IoT Based Voting System For Elections

Aswathy Saji, Gopika Sreekumar Nair, Mekha Nair C A, Sidharth Minu, Shibu V S, Sabareesh R S

Department of Computer Science and Engineering
Mar Baselios College of Engineering and Technology,
Trivandrum, Kerala, India

Abstract—The proposed online voting system with biometric authentication is an electronic voting system which seeks to make use of the uniqueness of human fingerprint to further enhance the level of trust and confidentiality of the voters in the system.For the voter registration and authentication processes which are performed on the desktop module, the voter is expected to have his or her fingerprints captured and the minutiae extracted that are stored on the database by election commission admin. This is done to prevent the occurrence of multiple registrations or identity. Thus, during the authentication period, voters are expected to undergo a matching verification of their fingerprint samples against the values stored in the database which is identified through the use of a unique voter identification number assigned during voting The project will be able to achieve a high success rate in the use for conducting elections as it can stamp multiple registrations by voters through the combined use of both the unique voter identification number and their unique fingerprints. Voters can thus proceed to the voting panel of the project to cast their votes after fingerprint verification on successful verification the election commission member will send you a unique key to your mobile. Then the voting window will be unblocked by prompting voters' names. Then voters can enter the unique id & select the candidate he/she wished to vote after successfully voting the voter will get notified. If the authentication request fails he/she can't proceed voting.

.

1 Introduction

As Abraham Lincoln famously quoted democracy as ”Democracy is for the people, by the people, of the people”. One of the most attractive features of democracy is that it allows its citizens to choose their own leader which makes elections one of the most important events to occur in any democratic country.

India being the largest democracy in the world, serves as a role model to other countries aspiring for a democratic reign. This brings upon a huge responsibility on the country to conduct the elections as fairly as possible to show that people can in fact choose leaders they wish with minimal hassles and issues.

The Election Commission of India is the most important body, responsible for conducting elections. The elections should be conducted in the right manner to ensure that the term “Democracy” does not lose its value. After various experiences by the voters and large numbers of surveys, it has been observed that there are so many problems associated with our current voting procedures making it unjust. Some of them are tampering of votes,long queues and various other faults.

The main aim of the project is to avoid such tampering and misconduct during elections. The system consists of a biometric device to initiate voting. Prior to this, the user is required to register their fingerprint along with the personal details into the system and database for further reference and validation processes. After verification, The users can proceed to cast their votes.

2 Problem Definition

In our current scenario, voting for candidates is quite a task,because of the long waits and the foul plays and tampering that take place during the course of elections. Usual scenario witnessed is that a person from a particular party collects a few voter’s id and does their voting against their wish, ultimately leading to their win.

This is often witnessed in the rural and backward areas of the country. Inorder to avoid tampering of votes a marking on the finger is used. But even that can be removed using lubricants or other methods. It's not just uneducated people or the rurally backward society that have this problem, even people who are settled outside India and face this issue. For example, an NRI resident wouldn’t know if someone voted using his or her name.

There have been many instances where goons use violent means to hurt the voters and get them to vote for a particular party against their wishes. There exist various scenarios where the authorities themselves have been cornered and out forced to act against what they are supposed to do.

Issues like these pose a fundamental threat to the nation and its people because corrupt leaders elect themselves forcefully into being the decision makers. In circumstances like this, the whole meaning of democracy and the very point of people electing their leaders is lost.

3 Literature Review

This section elaborates on the various biometric voting systems introduced by experts over time. The review aims to give information about the proposed model followed by the pros and cons of the model.

Paper[3] suggests the use of GSM modules along with the biometric system for voting. A touch screen is implemented to overcome the button problem in a regular EVM and also to select suitable candidates during voting. The GSM module is used to send the results to the corresponding authority.A PC is used to store the details of people in the database. If a match is not found an alarm/buzzer is used to generate the error message.Although the system can be considered to be secure and reliable, it may not cater to a system that intends to conduct voting in multiple locations simultaneously.

