Research Paper E-ISSN NO : 2455-295X | VOLUME : 9 | ISSUE : 6 | SPECIAL ISSUE JUNE-2023

IOT-BASED VOTING SYSTEM WITH FINGERPRINT IDENTIFICATION

DR M YUVARAJU	ASSISTANT PROFESSOR, EEE DEPARTMENT, ANNA UNIVERSITY REGIONAL CAMPUS, COIMBATORE, INDIA - 641046.
A SAKTHIVEL	UG STUDENT, DEPT OF EEE, ANNA UNIVERSITY REGIONAL CAMPUS, COIMBATORE, INDIA - 641046.
C MUTHUKUMARAN	UG STUDENT, DEPT OF EEE, ANNA UNIVERSITY REGIONAL CAMPUS, COIMBATORE, INDIA - 641046.
E ABISHEK	UG STUDENT, DEPT OF EEE, ANNA UNIVERSITY REGIONAL CAMPUS, COIMBATORE, INDIA - 641046.
R RAMANI	UG STUDENT, DEPT OF EEE, ANNA UNIVERSITY REGIONAL CAMPUS, COIMBATORE, INDIA - 641046.
E SWATHI	UG STUDENT, DEPT OF EEE, ANNA UNIVERSITY REGIONAL CAMPUS, COIMBATORE, INDIA - 641046.

ABSTRACT:

Voting is an important means for citizens to register their votes in a democracy like India. Voting typically involved enrolling in a polling place. This study examines a voting device that uses fingerprint identification and is Internet of Things-based. Main objective of our project's goals included reducing fraud and securing voting using fingerprint verification. The voter's fingerprint and personal information are both saved in a database. The system examines the Aadhar number of the associated user and, if confirmed, determines whether multiple votes have been registered whether the fingerprint matches the stored fingerprint. The messages "Matching Failed!" and "Aadhar Not Correct" will be displayed if the fingerprint matches are incorrect and the Aadhar number is incorrect, respectively.

KEYWORDS:

ELECTRONIC VOTING MACHINE (EVMS), AADHAR CARD, BIOMETRIC TEMPLATE, FINGERPRINT SENSORS.

INTRODUCTION

Each citizen has the right to vote in order to cast their ballot and choose their representative. Every individual in the democratic nation of India has the right to cast a ballot and express their opinions. By supporting a different candidate in the forthcoming election, voters also have the option of changing the ruling party. Voting is done not just to choose the government's representatives, but also to choose the heads of our society, banks, colleges, and other institutions.

The process of identifying someone based on their physical characteristics is known as biometrics. The main biometrics used to identify a person are the fingerprint, iris, face, voice, etc. Biometrics perform two essential tasks: the first is one-to-one matching, and the second is one-too-many matchings. The biometric sample was compared to the samples that had already been stored in one-to-many matching. It compares with the previously saved sample in one-to-one matching. The fastest security and most practical approach for user verifications is the biometric method. Password security is inferior to biometric security. Because each person's fingerprint is unique, it can be used as a signature, identification, and Verification mark.

In our project, we use fingerprints as a biometric. Each person will have a unique fingerprint. In our project, a user's fingerprint is utilised to authenticate them and gives them the ability to register to vote using fingerprint images. Three categories of fingerprint matching exist: pattern-based (or image-based), minutiae-based, and correlation-based matching. Two fingerprint images are superimposed in correlation-based matching, therefore the correlation between corresponding pixels was calculated for each alignment. Minute details from the two fingerprints were collected and stored as a set in the two-dimensional plane for minutiae-based matching. Finding the alignment between the template and the input minutiae sets that yields the greatest number of minutiae pairings is the matching approach. The candidate's fingerprint and the stored template can be compared using the pattern-based (or image-based) matching method. The photos must be oriented similarly and aligned for this to work. The programme does this by locating the middle of the fingerprint image and then centres around it. The sort, size, and orientation of the patterns within the aligned

fingerprint image are contained in the template in a pattern-based algorithm. Digital data storage was used in almost all industries. Most tasks involved creating a digital India was completed online. Online voting allows voters to cast their ballots from anywhere in the world. One method that assisted with online voting was thing talk. Finding results online speeds up the process.

Voters typically mark their ballots with a stamp to indicate which candidate they support before placing them in the ballot box. Each vote on each ballot box must be counted in order to determine the total number of votes, which is then added for each candidate. The candidate receiving the most votes will be declared the victor.

