

Secured Voting System Using Smartphone and Biometric Authentication

Kavitha .K^{1*} , Devanthi .C^{2*}

Assistant Professor, Department of ECE, Velalar College of Engineering and Technology, Erode, Tamil Nadu, India. ¹

Student, Department of ECE, Velalar College of Engineering and Technology, Erode, Tamil Nadu, India. ²

*Corresponding author:

ABSTRACT : This paper describes the strategy and functioning of the highly secure biometric authentication system E-smart voting system (ESVS) along with the OTP-based verification system to enhance voting during election. Additionally, the vote cast by a user is encrypted before it is stored in the database. ESVS uses Aadhar user number to identify and validate electors. With smart voting system, voters can cast their vote on mobile phones and stop all kinds of queues at polling booth. In the ESVS the user must first punch their Aadhar number. The ESVS uses the Aadhar number to authenticate the user via OTP which will be received on the linked mobile number of their registered Aadhar. Through highly sophisticated biometric authentication based on Aadhar, people without Smartphones can vote through ESVS with an additional authentication stage. Successfully, the Smart Voting System allows people to vote using smart phones, thus raising the lines piled up at polling booth. It also offers a highly reliable method for biometric authentication for people who do not have smartphones.

KEYWORDS: Electronic voting system, Cloud, Authentication ,Aadhar id, Voter id.

I. INTRODUCTION

The principles of democracy are based upon the decision of the people. Therefore, we need to take the correct decision to have a great vision. You can do this by "voting." The modern voting structures follow the issue of manually produced voter ID and other information. So, parallax errors are probable. In addition, the electronic voting system can be configured to convert people whatever and whomever they vote into the party or members of some other. Could be misused. Had been designed to prevent this automation. Most organisations and developed countries have brought the automated system on board.

II. EXISTING SYSTEM

The most of voting system uses the paper ballots and finger print scanner for reference. But this system increase the queues in the polling booth.

III. RELATED WORKS

1. Biometrically Secured Electronic Voting Machine

In that proposed system they have used Arduino and Finger Print Scanner that can identify each voter, count votes and can prevent fake votes. This system is more digital, technology-based and secured system.

Demerits:

- Cast voting through smart phone is not implemented.
- This will be increases the queues.

2. Secured and Transparent voting system using biometrics:

A secured electronic voting machine using unique identification number. To provide additional security along with the Aadhar number biometric identification is used. At the time of voting in the elections, the voter authentication can be done through biometric pattern. If the biometric information of the voter matches the database of the Aadhar then the person is allowed to cast their vote.

Demerits:

- Smart voting system is not enabled.
- Not reliable
- Is not user friendly

IV. PROPOSED SYSTEM

The system proposed is a protected e-voting system that uses Indian Unique Identification Authority (UIDAI) or aadhar database as its backend. The system ensures an individual's identification by matching fingerprints, and eligibility is verified by measuring the voter's age, thus redundantly the current voting cards. The program offered includes two databases. One is the Central database and the other is the polling station Area database. Central database called Central Identities Data Repository (CIDR) that forms the system's backbone. It includes all of India's people ' demographic and biometric data. It includes all of India's people ' demographic and biometric data. To reduce the load on the central database, there are local databases that will be located alongside the servers that will contain cached copies of the inhabitants ' data that fall below their territory. Based on population density, area and other factors, these zones are calculated. All the local repositories only collect CIDR data from those people who come under its control. This data is changed regularly and stored in dynamic form so that it can be erased if necessary, such as during security threats, natural disasters, maintenance work, etc. Local databases will only collect data relating to the voting process and exclude any other information that is irrelevant. Those databases will be used to produce electoral process statistics and tests. These databases allow voting from anywhere as long as the elector is in electoral circuits.

