DEVELOPING A SMART VOTING SYSTEM LINKED TO THE STATE OF ART AND FINGERPRINT VERIFICATION SYSTEM

Teesha Ahuja

Bharati College, University of Delhi

ABSTRACT

Voting is important for citizens to do in a democratic country like India. Voters typically cast their ballots in the polling booth. The electronic voting machine is used to cast votes as technology advances. An IoT-based voting machine with fingerprint verification is the subject of this paper. This project aims to make voting safer and reduce fraud by using fingerprint verification. A database contains the voter's information as well as their fingerprint. The system verifies the user's aadhar number and, if authenticated, determines whether multiple votes have been cast if the fingerprint matches the fingerprint that is stored. The message "Matching failed" will be displayed if the fingerprint matching is incorrect, and "Aadhar not matched" will be displayed if the aadhar number is incorrect. Using thingspeak, a voter can go to their home town and vote for the appropriate candidate, and the result can be obtained using the same method. This project's controller is the Arduino Uno. The fingerprint is used to verify the user's identity. Each person's fingerprints are at least slightly different. An "Already voted" message will be displayed whenever malpractice occurs.

The citizen's right to vote is protected, and this project guarantees fair elections. The board is programmed with the Arduino IDE, and the cloud stores and displays ballot cards. The system flags malpractice, and only registered voters can vote.

INTRODUCTION

Voting is the right of every citizen to choose their leader by voting. India is a democratic nation where people can vote and show their choices. By supporting the candidate in the upcoming election, people can also exercise their right to alter the party in power.

The purpose of voting is to select leaders for the government and schools, colleges, banks, society, and other institutions.

Biometrics is a method for identifying a person based on their physical characteristics. The iris, face, voice, and fingerprint are the biometrics used to identify an individual. Because it is unique to each person, the fingerprint can be used as a signature, verification, and authentication mark. One-to-one matching and one-too-many matching are two of biometrics' most important functions. When the biometric sample is compared to the samples that have already been stored, with too many matches, it compares with the previously stored sample in one-to-one matching. The biometric method improves user verification convenience and speeds up security. Password security is inferior to biometric security.

In this project, the fingerprint is used as a biometric. Every individual's fingerprints will be unique. In this project, the user's fingerprint is used to verify his identity, and he can vote based on the image of his fingerprint. Fingerprint matching comes in three varieties: pattern-based (or image-based) matching, correlation-based matching, and minutiae-based matching. Two fingerprint images are superimposed in correlation-based matching; Consequently, the correlation between corresponding pixels is calculated for various alignments. The two fingerprints' minutiae are extracted and stored as a set in a two-dimensional plane in minutiae-based matching. The alignment of the template and the input minutiae sets that produce the maximum number of minutiae pairings is determined using this matching approach. The stored template and the candidate's fingerprint are compared in the pattern-based (or image-based) matching method. The images must be aligned in the same orientation for this to work. The algorithm focuses on a central point in the fingerprint image to accomplish this. The patterns' sort, size, and orientation in the aligned fingerprint image are contained in the template in a pattern-based algorithm. Virtually every industry stores data digitally. The majority of tasks are done online to create a digital India. Online voting makes it easier for voters to cast ballots from anywhere worldwide. One method that facilitates online voting is Thingspeak. The system runs faster when results can be found online.

PROPOSED SYSTEM

The biometric verification method in this system is the fingerprint and its online version. The voter's aadhar number and fingerprint are entered into a database and kept there. The aadhar number is requested by the first voting system during the process. It checks the fingerprint to see if it matches the stored Aadhar number if it does. If the fingerprint matches, the system determines whether the individual has previously cast a ballot for the same election. The "Fingerprint and Aadhar number matches" if he has not voted. The message "Cast vote" will appear. The register will be increased following voting. A person has "already voted" if they have previously cast a ballot.

A buzzer sounds, and the message is shown.

Through Thingspeak, a keypad is used to cast votes. A person is permitted to vote when a message is displayed.

To begin voting, the system requires that the native place be entered using the keypad. The voter is then permitted to vote for the candidate of his choice. Thingspeak stores each voter's vote and voting time. The outcome will also be obtained. This system can also be used for postal voting because it uses Thingspeak. To oversee voting, a polling officer should be present. Because the system is online, voters can vote for candidates from their home town or city.

