IoT Based Voting System with Fingerprint Verification

K. Vidhya[1], K. N. Keerthana Raj[2], R. Naveen Kumar[3], Nishchal Shekar[4], H. R. Nithish[5*]

[1]*Assistant Professor, Department of Information Science and Engineering, East West Institute of Technology, Bangalore, India*
[2,3,4,5]*Student, Department of Information Science and Engineering, East West Institute of Technology, Bangalore, India*

Abstract: **The use of an IoT-based voting system with fingerprint verification ensures that voting is secure and that malpractice is reduced. The voter's information, including their fingerprint, is saved in a database. If the fingerprint matches one in the database, the system checks the user's data and, if they are authenticated, checks for multiple votes. If the fingerprint match is incorrect, the message "Record doesn't exist" will appear. The controller is an Arduino Uno, and the user is authenticated using a fingerprint sensor. When a misbehaviour occurs, the notice "Currently casted a ballot" will appear. The Arduino IDE is used to programme the device, and the cloud is used to display the voting form card and to collect data.**

Keywords: **Arduino Uno, Fingerprint Sensor-R305, Node MCU, LCD display, Buttons.**

1. Introduction

Elections were a distinguishing characteristic of democratic government; a discretionary framework is a set of principles that regulate how decisions and mandates are made and are not completely predetermined. Although non-political races may occur in companies, non-benefit associations, and casual associations, legislative discretionary frameworks were in charge of political discretionary frameworks. There were numerous electoral systems in use around the world. Paper polling forms, punch cards, and Optical Mark Sense Ballots were all used at the time. A few discretionary frameworks choose a solitary victor for a unique position, for example, state head, president or governor, while others choose numerous champs, like individuals from parliament or sheets of chiefs.

An electronic voting mechanism that uses human biometrics is the finger impression casting a ballot framework. It reduces the number of people needed and the amount of time it takes to conduct a survey.

In all of the nation's voting, the feature was accomplished. We were promoting a new method of voting in order to build a way of life for that aim. Votes may be physically counted under the existing structure, which raises the potential of errors such as duplicate counting and altogether missing counting.

Votes are sometimes manipulated and influenced by ideological groupings, resulting in incorrect ballot casting and mutilating the outcomes of political races for specific up-and-comers. This device is useful since it is easy to use, reliable, and precise. One of the most important aspects of a political campaign is the counting of votes. Because failure to complete the count may have an impact on people's sentiments about the existing administration, political decision counting should be straightforward, exact, and dependable; only then will the public have faith in the elections. Each polling station maintains a list of all electors assigned to it, and only those on the list are permitted to vote there. A simple electronic device that can be used to register votes is the Electrical Voting Machine. There were two distinct sorts of voting systems in use on the planet at the time, for example, Distance casting a ballot and Presence casting a ballot. In distance casting a ballot elector cast their vote from a spot other than a surveying stall for example by means of mail or web casting a ballot.

As a result, the foundation of mechanised e-casting, a ballot framework where political decision information is recorded, stored, and managed as digital information in the modern period, was security, secrecy, unchanging quality, and precision. E-voting security was graded on a scale of one to ten. At the time of voting, fingerprint detection can be used to authenticate the online voting process. Because National identification is a primary key of the system, it will make the system more secure by utilising the National identity card number, which is unique for each person, ensuring that no duplicate votes are cast. This system can be used with a login that requires the candidate's name, national identity card number, and fingerprint scan. Voters who are eligible to vote

Objective of the Research: The client is required to give a fingerprint at the surveying corner for the finger imprint casting a ballot project. To plan this application, the task makes use of fingerprint technology and Arduino systems. The main goal of this project is to provide a framework that requires clients to show their fingerprints as confirmation of identity. The framework examines the information from the Fingerprint and verifies it, after which it is saved in the data collection. The framework allows the individual to make their option if the offered subtleties match the data set facts. If the submitted Fingerprint information does not match what is stored, the system immediately triggers the feature, allowing security professionals to intervene and make the necessary modifications.

Background of the Research: This experiment was done out with the Arduino. The framework reads the data from the

Fingerprint module, compares it to the data stored elsewhere, and then proceeds to the next step. The Arduino, Fingerprint module, and pushbuttons are all used to build the framework.

The Arduino is control by program utilizing C/C++ to permit the connection point with the Fingerprint Module, the Arduino regulator checks this information with the generally existing information in the regulator's memory and afterward execute the orders coordinated by the regulator segment.