The following paper[4] suggests a model that implements a biometric voting system using an EVM.Here the fingerprint is scanned and checked with the database. If the user exists, he/she is allowed to cast his vote using the EVM.In this system each EVM is used for a particular location and the winner candidate is declared by the EVM itself after a particular period of time.

The model proposed in the following paper[5] uses Aadhar card information for the election process. Two databases are maintained, one central and another local. The unique Aadhar card number and fingerprint is used to authenticate the voter. As each vote is casted, it will be updated onto the local database.

4 Area of Interest

4.1 Internet of Things

IoT has been a concept that has been gaining much popularity over the past years.The power or strength of IoT lies in the fact that various devices can be embedded into systems which can be controlled from any place, at any time.

These devices are capable of representing themselves virtually, that can be helpful in capturing more data from more places. All the way from improving the production of a factory to giving real time city updates on traffic and pollution, it's the Internet of

Things that acts as the common platform that puts together diverse information and provides a common language for different devices and applications to communicate with each other.

The basic process consists of heterogeneous devices connected to each other in a network and these devices communicate through the platform. This platform integrates data from all the available devices and performs various analytics to find patterns and other valuable data that is relevant to the connected applications or industry specifications.

Increasingly, organizations in various industries specializing in different domains have been using IoT to operate efficiently and provide better and more enhanced services to users, thereby increasing their market value.

5 Proposed System

The proposed system is an IoT based biometric voting system which uses a fingerprint module to register the user's fingerprint. At first, the user's fingerprint is saved to the device and then further on to the database. During the process of elections, users are requested to cast their vote where their fingerprints will be verified leading to the remaining set of activities.

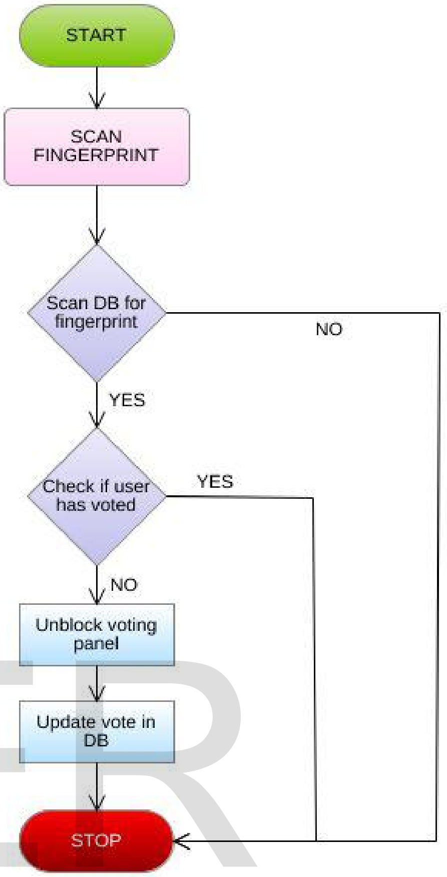


Fig 1: Flowchart

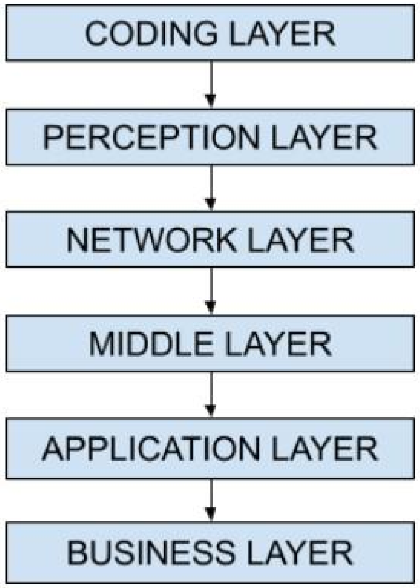


Fig 2: Basic Architecture

5.1 Basic Architecture

The system consists of a web based application which acts as an interface for most of the functions. The details collected from the application are subsequently stored to the database. The architecture of the system is based upon the functionality provided to different users by the system.