V. BLOCK DIAGRAM

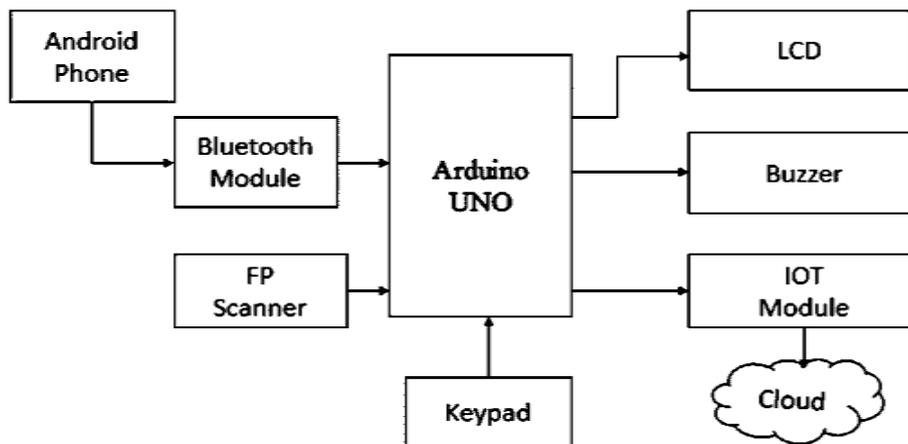


Fig 1: Block Diagram

VI. WORKING

1.ID GENERATIONFOR ONLINE VOTER

Aadhar card information consisting of each individual name, date of birth, gender, aadhar number, mail I d, address, state, district, left and right hand fingerprint along with retina scan and passport size photograph is stored in the admin database. Voting I d for people over 18years of age is created from the aadhar data as it is the eligibility criterion for voting. The people will access their voter I d for future use from their mail ids. For the voter I d information, a new database is created for the people over 18 years of age.

2.CASTING THE VOTE:

A voting machine will be built with monitoring, scanning etc., and a device will be connected to that machine via USB cables. The user must first sign in via fingerprint to the device. Authentication from the Aadhar fingerprint database is provided. If the fingerprint matches the user has to go through his / her face. The voter will be allowed to enter their

voter I d and cast their vote for their interested party if it matches. People who try to vote for the second time are not allowed as once authentication is granted to the finger print the user is denied login. The casted vote is updated in the database at each instance of time. With high accuracy and reliability, the election results may be published on the same day. People who vote online will also be going through some authentication process as well. We can cast their vote on their candidates via our app.

VII. HARDWARE DESCRIPTION

1.CIRCUIT DIAGRAM – ARDUINO TO 16x2 LCD MODULE

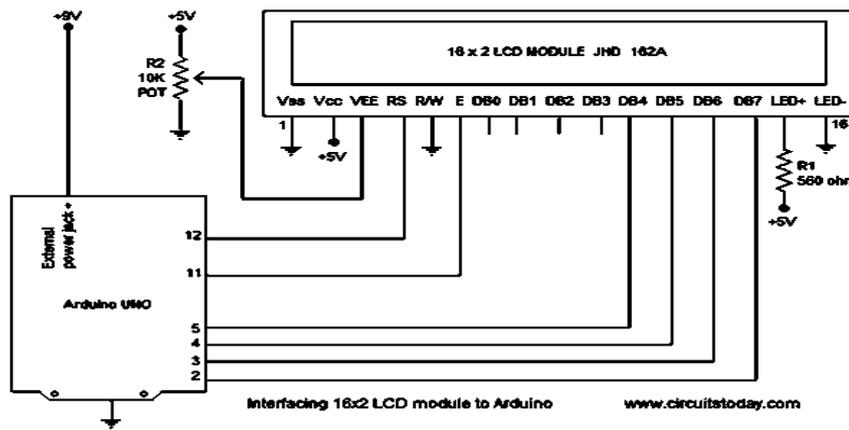


Fig 2: Interfacing Diagram

The LCD module's RS pin is attached to the arduino's digital pin 12. The LCD's R / W pin is grounded. The LCD module's activate pin connects to the arduino's digital pin 11. In this project the 4-bit mode interface between the LCD module and arduino. This means that there are only four of the LCD's optical input lines (DB4 to DB7). This method is very simple, requires fewer connections and you can nearly leverage the maximum LCD module capacity. The Arduino digital lines DB4, DB5, DB6 and DB7 are interfaced with Arduino digital pins 5, 4, 3 and 2. The 10 K Potentiometer is used to modify monitor contrast. The 560 ohm resistor R1 restricts the current in the back light LED. The arduino can be operated by means of the board's external power jack. + 5V needed in some other parts of the circuit may be tapped to the arduino board from the 5V source. The arduino can also be driven over the USB port from the PC. The full program for LCD to Arduino interface is displayed.