2. Existing System

Political race is the demonstration of party projecting votes to choose on person for a place of some sort or another. Political decision may include a public or confidential vote contingent upon the position. Most situation in the neighbourhood, state, and federal states are deciding on in an appointment of some sort or another. In paper-based decisions, electors cast their votes by just keeping their polling forms in fixed boxes disseminated across the discretionary circuits around a given country. Whenever the political race time frame closes, this multitude of boxes are opened and casts a ballot are included physically in presence of the ensured authorities. In this interaction, there can be mistake in including of votes or at times electors track down ways of casting a ballot at least a time or two. At times casts a ballot are even controlled to mutilate the aftereffects of an political decision in favour of certain competitors.

In 21" century society where electronic innovation is developing at a steadily expanding rate, it is hard to comprehend the reason why states were not changing over their paper based political race frameworks to electronic structure to insurance "One Person-One Vote and to wipe out misrepresentation and debasement.

3. Introducing New Direction

To address the concerns raised by the use of paper polling forms and to incorporate security techniques aimed at uncovering extortion and outrage while ensuring "One Person - One Vote," an electronic democratic framework must be implemented totally. Instead of using paper, this architecture would display voting forms on a television screen. Help screens would be available to voters by simply pressing a button, ensuring that all critical polling form fields have been correctly filled out, eliminating information section disappointments or votes wasted due to indecipherable handwriting or blunders. In general, you should ensure that the citizen is who they claim to be, rather than a name found in a nearby cemetery or on the internet.

4. Proposed System

The proposed framework connected variant electronic based finger impression Using Arduino, create a voting framework. In this context, use unique finger impression confirmation and the point of interaction acknowledges elector's public ID card number, gives a connection point to vote and display affirmative status or error messages Fingerprints are used for confirmation since they are faster and more accurate than other

biometric data and are widely used in the movement framework. In here, there could be a devoted group for this framework in the political race offices. Cuts off were put at far off area from the boll corners. They were accustomed to completing of the handling work, for example, unique mark handling, picture handling, moving information exchanged between the client and the data set, reports generated, and messages sent to voters

There is a focal information base contains all the segment and biometric information of each and every residents of India. To decrease load on the focal information base there were sub data sets in each area political race office that will be situated close by the servers which will contain duplicates of information of the resident that under in locale all the sub data sets recover information from focal data set just these individuals who go under its degree. The information is occasionally refreshed and is put away in unpredictable structure so it tends to be eradicated if and when fundamental sab data sets will recover just the information that is connected with the democratic interaction and bar all their unimportant in line.

These data bases will be used to generate reports and analyse the discretionary cycle's outcomes. These databases make it possible to allow citizens to vote from anywhere as long as they are within discretionary circuits.

To verify an individual, expect them to have a substantial No. of National Identity Card The number will be verified nearby data set first it is found then it will look through the focal data set. In the event that individual's number isn't found in the focal information base, then individual will be without any trace of faking part in the democratic cycle then again in the event that the number is available in the focal data set, the information of that individual will be stored to the sub data set.

This record is removed from the neighbourhood information base and shipped off au then, at that point, focusing servers for far their interaction for check the individual's unique mark will be examined at the client side and coordinated balanced at the servers with the information infracted from the nearby data set.

Advantages of Proposed System:
- It improves security performance.
- It avoids forgery.
- Due to compact size, it can be easily transported to different places.
- Power consumption and man power is less.

5. Design of Concept

The Fingerprint Voting System (FVS). Since the premise of any democratic framework is "One Person - One Vote", it makes sense that should confirm that a citizen is who they guarantee to be and that they have not recently casted a ballot in that frame of mind at another site (to wipe out twofold democratic) The fundamental reason for unique finger impression casting a ballot framework is to "Forestalling Fraudulent Voting This framework has essentially 5 sorts of modules. They are:
- Fingerprint enrolment
- Fingerprint verification

- Cast the vote
- Monitor for erroneous votes
- Create the final report

Identical mark Because it considers an auditable, simple, and secure contact, voting races indicate that people may trust the results. It also lowers the likelihood of human error. Individuals can acquire official political decision outcomes in almost no time thanks to finger imprint voting and electronic counting. instead of weeks. Once more, this forms trust Technology will be a helpful approach to further developing citizen schooling and enrolment, to build commitment and elector turnout It is truly adept at making casting a ballot more available, meaning it's simpler for impair individuals to autonomously vote.