The Election Commission Admin is the primary member and is the ultimate authority of the entire process. The admin can view and publish the final count of votes. Admin is responsible for adding the election commission members to carry out the elections in various locations throughout the country. They are the ones responsible for maintaining the database and also the authorized personnel who is in charge of the software. Admin controls the events such as enrollment, updation and deletion.

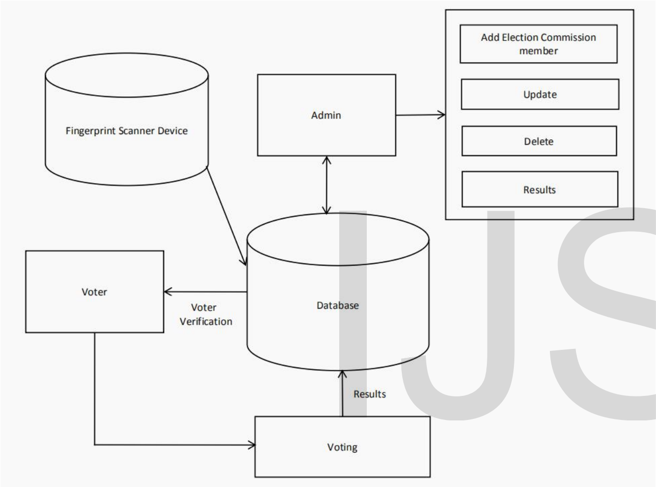


Fig 3: Application Design

Voters are required to provide the details and add their fingerprints to the device prior to the elections. The fingerprints are stored in both the device and the database.

The database consists of the following information:
Election Commission Admins
Election Commission Members
Candidate Details
Voter Details

Both the Admin and Member details consist of their username, password(encrypted), role and status information.
The variable ‘role' is used to identify if the member logging in is an Admin or a Member. For Admins, the role corresponds to ‘1' and ‘2' for members.
Similarly status is a variable used to check if the user logging in belongs to the election committee.
If the user is in the committee, the status corresponding will be ‘1' or else ‘0' and will be denied access to the system. This is to ensure any misoccurances from the authorities.

The candidate details comprises personal details of the candidate and details about their party.

The voters part of the database includes their essential details such as location, contact information, and their fingerprints which will be obtained from the device and stored as a bio_id.

The flowchart in Fig 2. gives an outlook of the proposed system.

5.2 Software Design

Software design includes 3 actors:-
1.Election Commission Admin
2.Election Commission Members
3.Voters

Election Commission Admin :-
Admin is the authority responsible for the entire database for an election.
Adding commission members, deletion and updation of records and publishing results are some of the main roles performed.

Election Commission Members :-
Responsible for collecting voters information and fingerprint
In charge of the procedures on the day of election in assigned locations
Can perform additions, updations and other modifications to the voter and candidate details.

Voters :-
Have to register in assigned locations submitting details and fingerprints.
On the day of elections, after the verification they can cast their votes.

6 System Components

This section of the report puts forward information about the various software and hardware components being used in the project.

6.1 Software

- FRONT END
  - Software is designed entirely using PHP.
  - Laravel framework is being used. Laravel provides a secure and stable platform to design the application flexibly as per requirement. It also provides functions to encrypt the passwords for security.
- BACK END
  - MySQL is used to store the details regarding voters,candidates and election commission members.

- Database will consist of voter details along with their fingerprint information stored as bio-id.

6.2 Hardware

1. Fingerprint Scanner Device

i. Finger Placement

A fingerprint scanner is being used to collect the voters fingerprints. The collected fingerprints are stored in the device and further in the database as bio_id.

Below mentioned are the most effective ways to use the device and record the fingerprint:

- Recommended Fingers

The index finger and the middle finger is usually preferred ; Thumb and little fingers are usually avoided as they can be clumsy.

