will be told to enter his/her mobile number. The user can enter the mobile number using the keypad provided.
- This will complete the registration process.
- Next comes the voting day.
- At the time of voting, the voter will first have to press the match button provided to start the system for voting.
- After pressing the match button, the LCD will prompt the voter to place his finger on the sensor to match the fingerprint within the database.
- If the fingerprint matches perfectly, the voter can proceed to the next step if he/she has not voted already before. This will be checked by the system.
- If the system does not find any match for the fingerprint in its database, the voter will not be allowed to vote.
- After fingerprint matching and the checking of vote status of the current voter, the system will send an OTP to users registered mobile number using the GSM module[22,23].
- The voter will be told to enter the OTP received on his/her mobile using the keypad.
- The system will check whether the OTP entered is correct or not.
- If the OTP is correct and verified the user will now be allowed to cast his/her vote to the candidate of choice. But if the entered OTP does not match then the system will reset again for the particular voter and he/she won't be allowed to cast his/her vote.
- After the OTP verification, the user can cast the vote using the push buttons provided to vote for the candidate of choice., and the vote count for the particular candidate will increment in the system.
- After all the voters have cast their votes, the results of the voting can be shown on the LCD using the RESULT button present on the system.

IX. Results and Discussions

The connections were made according to the circuit diagram and a working circuit was implemented using Arduino Uno and other interactive components. The code to implement the voting machine was developed providing a two-step verification of all the voters. A database was created containing the fingerprints and their respective mobile numbers during the registration process with complete honesty.

At the time of voting, the fingerprint of each voter was matched from the database thereby giving the first step of verification. Also, it was successfully checked whether the voter has already cast his/her vote or not.

Next, the OTP was generated and sent to the registered mobile number successfully which was used for the second verification step. Finally, the vote casting was done with complete security and integrity.

The result of the voting and all the other instructions and messages were displayed using the LCD.

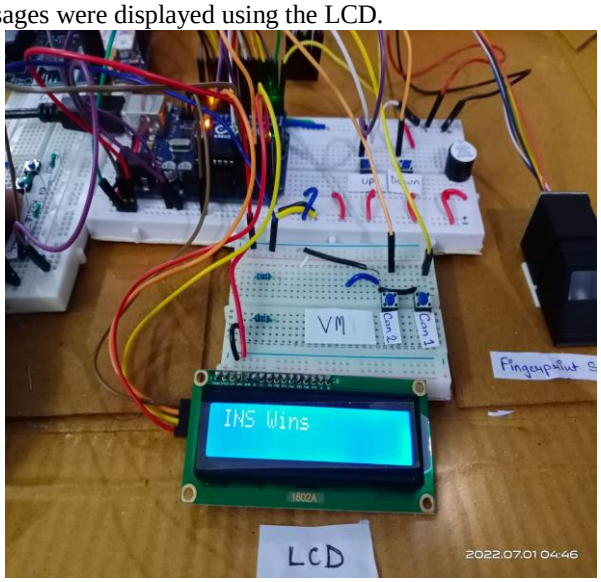

Figure 9 Voting Results

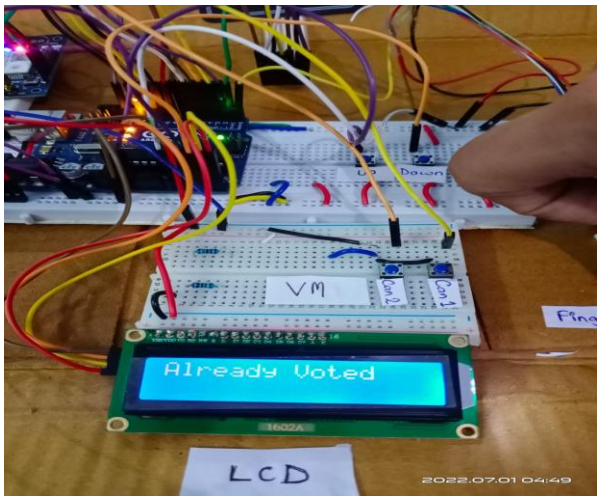

Figure 10 User Trying To Cast Vote Again

The proposed system was able to meet the expected outcomes: Recording and Creating a Database (Enrolment): The database was created consisting of Fingerprints and mobile numbers of the populous along with their respective ID.