Since everything was done manually, it will take longer to announce the elected officials. To avoid voting twice, each voter will have their fingertips tagged with ink after casting their ballot. Until the development of electronic voting machines, this method was used. The right to vote is one that all citizens in our nation, like those in India, have. In India, the people had the right to choose who would govern them for the foreseeable future. If the populace is dissatisfied with that leader, they will have the opportunity to elect a new one in the subsequent election. But numerous errors are being made, which have no bearing on the right outcome. It wastes more time and was less secure in the current systems. The voter must cast their ballot in the appropriate locations. Additionally, voting by mail was not very secure. In order to achieve the research's ultimate goal of developing a system that can prevent electoral misconduct, the project made use of the proper methodologies.

Each candidate who is qualified to vote has their fingerprint entered and saved in the systems. The biometric identification method employed fingerprints. The stored databases were compared to the fingerprint and Aadhar number stored in storage. It offers voter identification verification. Additionally, it looks to see if a voter has cast several ballots in a single election. The outcome will also be kept in the clouds. Voters can cast their ballots from anywhere in the world because the voting was conducted via the cloud. An alert will be generated if the confirmed voter attempts to cast their ballot more than once. Here, we were making use of the buzzer sound to alert us to the malpractice.

1.1 EXISTING SYSTEMS:

Today, electronic voting machines are utilised to count the votes. The control unit and the balloting unit are the two components of an electronic voting machine. The presiding officer was in charge of the control unit, and following a verification, voters were given the opportunity to cast their ballots. The voting compartment contained the voting unit. The presiding officer clicks the ballot button when the verification is complete so that the voter may cast their ballot. The button next to the candidate's name can be used by the voter. Voters under the current system must have their ID cards on them for verification. The presiding officer will confirm the voter's identity by consulting the list and ID card. This is the laborious work. All of the EVMs will be collected after the conclusion of the election and brought to the centre for counting. Selected government workers will conduct the vote count and then announce the results.

FIGURE1. ELECTRONIC VOTING MACHINE

This system as it is now having some issues. One issue is that no one, including the authorities, can connect any ballot to the voter. Another issue was that the EVM's installed software might be changed (security issues). The inability to independently confirm that all votes had been duly counted presented another issue. Another issue was accessibility; the system is flawless as long as the polls are open and all voters have access to it from the start to the finish of the election. One of the issues with the current system is when one candidate unlawfully casts the ballots of all or a significant portion of the electorate.

1.2. PROPOSED SYSTEM:

In this system, the online version of the fingerprint biometric technique of verification was used. A database was created and filled out using the voter's fingerprint and Aadhar number. The first system that asks for the Aadhar number throughout the voting process compares it to the stored Aadhar number before determining whether the fingerprint matches. If the fingerprints are a match, the system then checks to see if the voter has already cast a ballot in the same election. The Aadhar number and fingerprint match if he hasn't cast a ballot. display the message "Register to Vote." The register will be increased following the vote. The bell sounded and the message "Already voted!" was displayed if that person has already cast a ballot.

Voting was conducted by Thing talk on a keypad. When the register to vote notification appeared, that person was then eligible to vote. The voting method first asks the user to enter their home country using a keypad. The voter could then select the candidate of their choice. In Thing speak, votes and voting time are saved. The outcome will also be attained. This system can be used for postal voting as well because it speaks in Thing. To oversee voting, there should be a polling officer. Because the system was online, the voter could select a candidate from their own community.

2. LITERATURE SURVEY:

In Murali Prasad (2016), R. Murali Prasad, Polaiah Bojja, and Madhu Nakirekantidiscuss user login using the Aadhar number and password. The next step is to determine if the

person was entitled to register to vote. In this article, we look at policy related to electronic techniques and advancements in electronic data transmission and storage. In our paper, the user must first display their fingerprint in order to be verified as qualified to cast a ballot. The voter's information is retrieved from the tag via a fingerprint reader. The controller received the information from the reader and forwarded it along before comparing it to the data that has already been stored. A person was permitted to vote or poll their vote if the information matches the data that has been stored. If the information obtained from the fingerprint reader does not match the data that has been recorded, a notice will appear on the LCD screen. Using the switches, people cast their votes.

The system proposed by Rahil Rezwan, Huzaifa Ahmed, M. R. N. Biplob, S. M. Shuvo, and Md. Abdur Rahman [Huzaifa 2017] will be employed in a nation like Bangladesh. The electronic voting devices served as the system's foundation. They developed the database that houses the voter's fingerprint. When a fingerprint is put, the database that has been produced is checked for compatibility. The technology can tell if a voter is not registered or has registered more than once. The voter may cast their ballot if it matches the database.