- Finger Placement

a. Correct Method

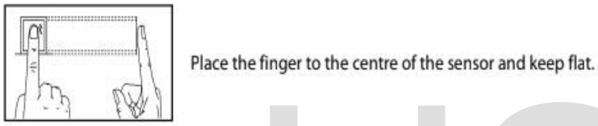


Fig. 4. Correct Placement

b. Incorrect Method

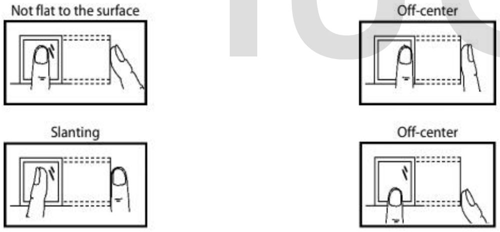


Fig. 5. Incorrect Placement

ii. Basic Concepts

a) **User Enrollment**

Typically users can enter upto 10 fingerprints using one ID number for multiple selections.

Theoretically all 10 fingers are preferred, however it is better to store the index and middle finger prints for maximum accuracy.

b) **User Verification**

This is the first step to initiate the voting process. When the voter scans his/her fingerprint, the device tries to match it with the prints stored in the device and the database. Upon successful verification, the user can proceed with voting.

The scanning is a 1:N process as the just entered print is made to find a match with the remaining templates in the device.

Fingerprint Verification :-

The two matching modes that can be used to verify the prints are 1:1 and 1:N.

(1) **1:1 fingerprint matching** : Here the voter's scanned fingerprint is compared to the ID number entered manually.

(2) **1:N fingerprint verification** : In this mode of verification, the scanned fingerprint is compared with all the templates in the device for a match.

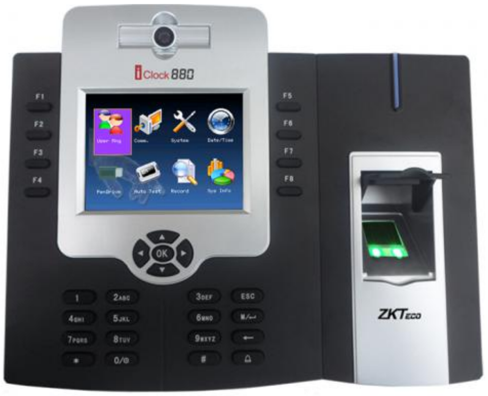
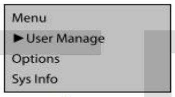


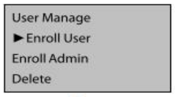
Fig 6. Fingerprint Scanner

iii. Deleting Enrolled Data

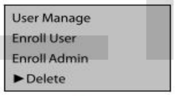
A user whose details have been enrolled into the device can be deleted following the series of steps demonstrated below(Specific to the device being used) :



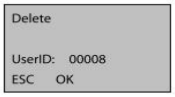
1



2



3



4

iv. TTS Web Server

Usually used for the text-to-speech configuration of the device. TTS related statements can be modified in the device settings to enable it. The changes will have to be saved and the device has to be restarted for the configurations to show.

Here the username is set by default and cannot be modified while the password can be changed.

v. External Connection with Fingerprint Reader

This feature is used on devices with USB interfaces. This feature helps to connect an external fingerprint reader to read the voters finger prints. Similar to the TTS configuration, to enable an external connection we need to alter the settings and restart the device.

vi. SOAP Interface

Definition :

SOAP is a protocol commonly used for exchange of data in a distributed, decentralized environment. It is a lightweight protocol with a capability to provide a scalable message handling framework using XML technology. The framework has been designed in such a way that it is independent of any particular programming model or any specific semantics.

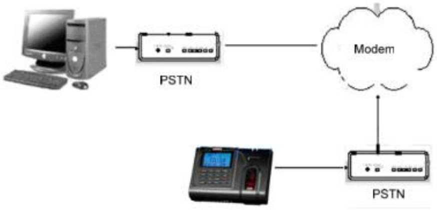


Fig 7: Schematic dagram of the connection

Application:
The device supports XML-based SOAP data interface. SOAP requests can be embedded in the program to download and upload the information and use it for fingerprint verification.Furthermore, user details can be imported, and also other required fingerprint data and verification records necessary can be accessed.

vii. POE Function

Overview:
Power over Ethernet is a feature that allows the use of DC power with the data to be provided to the Ethernet based terminal equipment without making changes to the architecture. This equipment can be a wireless LAN access point or an IP phone.
The two major components used in PoE are:-

- Power Sourcing Equipment (PSE), used to deliver power.
- Powered Device (PD), used to receive and utilize the power.
- Power and data are integrated in the same cabling system for PoE while Cat5/5E cables are used for data delivery and DC power transmission.