One reason this Finger print casting a ballot framework has been praised so exceptionally is that planned around the thought all gatherings, residents and political race commissions had the option to review the appointive interaction at each stage, including before a political decision has even started.

Citizen can cast a ballot the up-and-comer just a single time, the framework won't permit the contender to decide in favor of the subsequent time. The quantity of up-and-comer added to the framework by the administrator will be consequently erased after the finish of the political decision. Individuals can't abuse their votes.

This Fingerprint casting a ballot machine utilizing Fingerprint is principally an Arduino framework that makes the things simple in the surveying stalls during the political decision time. The client, who needs to survey their vote, needs to present the character evidence at the counter at the surveying stall. In the exploration project, the client no requirements to convey with their adequate material and citizen card. Citizen card is only Fingerprint which stores the subtleties of the individual like the name of the client, address, public personality card number, versatile number for contact and so forth.

When the political decision time surveying stops power unit is turned on, the polling form unit displays its "welcome to casting a ballot" message on LCD, indicating that the machine is ready and waiting for citizen input. The activity is controlled by the client using the press buttons.

Fingerprint Enrolment: First time elector saves their unique mark in enrolment handling. Assuming selecting mode, order is given, the regulator hangs tight for input and enacts the scanner to acknowledge the finger impression, showing "Enlist a unique finger impression!" on the LCD show. The applicant's unique mark is checked and convert picture in the initial time place the finger. Then, for the second time, ask the citizen to place a similar finger on a special format and compare it to the initial output's coordinates. The two prints were then matched and stored in the given id. This intriguing id is saved in the regulator's Fingerprint module memory for future reference. The framework is ready for voting after all enrolments have been completed.
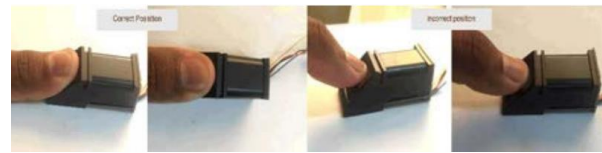

Fig. 1. Fingerprint enrolment

Fingerprint Verification: Before the vote projecting citizen needs to check for legitimacy to the democratic During this time for confirmation "Output your finger," the voter is asked after his or her unique finger impression is checked and compared to the fingerprints previously registered for the memory. If all goes well, the message "Cast your vote" will be displayed on LCD screens. If the finger impression does not match the currently preserved memory, the LCD displays "Didn't coordinate!" and the user is not allowed to cast a ballot projecting. Assuming the citizen has previously cast a ballot, the unique finger impression will be synchronised and displayed on the LCD with the words "Currently casted a ballot!" and a red light will be turned on.
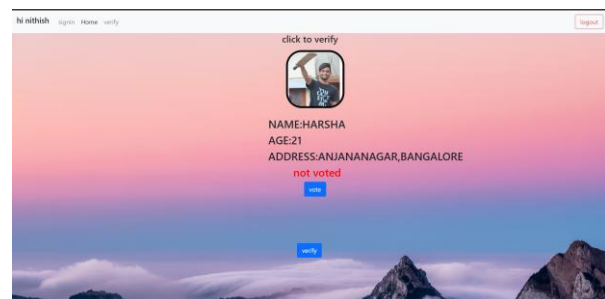

Fig. 2. Fingerprint verification

Cast the Votes: Following the check, the elector is entitled to cast a ballot, with the primary button crammed inside five buttons that appear for party selection; if a person selects a party, he or she is unable to select another party. The candidate must next choose which party to join after hitting three buttons inside another five fasteners. The LCD displays the message "No Access" if an elector hits the party selection button more than once and the applicant selection button more than three times. The pressed buttons are not counted.
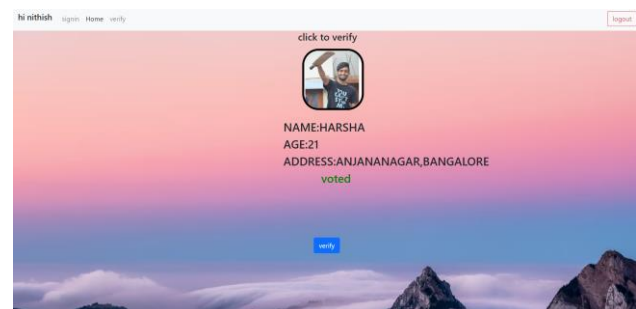