The system tallies the votes and can display the results after a predetermined amount of time. This technique enables quicker results display. The findings are published more quickly and accurately thanks to this technology.

In their article from 2015, Anandaraj S, Anish R, and Devakumar P.V. describe various voting procedures.

The introduction of various voting machines. In our study, we list the drawbacks of computerised voting devices. It states that after recording their vote, voters using electronic voting machines will be able to acquire any acknowledgement. Votes are manually counted. Our article outlines a quick and secure approach for employing biometrics to cast ballots. The key goal is to make the model more flexible, secure, and scalable while also reducing the amount of time needed to announce results.

The voting process at this place utilised a fingerprint module. The person's fingerprint information was already in the official database. The computer, which has a complete record of the people who are entitled to vote, was connected to the voting machine. Because the touch screen was user-friendly, it was used. The identification survey was obtained using printers. The results were transmitted to the appropriate authority via a GSM module.

3. METHODOLOGY

The controller, fingerprint module, GSM module, keypad, power supply, and cloud are the main components of the functional block diagram of an IoT-based voting system with fingerprint identification.
This system's controller was an Arduino Uno. The laptop supplied the machine with power. The vote was counted using a keypad.

On the serial monitor, messages pertaining to system guidelines and any violations will be shown.

The voter's finger was placed on the fingerprint module, which was also used to hold the voter's fingerprint database.

The fingerprint module compares each user's fingerprint to the fingerprints stored in the database to determine who they belong to and displays a message if they do. The serial monitor will display the matching result. The cloud was used to store the voting ballots. Each candidate's final count was recorded in a different cloud field. Thing speak was utilised in this instance to store the candidate's final count. The controller receives cellular service from a SIM900 GSM Module. When someone casts their ballot for the second time, a buzzer sounds as a warning. The group was split into the voting unit and the finger-print unit.

The block diagram of the verification unit is shown in figure 3.1. It mostly addresses enrolment and matching. It primarily consists of the fingerprint module, which was used to save the voter's fingerprint and compare it to the database to see if they match. The voter's Aadhar number was also saved in this location. The system additionally validates each user's Aadhar number that is saved in the database. The system checks to see whether someone attempts to cast their ballot more than once. The second voting was announced via a buzzer.

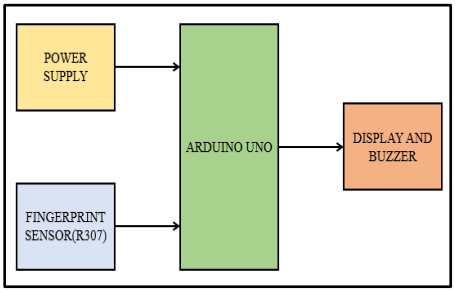

FIGURE 3.1BLOCK DIAGRAM OF VERIFICATION UNIT

Figure 3.2 illustrates how voting works. When the fingerprint device displays the message that the user was qualified to register to vote, they can do so through this unit. The register will be increased following the vote.

Voters have a choice in where they choose to cast their ballots. Voting was conducted using the keypad and Thing talk. Results can finally be seen on the Arduino's serial monitor.

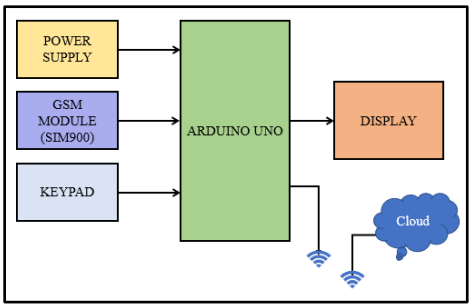

FIGURE 3.2 BLOCK DIAGRAM OF VOTING UNIT

3.1. SYSTEM WORKING:

The voter must first register their Aadhar number and fingerprint. The enrolled data will be compared during the voting process to see if there are any matches, and whether there have been any previous votes cast for that user. The buzzer alarm and "Already voted" message will appear if the voter has already cast a ballot. If they haven't voted before, they can register to vote via Thing Speak, where they can choose their country of residence and enter their vote, which will be added to the register. The results can then be acquired following the voting.

