AADHAR BASED ELECTRONIC VOTING SYSTEM USING BIOMETRIC AUTHENTICATION AND IOT

Sarankumar.V\textsuperscript{1}, Sasi Kumar.M\textsuperscript{1}, Ramprabu.K\textsuperscript{1}, Sathishkumar.A\textsuperscript{1}
Mr. S. Gladwin Moses Stephen \textsuperscript{2}
\textsuperscript{1}Student, \textsuperscript{2}Assistant Professor
Department of Electronics and Communication Engineering,
Akshaya College of Engineering and Technology, Coimbatore

Abstract—The main purpose of this project is to develop a secure Electronic voting machine using Finger print identification method, for finger print accessing we use AADHAR card database model which is a safe and secure system to avoid misconceptions taking place in elections. Aadhaar enrolment process was done in India few years back. At that time, Indian government collected details of finger prints and IRIS of every individual. This entire data of each and every person persists in the database of Indian government. If Indian Government links this database to voter Id present in today’s voting system, then everyone can easily cast their votes using fingerprint authentication. In this system a confirmation message is sent to the voter’s registered mobile number regarding the casted vote. Also the voted data and voters details can be sent to the nearby Database Administration unit using IOT. If an unauthorized person enters into polling booth to cast his vote or if already vote casted person enters into booth with his RFID tag for 2nd time voting, buzzer will alert booth level officer. Using this biometric system for voting purpose, we can easily avoid rigging in elections.

Keywords— Arduino Mega, Fingerprint, RFID, Aadhar, Electronic Voting System, IOT, SMS

I. INTRODUCTION
This paper determines policy regarding the electronic approaches and developments towards data storage and transmission. The user should show his voter ID card whenever he goes to the booth to poll his vote which is often a time consuming method because the person needs to check the voter ID card with the list he has, make sure it as an authorized card and then enable the person to poll his vote. To avoid this type of problems, a finger print based voting machine wherever the individuals no ought to carry his ID which contains his entire details is designed. The voter places his Finger on the fingerprint module. This information is passed to the controlling unit for the verification and the controller reads DATA from the reader and compares this data with the already existing data. If the data matches with the already stored information, the person is allowed to poll his vote. If not, a message is displayed on LCD and therefor e the person isn't allowed to poll his vote. The polling mechanism carries out manually using the switches. LCD is employed to display the related messages. Voting is a method by which the electorates appoint their representatives. The objective of voting is to permit voters to exercise their right to express their choices regarding specific issues, items of legislation, citizen initiatives, constitutional amendments, recalls and/or to decide on their government and political representatives. Technology is being employed additional and more as a tool to help voters to cast their votes. To permit the exercise of this right, the majority voting systems around the world include the following steps: citizen identification and authentication, voting and recording of votes cast, vote counting, publication of election results. Voter identification is needed during two phases of the
electoral process: first for voter registration so as to determine the right to vote and subsequently, at voting time, to allow a citizen to exercise their right to vote by verifying if the person satisfies all the necessities required to vote (authentication). Security could be a heart of e-voting method. So the requirement of designing a secure e-voting system is very vital. Usually, mechanisms that ensure the security and privacy of an election are often time consuming, expensive for election administrators, and inconvenient for voters. There are completely different levels of e-voting security. Also, security should be applied to hide votes from publicity. There’s no measurement for acceptable security level, as a result of the extent depends on kind of the information. An appropriate security level is always a compromise between usability and strength of security method. The secured e-voting process can be done by linking the voting machines with the Aadhar, an Indian citizen identification data base with a unique identification number for every citizen. The Aadhar based EVS can result in secured e-voting process. As a result of no two or more voter’s data can match as this system uses biometrics.

Biometrics is the science and technology of measuring and analyzing biological data. In information technology, biometrics refers to technologies that measure and analyze human body characteristics, such as DNA, fingerprints, eye retinas and irises, voice patterns, facial patterns and hand measurements, for authentication purposes. During this paper used thumb impression for the purpose of voter identification or authentication. As the thumb impression of each individual is exclusive, it helps in maximizing the accuracy. Aadhar database is created containing the thumb impressions of all the voters in the constituency. Illegal votes and repetition of votes is checked for in this system. Hence if this system is utilized the elections would be truthful and free from rigging.

II. SYSTEM ANALYSIS AND RELATED WORK

1) RFID:

In this paper, RFID tags have been used. Each and every tag contains the information related to individual voters. Our micro controller Arduino Mega 2560 contains the details of the voter. When RFID tag placed near to RFID reader, RFID reader activate the details of particular information of RFID tag which is preloaded into micro controller memory. RFID tag transmits its information to the RFID reader by taking advantage of the fact that each time the tag draws energy from the RFID reader's magnetic field, the RFID reader itself can detect a corresponding voltage drop across its antenna leads. Capitalizing on this phenomenon, the tag can communicate binary information to the reader by switching ON and OFF a load resistor to perform load modulation.

2) Fingerprint Identification Module:
Fingerprint processing includes two parts: fingerprint enrollment and fingerprint matching. When enrolling, user needs to enter the finger two times. The system will process the two time image and store the template. When matching, user enters the finger through optical sensor and system will generate a template of the finger based on processing results and store the template. When matching, system will compare the live fingerprint with specific template designated in the Module; for 1:N matching, or searching, system will search the whole finger library for the matching finger. In both circumstances, system will return the matching result, success or failure. Fingerprint is very safe and convenient device for security instead of password that is vulnerable to fraud and is hard to remember biometric process for authentication, identification and verification functions that let your fingerprints act like digital passwords that cannot be lost, forgotten or stolen.