Fig. 3. Cast the vote

Generate Final Report: The democratic vote was counted using the report button squeezed after completing vote projections to ascertain who won and which party won in the political option. The framework has a report produce button

inside the crate to address the security issue. It is only accessible to administrators. In the aftermath of getting the system back up, all information was erased from the machine once the political campaign was completed.
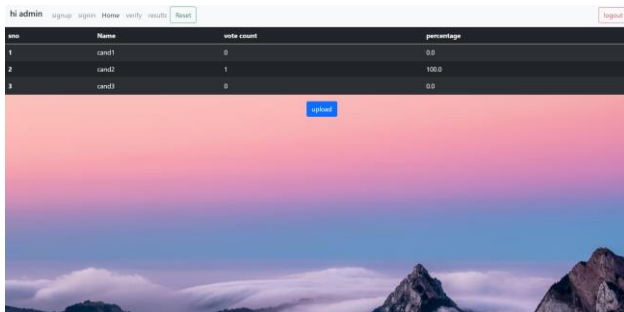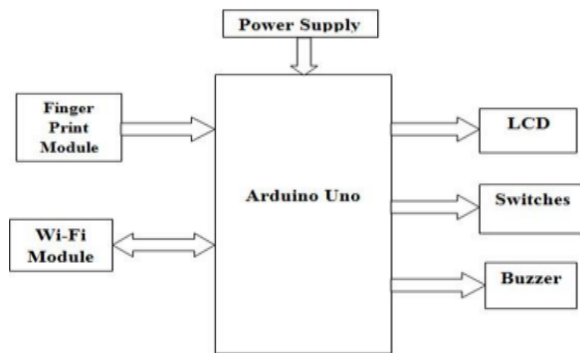

Fig. 4. Final report

Fig. 5. System architecture

Algorithm of Fingerprint Voting System:

Step 1: Begin

Step 2: Examine your index finger.

Step 3: Make sure your fingers are in sync.

Step 4: A match has been found.

Step 5: Place your ballot.

Step 6: Select a button from the list of parties.

Step 7: Choose a party

Step 8: Select three candidates from the drop-down menu.

Step 9: Choose a candidate

Step 10: Your Vote Has Been Accepted

Step 11: Put an end to it.

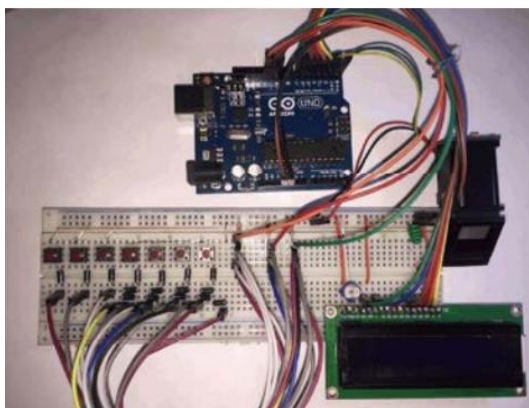Fig. 6. Circuit connection

A. Arduino Uno

Because of the ATmega328, the Arduino Uno is a microcontroller board (Figure 7). It features 14 computerised input/yield pins, six simple information sources, a 16 MHz precious stone oscillator, a USB connector, a power space, an ICSP header, and a reset button. It comes with everything you'll need to get started with the microcontroller; simply connect it to a PC via USB or power it with an AC-to-DC adapter or battery. The Arduino differs from previous sheets in that it does not make use of the FTDI USB-to-chronic driver chip. In the end, it incorporates an Atmega8U2 that has been adapted as a USB-to-chronic converter.

Fig. 7. Arduino Uno

B. Fingerprint Module

Finger impression module is an information gadget that captures an advanced image of the unique mark design and is used for Unique mark processing. Finger impression enrolment and coordination are both unique (the matching can be 1:1 or 1: N). The client must enter the finger twice when selecting. The framework will handle double cross finger images, construct a finger layout based on handling outcomes, and save the format. A live filter is a picture that has been captured. This real-time output is carefully processed into a biometric that is stored and used for coordination. When coordinating, the customer places his or her finger on an optical sensor, and the framework creates a finger format and compares it to other forms.
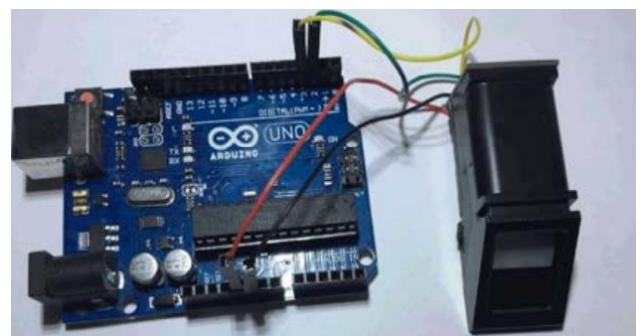