2.PROGRAM – ARDUINO TO LCD

```
#include<LiquidCrystal.h>
LiquidCrystalled(12, 11, 5, 4, 3, 2); // sets the interfacing pins
void setup()
{
lcd.begin(16, 2); // initializes the 16x2 LCD
}
void loop()
{
lcd.setCursor(0,0); //sets the cursor at row 0 column 0
lcd.print("16x2 LCD MODULE"); // prints 16x2 LCD MODULE
lcd.setCursor(2,1); //sets the cursor at row 1 column 2
lcd.print("HELLO WORLD"); // prints HELLO WORLD
}
```

3.FINGERPRINT RECOGNITION

Fingerprint recognition or fingerprint authentication refers to the automatic process used to validate a connection between two human fingerprints. Fingerprints are one of many types of biometrics used to identify and validate individuals. This article addresses two major classes of algorithms (minutia and pattern) and four types of sensors (optical, ultrasonic, passive, and active capacitance).

A)Background

The analysis of fingerprints for matching purposes generally requires the comparison of several features of the print pattern. These include patterns, which are aggregate characteristics of ridges, and minutia points, which are unique features found within the patterns. It is also necessary to know the structure and properties of human skin in order to successfully employ some of the imaging technologies.

B)Patterns

The three basic patterns of fingerprint ridges are the arch, loop, and whorl:

- Arch: The ridges come in from one side of the finger, grow in the middle making an arc, and leave the other side of the finger afterwards.
- Loop: The ridges come in from one side of a leg, form a curve and exit on the same side.
- Whorl: Ridges on the finger shape circularly around a center point.

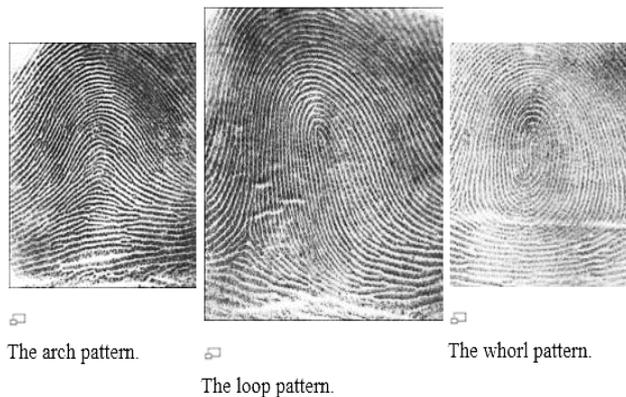


Fig 3: Pattern for Fingerprint Recognition

C)Minutia features

The major features of fingerprint ridges in Minutia are: ridge top, bifurcation, and short ridge (or dot). The finishing ridge is the ending point of a mountain. Bifurcations are points where a single ridge divides up into two ridges. Short ridges (or dots) are ridges that are considerably shorter than the fingerprint's average ridge length. Minutiae and patterns are very significant in fingerprint research, since no two fingers have been shown to be the same.

4.BLYNK APP – IOT PLATFORM

Blynk is a forum for controlling Arduino, Raspberry Pi and the likes of iOS and Android devices over the Internet. It's a digital dashboard where you can easily drag and drop widgets to create a visual interface for your project. Blynk is not tied to any particular board or shield. Alternatively, it does support your choice of hardware. Whether you're connecting your Arduino or Raspberry Pi to the Internet through Wi-Fi, Ethernet or this new ESP8266 chip, Blynk will get you online and ready for Internet Of Your Things.

