UNSUPERVISED SECURED ELECTRONIC VOTING MACHINE

Secured electronic voting machine using the biometric identification of voters

[1]Aiswarya K, [2]Anagha D, [3]Anjaly V Sajeev, [4]Aparna S

Department Of Electronics and Communication Engineering,
NSS College of Engineering, Palakkad, Kerala.

***Abstract*—The EVM (electronic voting machine) in India suffers many security issues .Electronic voting is a term encompassing several different types of voting, embracing electronic means of both casting and counting votes. In the proposed system, the voting system is managed in an easier way as all the users should login by verifying his/her iris scan linked with aadhar database and click on his/her favorable candidates to cast the vote. This features a larger security in the sense that voter high security password is confirmed before the vote is accepted in the main database of ECI. The extra feature of the model is that the voter will ensure if his/her vote has gone to correct candidate/party. The votes are going to be done automatically, therefore saving an enormous time and facilitate ECI to announce the result at a very short time period.**

***IndexTerms*—Arduino, Biometric identification, Finger print, Iris scan**

I. Introduction

The project proposes a Secured Unsupervised Electronic Voting Machine where in the requirement of more than a single polling officer is not required. Unlike the existing election system, the officer need not check each voter manually and instead each voter is identified using his unique biometrics. In this ubiquitous network society, information is available easily to everyone, anytime and anywhere. Hence a more secured form of voting is the need of the hour. Since each voter is identified using his unique biometrics, faking of votes can be avoided, making this system more secured. Our idea is to make it secure by identifying each user by the fingerprint verification and face verification method. Because the identification data is inside the body, the forging or faking of votes is nearly impossible making it a very secure system. The identified voter, if valid can proceed for casting his vote after which an SMS is sent to the registered mobile number.

In the modern world, there is an increasing need for electronic services and their security. Usages of new technology in the voting process improve the elections in natural. This new technology refers to electronic voting systems where the election data is recorded, stored and processed primarily as digital information. In the past, usually, information security was used mostly in military and government institutions. But, now need for this type of security is growing in everyday usage. In computing, e services and information security is necessary to ensure that data, communications or documents (electronic or physical) are secure and privacy is enabled. Advances in cryptographic techniques allow pretty good privacy on voting systems. Security is a heart of electronic voting process. Therefore the necessity of designing a secured electronic voting system is very important.

Usually, mechanisms that ensure the security and privacy of an election can be time-consuming, expensive for election administrators, and inconvenient for voters. Therefore serious measures must be taken to keep it out of public domain. An acceptable security level is always a compromise between usability and strength of security method. Authenticating voters and thus securing the data are most important. It ensures that vote casting cannot be altered by unauthorized person.

II. EXISTING ELECTRONIC VOTING MACHINE

Electronic Voting Systems (EVMs) have replaced paper ballots in local, state and general (parliamentary) elections in India. Indian voting machines use a two-piece system with a balloting unit presenting the voter with a button (momentary switch) for each choice connected by a cable to an electronic ballot box. An EVM consists of two units, control unit and balloting unit. The two units are joined by a five-meter cable. The control unit is with the presiding officer or a polling officer and the balloting Unit is placed inside the voting compartment. Instead of issuing a ballot paper, the officer in-charge of the Control

Unit will press the Ballot Button. This will enable the voter to cast his vote by pressing the blue button on the balloting unit against the candidate and symbol of his choice. The controller used in EVMs has its operating program etched permanently in silicon at the time of manufacturing by the manufacturer. No one (including the manufacturer) can change the program once the controller is manufactured.

III. SECURITY ISSUES FACED

In the existing EVM each voter is identified using his voter ID which can be easily faked. This identification of voter is done by the polling officer and to err is human, which can result in an unfair biased election result. The recorded vote need not be necessarily cast by the recorded person. The existing EVM does not have any option to let the voter know if his vote has been successfully recorded. Faking of votes is easier as there is no way to uniquely identify the voters. A candidate can know how many people from a polling station voted for him. This is a significant issue particularly if lop-sided votes for/against a candidate are cast in individual polling stations and the winning candidate might show favoritism or hold grudge on specific areas. The control units do not electronically transmit their results back the Election Commission, even though a simple and unconditionally secure protocol for doing this exists. The Indian EVMs are purposely designed as stand-alone units to prevent any intrusion during electronic transmission of results. Instead, the EVMs are collected in counting booths and tallied on the assigned counting day(s) in the presence of polling agents of the candidates. EVMs are vulnerable to India's varied climate which has great extremes of temperature and humidity, as well as other environmental hazards such as dust and pollution.