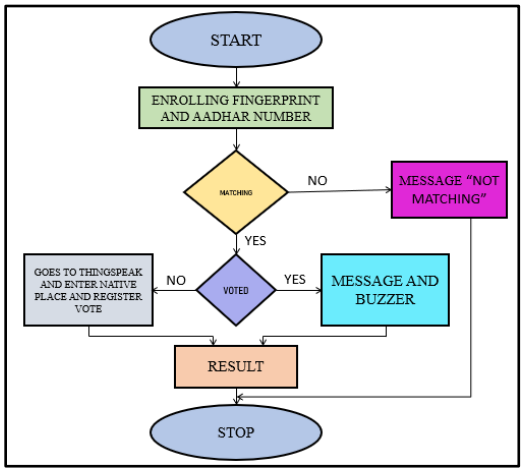

FIGURE 3.3 SYSTEM WORKING

3.2. HARDWARE REQUIREMENT:

FINGERPRINT SENSOR:

The optical fingerprint sensor, high-speed DSP processor, high-performance fingerprint alignment algorithm, high-capacity FLASH chips, and additional hardware and software components are all included in the fingerprint module. It has a simple structure, stable performance, and includes features for fingerprint entry, image processing, fingerprint matching, search, and template storage, among others. RS232 interface may be the TTL level, the default baud rate was 57600, can be changed, ask the communication protocol, microcontroller, like ARM, DSP and other serial devices with the connection, 3.3V- 5V microcontroller were often connected directly. Fingerprint module has the two interfaces TTL UART and USB2.0. USB2.0 interface were often connected to the computer.

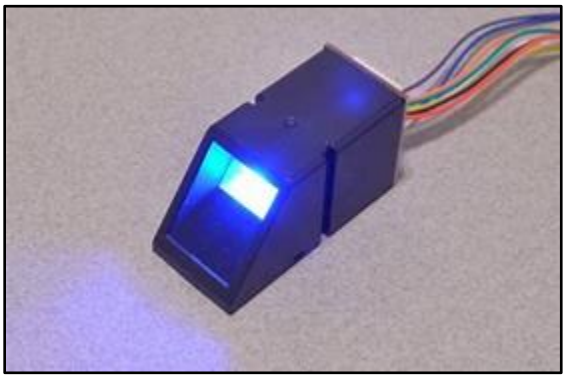

FIGURE 3.4 FINGERPRINT MODULE

SIM900 GSM MODULE:

A mobile device or computer and a GSM or GPRS system communicate using a chip or circuit known as a GSM module or GPRS module. The modem (modulator -demodulator) is crucial in this situation.

These modules are made up of computer communication interfaces (such as RS-232, USB 2.0, and others) as well as a GSM module or GPRS modem that is powered by the power supply circuit.

A GSM modem can be a standalone modem device connected through serial, USB, or Bluetooth, or it might be a mobile phone with GSM modem functionality.

FIGURE 3.5 SIM900 GSM MODULES

3.3. SOFTWARE REQUIREMENT

ARDUINO IDE:

The Arduino Integrated Development Environment (IDE), also known as the Arduino Software, includes a text editor for writing code, a message box, a text console, a toolbar with buttons for frequently used operations, and a number of menus. To upload programmes and communicate with the Arduino and Genuino hardware, a connection is made. Sketches are programmes created with the Arduino Software (IDE). These drawings were created using a text editor and saved with the .ino file extension. The editor offers tools for searching for and replacing text as well as for cutting and pasting. The message section indicates faults and provides feedback while storing and exporting. The console shows all text output from the Arduino Software (IDE), including error messages in their entirety and other data. The bottom right-hand corner of the window displays the configured board and serial port. The toolbar buttons allow verifying and the uploading programmes, creating, opening, and the saving sketches, and opening the serial monitor.

THING SPEAK:

The HTTP protocol is used by the open-source Internet of Things (IoT) application and API known as Thing Speak to store and retrieve data from objects over the internet or a local area network. The development of location tracking, sensor logging, and social networks of things with status updates are all made possible by Thing Speak. In Thing Speak, we must first create the account. Sign in to start a new channel. We will obtain the API key and channel id.

4. RESULTS

The suggested system was put into action. On this system, there were primarily two units: one for verification and

the other for voting. The Arduino IDE is used to programme the Arduino UNO. There were three possibilities in the verification unit: voting for the first time, voting more than once, and a discrepancy between the fingerprint and the Aadhar number. When a person attempts to vote for the first time, their fingerprint and Aadhar number are compared to the data in the database; if a match is found, they can register a vote and the message "Authenticated. Proceed" appears in the Arduino's serial monitor.

If an authenticated user attempts to register vote more than once, a buzzer sound is generated and the message "already voted" appears in the serial monitor. They will be unable to vote if their fingerprint and Aadhar number are not found in the database. The voter can register to vote in the voting unit by using the keypad via Thing Speak, and the authorised officer receives a summary of votes.