METHODOLOGY

The IoT-based voting machine with fingerprint verification's functional block diagram includes a controller, fingerprint module, Wi-Fi module, keypad, power supply, and cloud. Arduino Uno is the controller used in this system. The laptop supplies the system with power. The vote is

polled using a keypad. The finger is placed using the fingerprint module; It is used to store the fingerprint database of voters. The serial monitor will display messages regarding the system's instructions and any misbehaviour.

Figure 1. Block diagram of verification unit

The fingerprint module shows a message if the fingerprint belongs to an authenticated person after comparing it to the fingerprint in the database. The matching result will be displayed on the serial monitor. The cloud is where the voting paper is kept. Each candidate's final count is saved in a different cloud field. Thingspeak is used to store the candidate's final count in this case. The controller gets Wi-Fi from the ESP8266. When a voter votes for the second time, the buzzer sounds an alarm. They are divided into two groups here: voting and the fingerprint.

The verification unit's block diagram can be seen in Figure 1. It primarily addresses enrollment and matching. It includes the fingerprint module that stores the voter's fingerprint and compares it to a database to see if it matches. The voter's aadhar number is also stored here. Additionally, the database's aadhar count is checked by the system. The system checks to see if that person tried to vote multiple times. When there is a second vote, a buzzer sounds.

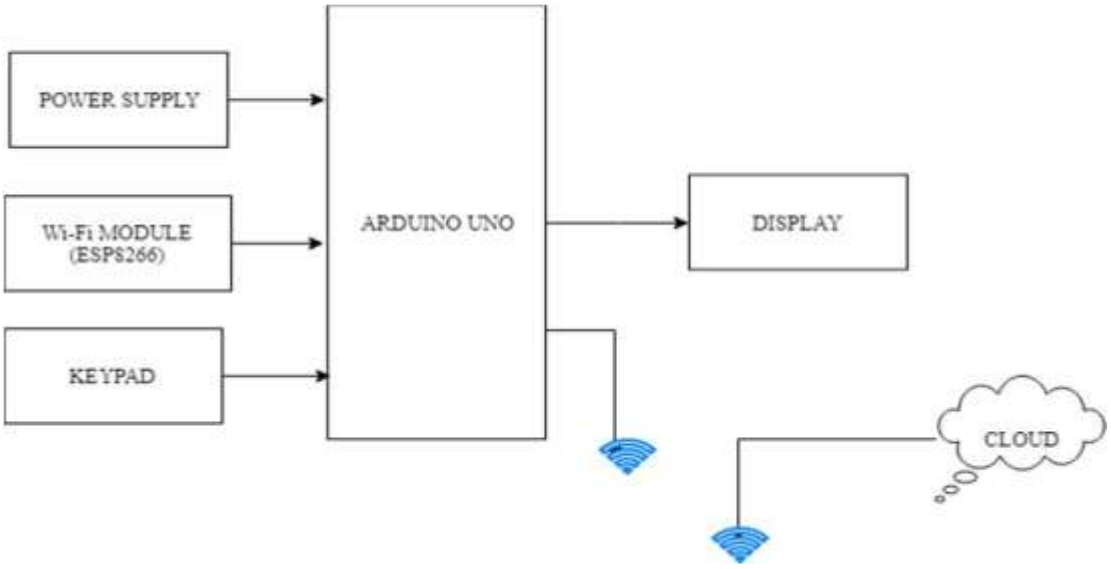


Figure 2. Block diagram of voting unit

A. The system's operation: The voter should enrol using his fingerprint and Aadhar number first. It compares the enrolled data with any previous entries for that user during the voting process to see if they match. A buzzer alarm and the message "Already voted" will appear if that voter has previously voted. If he has yet to vote, he can do so through ThingSpeak, where he chooses his home town and votes, and a register will be added. The result can then be obtained after the voting.