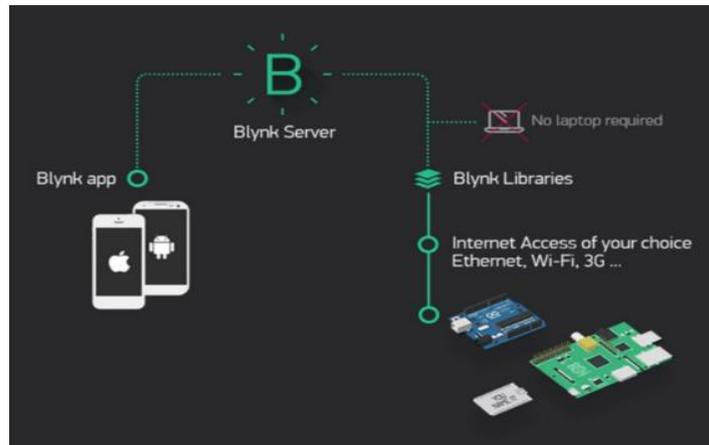


Fig 4: IOT Platform in Blynk App

VIII. FLOWCHART

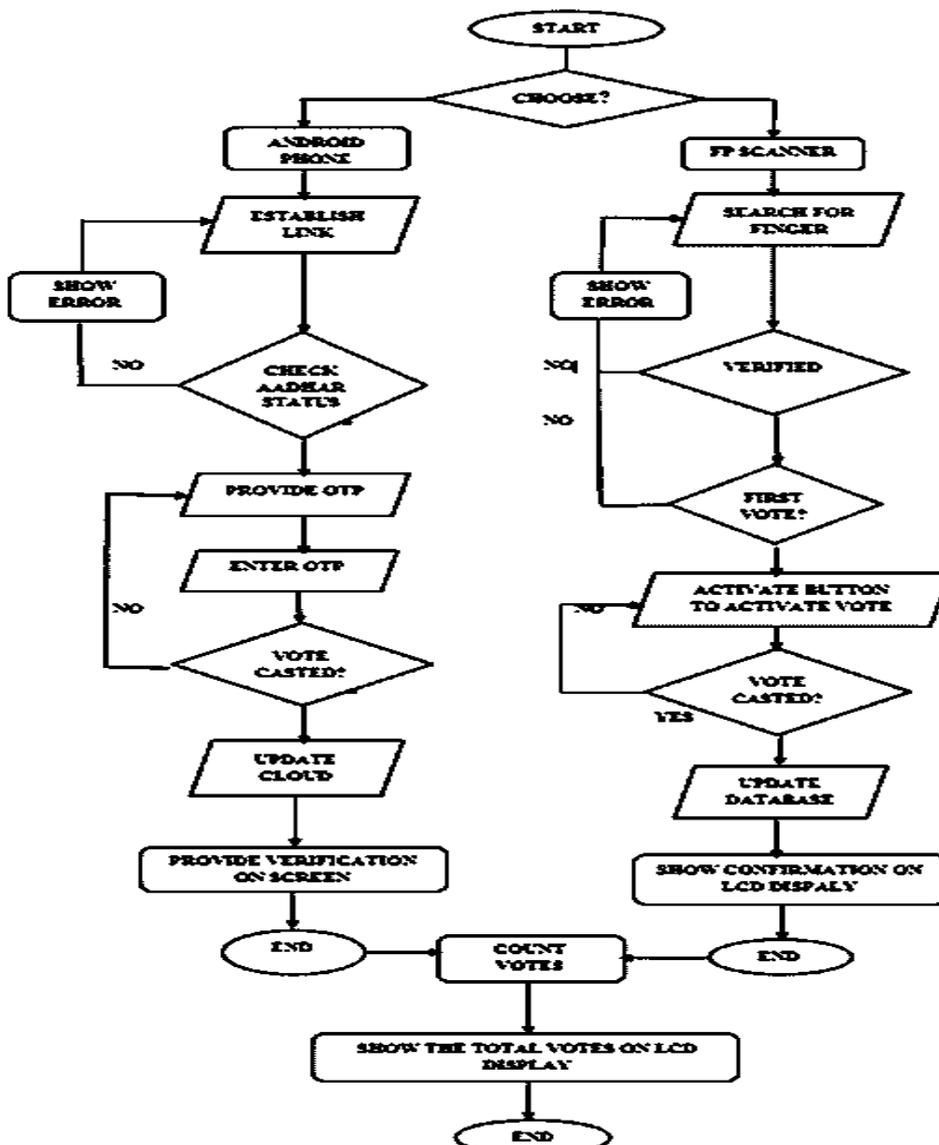
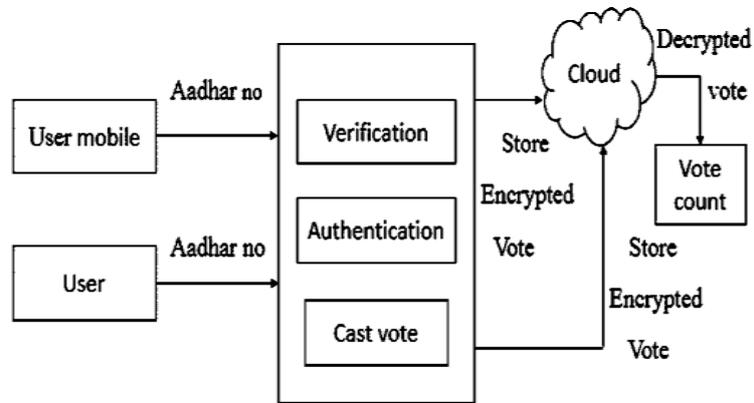