Two–Factor Authentication: During the voting procedure, the fingerprints were successfully verified[24,25]. Thereafter, for two-factor authentication, an OTP was sent to the voter's Registered Mobile Number. On successful verification of OTP, the voter was allowed to cast their vote.

Successful Polling Action: After casting the vote, the user was denied access to the voting system, in case he/she attempts to recast the vote.

Successful Result Generation: After successful completion of the voting procedure, the result was computed and successfully displayed on the LCD screen.

X. Conclusion and Future Work

Conclusion: - Fingerprints have been among the most widely used ways for human identification for more than a century; automated biometric systems are only accessible for the last few decades.

This work is implemented and assessed effectively. The findings obtained were substantial and similar. It demonstrates that the fingerprint image enhancement phase will increase the performance of the fingerprint-based identification system's verification process.

Since fingerprints are widely accepted by the public at large, law enforcement, and the forensic scientific community, they would continue to be used in many governments' legacy applications and will be included into future systems for applications that need a trustworthy biometric.

This biometric voting method will allow India to have fair elections.

This will prevent illicit activities such as rigging. Citizens may be certain that only they can pick their leaders, therefore exercising their democratic prerogative.

Future Work: The fingerprint module's memory may be increased. A 1mb flash storage fingerprint module may be used to increase capacity.

Larger external memory (EEPROMs) may be used to store the fingerprint picture, which can be retrieved later for comparison.[26]

Adding a Smart Card have the to the current module is intended to increase security and save database storage. The smart cards may augment the n-factor authentication and replace the OTP procedure.

It is possible to include audio output in different languages to make the vote or polling process more user-friendly for illiterate voters.

In addition, retinal scanning may be enhanced to making the system safer and resilient.

REFERENCES

[1] Ashok Kumar D., Ummal Sariba Begum T., "*A Novel design of Electronic Voting System Using Fingerprint*", International Journal of Innovative Technology & Creative Engineering (ISSN:2045-8711),Vol.1,No.1. pp: 12 19, January 2011.

[2] California Internet Voting Task Force. "*A Report on the Feasibility of Internet Voting*", Jan.2000.