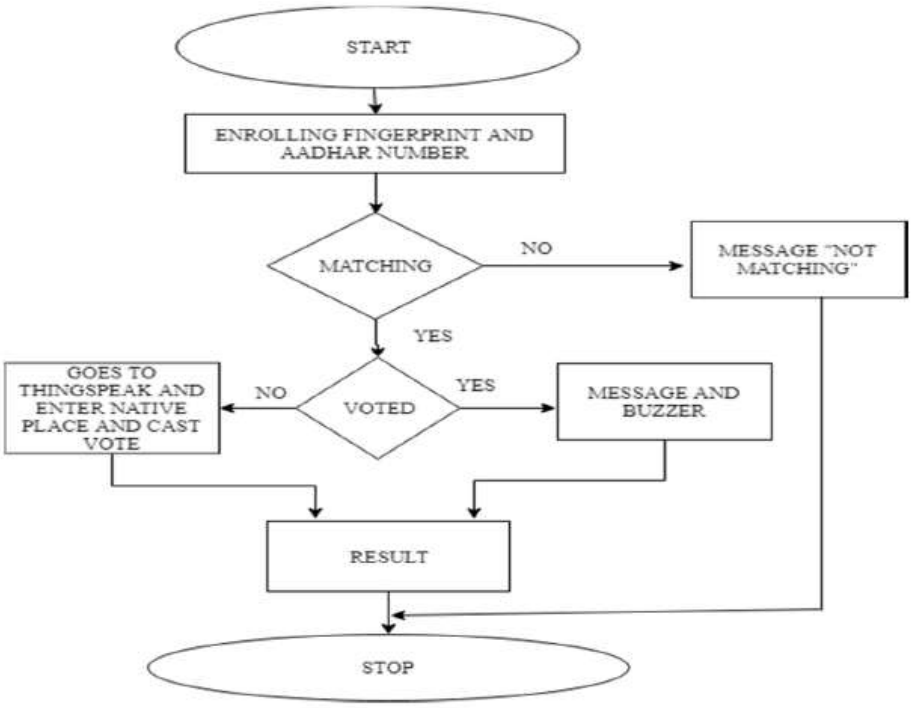


Figure 3 System Working

B. Fingerprint Module Hardware Requirements

The optical fingerprint sensor, a high-speed DSP processor, a high-performance fingerprint alignment algorithm, high-capacity FLASH chips, and other hardware and software make up the fingerprint Module. Other functions include fingerprint entry, image processing, matching, search and template storage, and more. There are TTL UART and USB2.0 interfaces on the fingerprint module; The computer is frequently connected to the USB2.0 interface; The default baud rate for the RS232 interface is 57600, but it can be changed by asking for a communication protocol. Microcontrollers like ARM, DSP, and other serial devices are connected via a connection, and 3.3V to 5V microcontrollers are frequently connected directly.

Figure 4: Fingerprint Module

1) ESP8266: The ESP8266's system-on-chip (SoC) module supports Wi-Fi. It is mostly used to create embedded Internet of Things (IoT) applications. It has a RISC 32-bit CPU. The boot ROM is 64 KB, the instruction RAM is 64 KB, and the data RAM is 96 KB. SPI is used to access flash memory from outside the computer. The ESP8266 module is a standalone, low-cost wireless transceiver for IoT development at the endpoint. The microcontroller must communicate with the ESP8266 module using a set of AT commands. The microcontroller uses a UART with a specified baud to communicate with the ESP8266-01 modules.