Advantages:

- Cost-effective as it is only required to support a single cable. PoE can enable an increasing number of devices over Ethernet, hence greatly reducing deployment costs keeping device management very simple.
- Easy-to-install and easy-to-manage.
- Safe as it only supplies powers to devices that require it, eliminating the creepage risk..
- Ease of management of network devices.

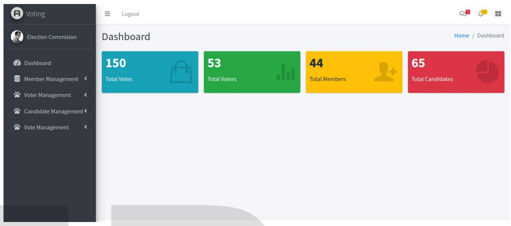
2. ROUTER

It is used to connect the fingerprint scanner to the system to enable transfer of fingerprints and other details to and from the database.

FIG. 8

7 RESULT

The proposed system delivers a result as expected by the architecture. The votes are updated into the database which is then calculated and the results are displayed on the admins page and as a consolidated result on the dashboard as shown below. After various levels of testing, the system is seen to be about 97% accurate with its results.



Dashboard

150 Total Votes

53 Total Voters

44 Total Members

65 Total Candidates

8 CONCLUSION

Our proposed electronic voting system with biometric authentication aims at implementing a voting system that mainly uses the human fingerprint as a key property to enhance the confidentiality in the voting process. We aim to eliminate tampering and other foul plays associated with voting thereby enhancing and maintaining confidentiality and security.The proposed electronic voting system is faster and more efficient in terms of security than the conventional systems that are being used over the years. The application prevents illegal voters and multiple votes being cast by a single voter.
It is much easier to use, transparent and maintains integrity of the process. The system checks the eligibility of the voter and prevents multiple entries by a single individual.Fingerprint based voting system reduces polling time, reduces the equipment to be carried to each polling booth ultimately enhancing portability. An electronic voting process can be carried out much easily compared to the conventional paper ballot system, and reduces the staff in every voting centre. It provides easy and accurate counting without any troubles.The system also aims at providing a fair and equal opportunity to every citizen to cast their vote and elect a leader without any biases as democracy suggests. As a whole, our system expects to overcome most of the problems faced during the voting period by the conventional paper ballot system. This will ensure a more secure voting procedure which is quite a necessity at this point.

References

[1]Naik, Devendra Vijay. "Smart wireless authenticating voting machine." In *2015 International Conference on Communications and Signal Processing (ICCSP)*, pp. 0785-0788. IEEE, 2015.

[2]M. Khasawneh, M. Malkawi, O. Al-Jarrah, L. Barakat, T. S. Hayajneh and M. S. Ebaid, "A biometric-secure e-voting system for election processes," 2008 5th International Symposium on Mechatronics and Its Applications, Amman, 2008, pp. 1-8, doi: 10.1109/ISMA.2008.4648818.

[3] 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, 2015, pp. 1-5.

[4] R. Rezwan, H. Ahmed, M. R. N. Biplob, S. M. Shuvo and M. A. Rahman, "Biometrically secured electronic voting machine," 2017 IEEE Region 10 Humanitarian Technology Conference (R10-HTC), Dhaka, 2017, pp. 510-512.

[5] C. J. Lakshmi and S. Kalpana, "Secured and transparent voting system using biometrics," 2018 2nd International Conference on Inventive Systems and Control (ICISC), Coimbatore, 2018, pp. 343-350.