Fig. 8. Fingerprint module

C. LCD Display

The LCD show includes an LED backdrop and can display two columns with up to 16 characters each. On the showcase, you can see the square shapes of each person as well as the pixels that make them up. The showcase is white on blue and is

designed to display text. The LCD panel serves as a point of engagement between the client and Arduino, displaying messages such as when to register and vote, as well as whether or not their vote is valid. It also displays "welcome" messages at first and "spot your finger" messages during enrolment, "recognising" messages when the regulator compares the information base to see if the client is valid or not, and "if significant" displays "if significant."

Fig. 9. LCD display

D. Node MCU

Opensource prototyping board plans are available for NodeMCU, an opensource firmware. The term "Node MCU" combines the terms "hub" and "MCU" (miniature regulator unit). The firmware as well as the prototyping board plans are both free source. NodeMCU is a LUA-based open-source firmware for the ESP8266 Wi-Fi chip. NodeMCU firmware is included with the ESP8266 Development board/pack, such as the NodeMCU Development board, to investigate its utility with the ESP8266 chip. The programming model for NodeMCU is similar to Node.js, but in Lua. It's unique and tailored to the occasion. As a result, many capacities have callback capacity limits.

Fig. 10. Node MCU

6. Implementation

The fingerprint module is utilized to recognize the finger impression of the citizen. The centralized data set gives the information of the elector alongside his fingerprint. The programming module is utilized to check the citizen in light of the fingerprint received by the finger impression sensor and

coordinates with the elector information present in the data set and it additionally manages the tolerant, handling, putting away the vote in cloud in real-time. LCD and buzzer is utilized to give affirmation to the citizen. Buttons are utilized to make the choice to up-and-comer. The entire activity done by the clients is refreshed on IoT server. The Arduino gives information of clients and updates the activity done by client. Elector is permitted surveying just whenever they are confirmed with fingerprint sensor.

Software Implementation:

The software module is based on Django web-framework along with py-serial to support IoT interface. There are two types of login they are:

1. Admin:
    *   He has the ability to add booth representative.
    *   He can verify the voter.
    *   He can reset the voter status to "NOT VOTED" and truncate the result database.
    *   He can view the result in real-time.
2. Booth Representative: He can verify the voter.
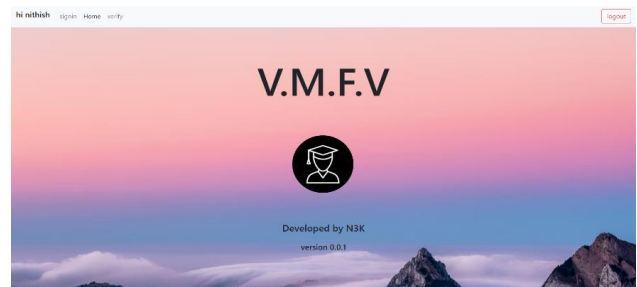

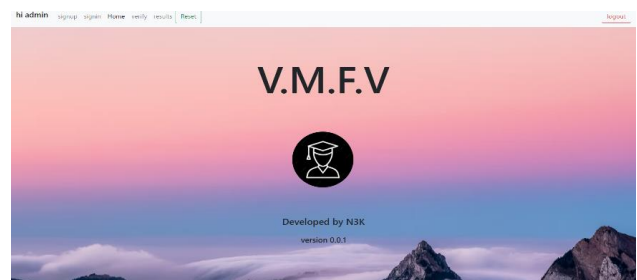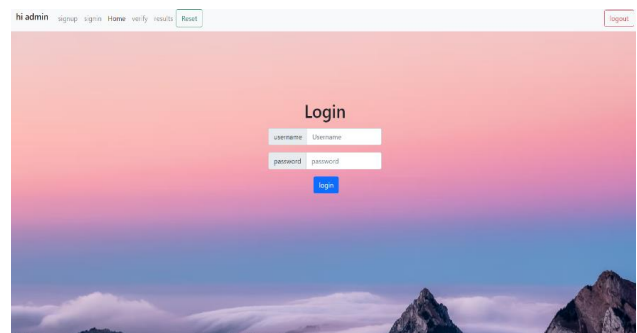Fig. 11. Admin Home Page