3) Liquid Crystal Display:
LCD stands for Liquid Crystal Display. LCD components are “specialized” for being used...
with the microcontrollers, which means that they cannot be activated by standard IC circuits. They are used for writing different messages on a miniature LCD. When user places RFID tag near RFID reader, user details will be displayed on LCD screen. Then the voter is allowed to cast his vote. If LED blinks once, then one message will be shown like this in the LCD screen, “VOTED SUCCESSFULLY”.

4) RS232 (Serial Communication Interface):
In this project, RS232 serial data transmission cable is used to connect finger print module with Arduino. In general images will be store in chip memory in the form of binary digits like ON(1) and OFF(0). Like this, voters finger print also stored in the memory of Arduino in the form of Binary digits. When we place our finger for biometric authentication, the data will be transfer to microcontroller in the form of stream of bits serially through RS232 cable. This entire stream of bits will be collected and compared by microcontroller. If perfect match found, voting process initiated.

UART (Universal Asynchronous Receiver Transmitter) or USART (Universal Synchronous Asynchronous Receiver Transmitter) are one of the basic interface which you will find in almost all the controllers available in the market till date. This interface provides a cost effective simple and reliable communication between one controller to another controller or between a controller and PC.

III. DESIGN AND IMPLEMENTATION
In this technique, the details of the voter can get from the AADHAR card database. It is the newly developed information which has all the information concerning the people. By using this database took the voter’ information will be stored within the personal computer. At the time of elections, for finger print accessing used finger sensing module.

Fingerprint verification could also be an honest choice for in e-voting systems, where you can provide users adequate explanation and training, and where the system operates in a controlled environment. It is not stunning that the workstation access application area looks to be based almost exclusively on finger prints, as a result of the relatively low price, small size, and easy integration of fingerprint authentication devices. Capture the finger vein image and compare or match to database, capture finger vein and database finger vein matched suggests that this person will be valid for polling section and if condition is satisfied automatically.

The elector forge his/her vote using the user interface provided on the system application. After the completion of his/her voting process, a “voting successfully” message is displayed on the screen. The amount of votes is counted by the system and therefore the data are sent to the Server through the online technology.

In earlier days the election process is in such a way that there will be a box and a paper with all the political parties list. Whereas voting the voter has to put a stamp over the party symbol of his/her desired candidate in a specific consistency.
This is an extended time consuming method and extremely a lot of prone to errors. Additionally the probabilities for rigging were a lot of during this traditional methodology. To beat of these ballot papers, stamps, boxes etc., going for Aadhar based EVS. So that, to beat time consumption, Rigging and insecurities. Here in Aadhar primarily based EVS, using the information primarily based server for Aadhar details, Internet of things for the online technology and Arduino is employed for interfacing with all other modules.

Fig2. Process Flowchart of EVS

The elector has to scan his thumb mistreatment the biometric and providing the thumb data that’s scanned is matched with the pre-loaded server information the elector can permit to forge the vote. Otherwise the Authentication will fail and voter will not be able to cast the vote. Once the voter is authenticated the details of parties will enable and conjointly the data of elector are shown on the system. When casting the vote the switches are disabled till next voter is authenticated and LCD shows a message as “thank you for voting”. Then after exiting the user interface a SMS is sent to the voter’s registered mobile number regarding the voting. The token is additionally useful to verify the vote casted by the voter. The overall data of casted votes is distributed to the server mistreatment net technology in order that the results are often declared among all the consistencies.

IV. SYSTEM TESTING AND EVALUATION

Fig3. Aadhar – Voter Id linking and enrollment model

Fig4. Voting System User Interface
To assess the functionality of the EVS, we made ten different entries to the systems using 10 AADHAR cards as prototype national voter ID cards. These ID cards were assigned to each person and their corresponding information and fingerprint ID were entered into the system. For the test, the candidates for votes were listed as #1, #2 and so on. To check the accuracy of the fingerprint device a total of ten fingerprints were stored in the fingerprint sensor’s memory. The confidence level received for the each of these fingerprints was collected in experimental trials. The graph in Fig. 5 shows the trend of the confidence level with the number of trials. When plotted for the best line, a linear curve with confidence level of higher than 100 was received as illustrated in Fig. 6. This demonstrates a good accuracy and the reliability of the fingerprint sensor.

The test for the system’s usability and user-friendliness was determined by carrying out a survey among a group of selected people. On a scale of 1 to 10, feedback was taken from 10 participants. It is evident from the modal score of 6 on usability that most users found the system to be fairly usable. On the other hand, the highest frequency score for user friendliness was 8, indicating that the system is highly user-friendly.

V. CONCLUSION AND FUTURE WORK

It is important to mention that the concept of electronic voting systems is not just a novel theory. The process taken up under the limited scope of this research aims to demonstrate an implementation for fault free voting and a larger scale of the voting frontier. Thus the machine still has certain limitations that may need to be overcome to allow it to reach the next level. The devices integrated in this prototype need to be upgraded to more robust and durable alternatives for large scale production as the fingerprint device we use, can store a total of 256 fingerprints but for mission critical scenarios, the fingerprint reader should be linked to a dynamic database. In this version the Graphical User Interface should be easier and limited to be handled by the voter. The obvious advantage of biometrics is that it cannot be altered or copied and the window of impersonation is nullified. To allow transparency with the user of the system, the SMS sent through the GSM module to the voter’s registered mobile number. The advantage of not handing out a ballot to the user means that the voter is not able to manipulate or misplace the vote. Overall, the system shows an attempt towards better confidence of electronic voting machines. The integrated system eradicates common issues faced and ensures both voters and candidates a trusted means for elections. In future if, IRIS Technology is adopted for authentication purpose, we can get better results compared to Biometric System. If networking is provided among polling booths
with AADHAAR data collected Server with the help of internet, we can easily get better security.

REFERENCES