[3] D. Balzarotti, G. Banks, M. Cova, V. Felmetsger, R. A Kemmerer, W. Robertson, F. Valeur, and G. Vigna, "*An Experience in Testing the Security of Real-World Electronic Voting Systems*," IEEE Transactions on Software Engineering, vol. 36, no. 4, 2010.
[4] R. Hite, "*All Levels of Government are needed to Address Electronic Voting System Challenges*," Technical report, GAO, 2007.
[5] Madhura Anil Joshi, Kajal Vijay Patil, Dr. P. G. Poonacha *Mobile Based Facial Recognition Using OTP Verification for Voting System*, International Conference on Computational Intelligence and Networks (CINE 2015), 978-1-4799-8047-5/15/$31.00c.
[6] Oluwafemi O. Oni, Funso A. Iyanda, John O. Itiola *"E-Voting System with Physical Verification Using OTP Algorithm"*, 2015 International Journal of Hybrid Information Technology Vol.8, No.8 (2015), pp.161-166.
[7] R. Alaguvel G. Gnanavel "*Offline and Online E-Voting System with Embedded Security for Real Time*" International Journal of Engineering Research (ISSN: 2319-6890) vol. 2 no. 2 pp. 76-82 April 2013
[8] N. Al-Nuaimi, A. Al-Suwaidi and A. Al-Ali, "*A secure e-voting scheme based on fingerprint biometrics and elliptic curve cryptography*," Journal of King Saud University - Computer and Information Sciences, vol. 28, no. 1, pp. 1-10, 2016. doi: 10.1016/j.jksuci.2015.04.001.
[9] A. Ayyub and M. S. Hossain, "*A secure e-voting system using fingerprint biometric authentication*," IEEE Access, vol. 6, pp. 71684-71696, 2018. doi: 10.1109/ACCESS.2018.2882918.
[10] H. Baliyan and A. K. Gupta, "*A secure and efficient e-voting system using biometric authentication*," International Journal of Computer Science and Information Security, vol. 15, no. 2, pp. 141-150, 2017.
[11] R. K. Bhoi, K. K. Das and P. K. Jana, "*A novel biometric security protocol for electronic voting machines using fingerprints*," Journal of Ambient Intelligence and Humanized Computing, vol. 7, no. 3, pp. 383-391, 2016. doi: 10.1007/s12652-015-0349-8.
[12] S. Chandrasekaran, C. Velayutham and S. Sundaram, "*An efficient and secure e-voting system using biometric authentication*," Procedia Computer Science, vol. 132, pp. 1087-1096, 2018. doi: 10.1016/j.procs.2018.05.166.
[13] M. Chawla and V. Sharma, "*A secure e-voting system using biometric authentication*," International Journal of Computer Applications, vol. 111, no. 1, pp. 19-23, 2015. doi: 10.5120/19647-5802.
[14] A. Deshpande, P. Kulkarni and P. Kshirsagar, "*An enhanced fingerprint based secure electronic voting system*," Journal of King Saud University - Computer and Information Sciences, vol. 29, no. 2, pp. 156-163, 2017. doi: 10.1016/j.jksuci.2016.03.001.
[15] S. Goel and A. Sharma, "*Secure e-voting system using fingerprint biometric authentication*," Journal of Advanced Research in Dynamical and Control Systems, vol. 9, no. 8, pp. 878-885, 2017.
[16] A. E. Hassanien and M. M. Fouad, "*A secure e-voting system using fingerprint biometric authentication*," Journal of Computer and Communications, vol. 3, no. 4, pp. 131-142, 2015. doi: 10.4236/jcc.2015.34018.
[17] M. Y. Javed and M. Z. Iqbal, "*A secure electronic voting system based on biometric authentication*," Journal of Information Security, vol. 8, no. 3, pp. 161-171, 2017. doi: 10.4236/jis.2017.83011.
[18] S. Kaur and B. Singh, "*Design and implementation of secure e-voting system using fingerprint recognition*," International Journal of Computer Science and Network Security, vol. 17, no. 8, pp. 43-50, 2017.
[19] A. Khurana and D. Singh, "*Secure electronic voting system using fingerprint authentication*," International Journal of Computer Science and Information Technologies, vol. 7, no. 1, pp. 145-148, 2016.
[20] D. W. Kim, J. W. Lee, and H. K. Kim, "*A secure e-voting system using fingerprint biometric and visual cryptography*," Multimedia Tools and Applications, vol. 76, no. 7, pp. 9469-9485, 2017.
[21] D. Kumar and S. Kumar, "*A secure e-voting system using fingerprint authentication and AES encryption*," International Journal of Advanced Research in Computer and Communication Engineering, vol. 6, no. 3, pp. 321-326, 2017.
[22] M. N. Kumbhar, A. B. Kharat, and V. M. Jadhav, "*A secure e-voting system using biometric authentication and blockchain technology*," International Journal of Pure and Applied Mathematics, vol. 119, no. 12, pp. 2291-2300, 2018.
[23] K. J. Lee, Y. H. Park, and H. K. Kim, "*A secure e-voting system using biometrics and visual cryptography*," Journal of Computational and Theoretical Nanoscience, vol. 13, no. 12, pp. 9535-9540, 2016.
[24] M. Masood, F. Siddiqui, and M. S. Shamsi, "*A secure e-voting scheme based on fingerprint biometrics and elliptic curve cryptography*," International Journal of Computer Applications, vol. 150, no. 5, pp. 10-16, 2016.
[25] M. Mustafa, H. Zafar, and F. Mushtaq, "*A secure e-voting system using biometric authentication and AES encryption*," Journal of Electronic Imaging, vol. 27, no. 4, pp. 1-8, 2018.
[26] M. S. Uddin, A. Ullah, and M. A. Kabir, "*A secure e-voting system based on fingerprint authentication and visual cryptography*," Journal of Theoretical and Applied Information Technology, vol. 95, no. 10, pp. 2297-2309, 2017.