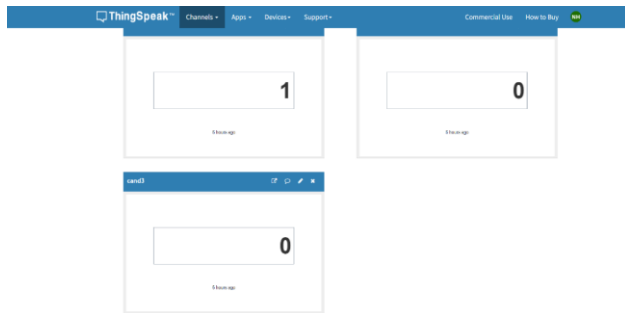Fig. 12. Home Page

Fig. 13. Login Page

Fig. 14. Thingspeak channel
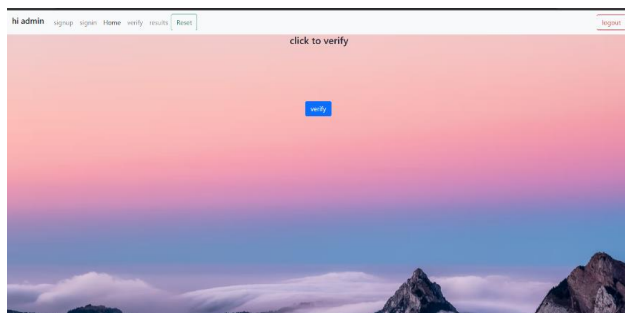

Fig. 15. Result of the implementation

Fig. 16. Verify Page

7. Conclusion and Future Scope

All through this writing review scientists proposed a great and proficient biometric casting a ballot machine had all the more extra highlights and better over customary democratic framework. The benefit of this framework are quicker result, better exactness, further developed openness, okay of mechanical, human blunders. It was additionally more possible, practical, convenience, less power utilization, efficient, and not additional equipment necessity. The cycle stream is extremely straightforward and remarkable. A few significant focuses are raised during this study that is has a few constraints and we need to future work on it. Some extra element added with equipment like huge showcase, webcams and sensors can be coordinated with casting a ballot machine for additional security and quick work.

- It has less memory so expanded memory limit.
- People groups without any hands will not have the option to make choice so in ongoing we ought to utilize multi-biometric frameworks by iris output or facial acknowledgment in model.
- Better point of interaction.
- Enormous volume of information base which require some investment to check and confirm.

References

[1] Vishal Vilas Natu, Savvy Voting utilizing Biometric "Global Journal of Emerging Technology and Advanced Engineering, 2014.

[2] Khasawneh, M., M. Malkawi and O. Al-Jarrah, 2008. A Biometric-Secure e-Voting System for Election Process, Proceeding of the 5th International Symposium on Mechatronics and its Applications (ISMA08), Amman, Jordan.

[3] Virendra Kumar Yadav, Saumya Batham, Mradul Jain, Shivani Sharma, An Approach to Electronic Voting System utilizing UIDAI, International Conference on Electronics and Communication Systems, 2014.

[4] Chaum, D. L., Untraceable Electronic Mail, Return Addresses and Digital Pseudonyms, Communicate of the ACM, 24(2): 84-88, 1981.

[5] Virendra Kumar Yadav, Saumya Batham, Mradul Jain, Shivani Sharma, 2014. An Approach to Electronic Voting System using UIDAI, 2014 International Conference on Electronics and Communication Systems.

[6] Ashok, Kumar D. and T. Ummal Begum, A Novel design of Electronic Voting System Using Fingerprint, 2011.

[7] Jefferson, D., A. Rubin, B. Simons and D. Wagner, A Security Analysis of the Secure Electronic Registration and Voting Experiment (SERVE), Technical Report, 2009, available at: http://www.servesecurityreport.org

[8] Qijun Zhao, Lei Zhang, David Zhang and Nan Luo, Adaptive Pore Model for Fingerprint Pore Extraction. Proc. IEEE, 2008.

[9] Moheb R. Girgis, Tarek M. Mahmoud and Tarek Abd-El-Hafeez, An Approach to Image Extraction and Accurate Skin Detection from Web Pages. World academy of Science, Engineering and Technology, pp. 27, 2007.

[10] Manvjeet Kaur, Mukhwinder Singh, Akshay Girdhar and Parvinder S. Sandhu, Unique mark Verification System utilizing Minutiae Extraction Technique. World foundation of Science, Engineering and Technology, pp. 46, 2008.