C. Arduino's Software Requirement

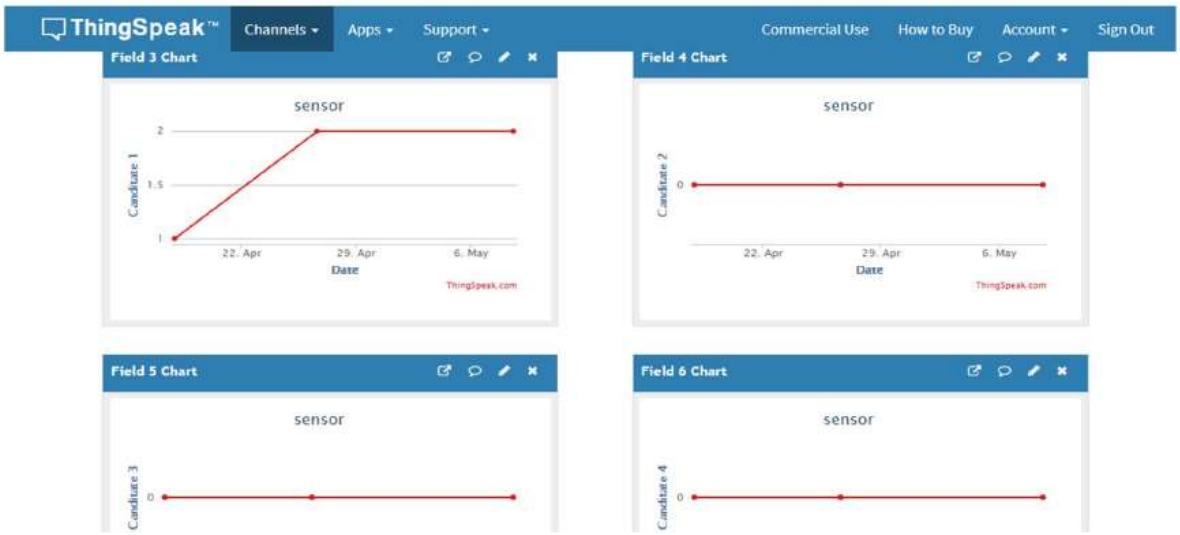
1) Ide: A text editor for writing code, a message area, a text console, a toolbar with buttons for common functions, and a series of menus make up the Arduino Integrated Development Environment (IDE). It communicates and uploads programs by connecting to the Arduino and Genuino hardware. Sketches are programs created with Arduino Software (IDE). The file extension is used to save these sketches written in the text editor. No. The editor has tools for searching and replacing text and cutting and pasting. While saving and exporting, the message area displays errors and provides feedback. The Arduino Software (IDE) outputs text to the console, which includes all of the information, including complete error messages. The

configured board and serial port are displayed in the window's bottom right corner. Using the toolbar buttons, you can open the serial monitor, create, open, and save sketches, and verify and upload programs.

2) Wordspeak: ThingSpeak is an open-source application and API for the Internet of Things (IoT) that uses the HTTP protocol to store and retrieve data from objects over the internet or a Local Area Network. Applications for location tracking, sensor logging, and a social network of things with status updates are all made possible by Thingspeak. To begin, we must sign up for an account in ThingSpeak. Create a new channel by logging in. We will acquire an

IMPLEMENTATION RESULTS

The proposed system has been implemented. This system primarily consists of two units, one for voting and one for verification. The Arduino IDE was used to program the Arduino UNO. The verification unit has three scenarios: voting for the first time, voting multiple times, and having a fingerprint and Aadhar number that does not match. A user's fingerprint and Aadhar number are compared to data in the database when they attempt to vote for the first time; He can vote in the event of a match, and the message "Authenticated". On the Arduino's serial monitor, the message "Proceed" appears. A buzzer sound and an "already voted" message will be displayed on the serial monitor if an authenticated user attempts to vote multiple times. A person can only vote if the database contains his fingerprint and Aadhar numbers. The authorized officer receives the voting summary after the voter uses a Thing Speak-enabled keypad in the voting unit to cast their vote.



CONCLUSION

As India is a democratic nation, all citizens have the right to select a leader. The concept presented here is a voting system based on IoT. The entire world is moving completely digital. Here, voting is also digitized as part of digitization. This project has the advantage of speeding up the announcement of the outcome. Implementing biometrics and Aadhar number

verification makes the system more secure. Only one person can vote under this system. Voting multiple times is not allowed. Postal voting can also be conducted using this system.

REFERENCES

1. Anandaraj S, Anish R and Devakumar P.V, Secured electronic voting machine using biometric, *2015 International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS)*, Coimbatore, India, 2015, pp. 1-5, doi: 10.1109/ICIIECS.2015.7192976.IEEE.

2. D. Ashok Kumar, T. Ummal Sariba Begum, (2012), Electronic Voting Machine – A Review, *Proceedings of the International Conference on Pattern Recognition, Informatics and Medical Engineering*, March 21-23, 2012.

3. R. Rezwan, H. Ahmed, M. R. N. Biplob, S. M. Shuvo and M. A. Rahman, (2017), Biometrically secured electronic voting machine, *2017 IEEE Region 10 Humanitarian Technology Conference (R10-HTC)*, Dhaka, Bangladesh, 2017, pp. 510-512, doi: 10.1109/R10-HTC.2017.8289010.

4. R. Murali Prasad, Madhu Nakirekanti, Polaiah Bojja, (2016), AADHAR based Electronic voting Machine using Arduino. *International Journal of Computer Applications* (0975-8887) Volume 145 - No.12, July 2016