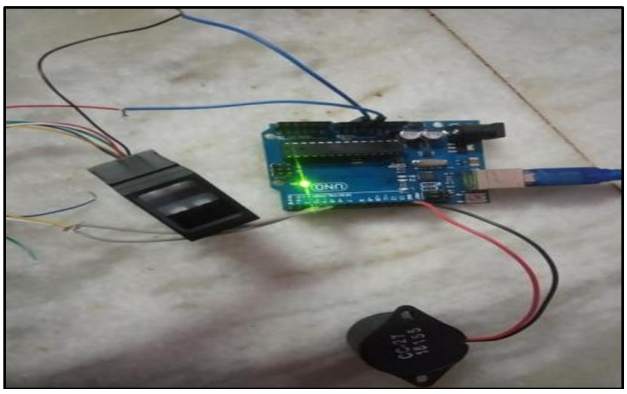

FIGURE 4.1 VERIFICATION UNIT

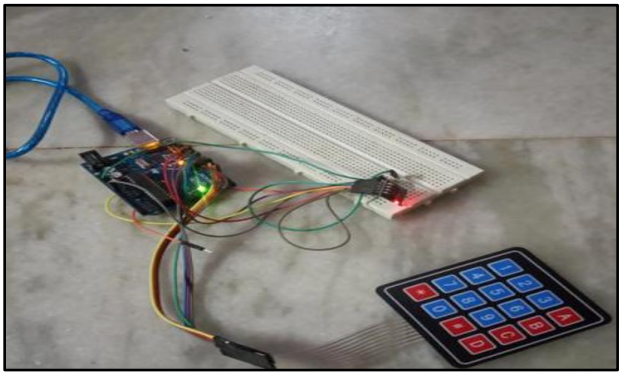

FIGURE 4.2 VOTING UNIT

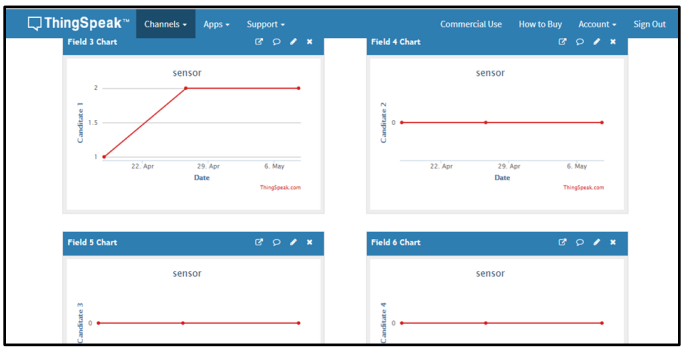

FIGURE 4.3 THING SPEAK

5. CONCLUSION

The voting system based on IoT was the proposal proposed here. Because India is a democratic country, all citizens have the right to select who leads them. The entire world was becoming digitised. Voting was also digitised as part of the digitalization process. One advantage of our project is that it shortens the time it takes to reveal the results. Biometrics and Aadhar number verification were used to make the system more secure. This mechanism only allows one person to vote once. Multiple voting was not permitted. This approach can also be used for postal voting.

6. FURTHER SCOPE

This voting mechanism contributes to the security of the vote. Using IoT-based voting, postal voting may likewise be made secure. This technique allows anyone to vote from anywhere on the planet. This technology is faster than the current ways for obtaining results. A controller with more memory aids in the storage of more data. More biometrics, such as facial recognition, iris recognition, and so on, can improve security. We can fully automate the system by improving online security.

REFERENCES

1. 2015 [Anandaraj] "Secured electronic voting machine employing biometric," by Anandaraj S, Anish R, and Devakumar P.V. IEEE's 2015 International Conference on Innovations in Information, Embedded, and Communication Systems will take place on March 19 and 20, 2015.

2. [Ashok 2012] Electronic voting machine, International Conference on Pattern Recognition, IEEE, Salem, Tamil Nadu, India, 21–23 March 2012, D. Ashok Kumar and T. UmmalSariba Begum Department of Computer Science, Government Arts, College.

3. 2017's Husaifa "Biometrically Secured Electronic Voting Machine," 2017 IEEE Region 10 Humanitarian Technology Conference (R10-HTC), Dhaka, Bangladesh, 21–23 December 2017. Huzaifa Ahmed, M. R. N. Biplob, Md. Abdur Rahman, Rahil Rezwan, and S. M. Shuvo.

4. [2016 Murali Prasad] "AADHAR based Electronic voting Machine using Arduino," by R. Murali Prasad, Madhu Nakirekanti, and Polaiah Bojja. 145th issue of the International Journal of Computer Applications (0975-8887), July 2016.