Fig 5: Flow Diagram

IX. ARCHITECTURE DIAGRAM



Smart voting system

Fig 6: Architecture Diagram

X. RESULT

1.RESULT THROUGH SMART PHONE:

Each voter have a separate link, this link will be send by the verification of Aadhar details. After that voter cast their vote with the help of OTP.

2.RESULT THROUGH BIOMETRIC AUTHENTICATION:

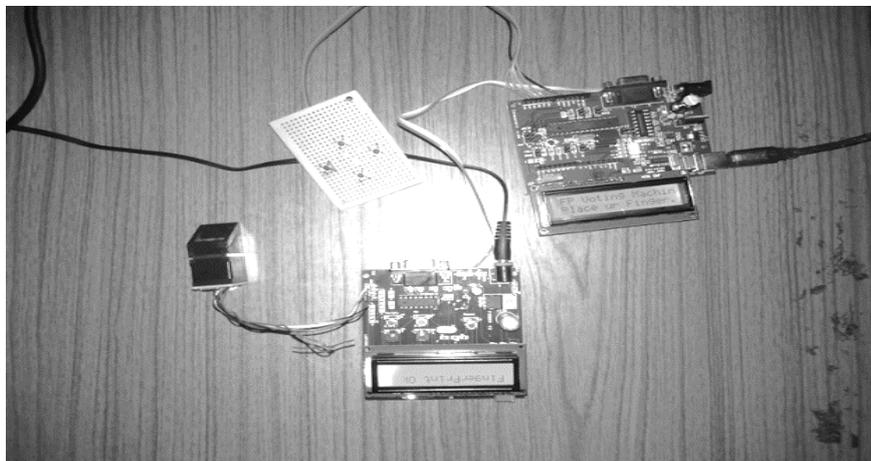


Fig 7: Circuit for Biometric authentication

XI. MERITS

- Automatic voting I d generation
- Digital voting
- Manual job reduction
- Transparent voting system
- Secure voting system, by matching smartphones and fingerprints.



XII. CONCLUSION

A country with less voting numbers will fail to grow as it is very important to choose a right leader for the nation. Sadly, in the 100 per cent vote our country fails. This is primarily due to a security level flaw in the current voting system. Our implementation tends to make our nation a developed country by creating a high-security voting system to increase the percentage of votes.

REFERENCES

- [1] Biometrically Secured Electronic Voting Machine RahilRezwan, Huzaifa Ahmed, M. R. N. Biplob, S. M. Shuvo, Md. Abdur Rahman Department of Electrical and Electronic Engineering American International University Bangladeshrahi.lsh18@gmail.com,2017
- [2] “Secured and transparent voting system using biometrics” ch.jayalakshmi , s.kalpana dept. of eiesiddharthaengg. college v.r. siddharthaengg. College .
- [3] C. W. Gear, “Multibody grouping from motion images,” Int. J. Comput. Vis., vol. 29, no. 2, pp. 133–150, 1998.
- [4] E. Elhamifar and R. Vidal, “Sparse subspace clustering: Algorithm, theory, and applications,” IEEE Trans. Pattern Anal. Mach. Intell., vol. 35, no. 11, pp. 2765–2781, Nov. 2013.
- [5] F. Flores-Mangas and A. D. Jepson, “Fast rigid motion segmentation via incrementally-complex local models,” in Proc. IEEE Conf. Comput. Vis. Pattern Recognit. (CVPR), Jun. 2013, pp. 2259–2266.