IV. THE PROPOSED SYSTEM

Commercial electronic voting systems have experienced many high-prole software, hardware, and usability failures in real elections. While it is tempting to abandon electronic voting altogether, the proposed system shows how careful application of biometric identification systems can yield voting systems that surpass current systems and their analog forebears in trustworthiness and usability. The secured electronic voting system is a complete electronic voting system that combines several recent research results into a coherent whole that can provide strong end-to-end security guarantee to voters. The system also allow any voter to challenge the system, while the election is ongoing, to produce proof that ballots are cast as intended. The proposed system design offers a number of pragmatic benefits that can help reduce the faking of votes and impact of poll worker or voter errors.

Features:

The main goal of a secure voting system is to ensure the privacy of the voters and of the votes. A secure e-voting system satisfies the following requirements,

- Eligibility: only votes of legitimate voters shall be taken into account.
- Anonymity: votes are set secret.
- Accuracy: cast ballot cannot be altered. Therefore, it must not be possible to delete ballots nor to add ballots, once the election has been closed.
- Fairness: partial tabulation is impossible.
- Vote and go: once a voter has casted their vote, no further action prior to the end of the election.
- Public verifiability: anyone should be able to readily check the validity of the wholevoting process.

Components Used

Fingerprint recognition or fingerprint authentication refers to the automated method of verifying a match between two human fingerprints. Fingerprints are one of many forms of biometrics used to identify individuals and verify their identity. Here we use the R305 optical Fingerprint scanner module. Fingerprint processing has three primary functions: enrolment, searching and verification. Among these functions, enrolment which captures fingerprint image from the sensor plays an important role. For this purpose we use a software the SFG Demo, the interfacing of which is shown in Fig.4.2.Using the software support, we can enroll the fingerprints which are stored within the module and can be used later on for voter authentication. The recorded images are stored within the R305 module as a database. The fingerprints are stored in addresses which can be retrieved while verification. R305 and S630 are common modules used for fingerprint scanners, with the aid of a powerful DSP in its core. Basically both of these modules work the same way, we can communicate with them using a packet of hex codes in a specific format.

Arduino is an open source, computer hardware and software company, project, and user community that designs and manufactures micro controller kits for building digital devices and interactive objects that can sense and control objects in the physical world. The project's products are distributed as open-source hardware and software. Arduino board designs use a variety of microprocessors and controllers. The boards are equipped with sets of digital and analog input/output (I/O) pins that may be interfaced to various expansion boards (shields) and other circuits. The boards feature serial communications interfaces, including Universal Serial Bus (USB) on some models, which are also used for loading programs from personal computers.

The GPRS Shield is compatible with all boards which have the same form factor (and pinout) as a standard Arduino Board. The GPRS Shield is configured and controlled via its UART using simple AT commands. Based on the SIM800 module from SIMCOM, the GPRS Shield is like a cell phone. Besides the communications features, the GPRS Shield has 12 GPIOs, 2 PWMs and an ADC. This is an ultra-compact and reliable wireless module. The GPRS Shield is compatible with all boards which have the same form factor (and pinout) as a standard Arduino Board. The GPRS Shield is configured and controlled via its UART using simple AT commands. Based on the SIM800 module from SIMCOM, the GPRS Shield is like a cell phone. Besides the communications features, the GPRS Shield has 12 GPIOs, 2 PWMs and an ADC.

V. DESIGN AND IMPLEMENTATION

Supply Section of this circuit consists of a 12 volts adaptor. The output of the regulator is +5 volts, which is used for all other digital applications. The voting machine consists of four keys, which are connected to four separate pins of microcontroller. These pins are made high to act as input port .The display section uses the port 1 of microcontroller. This port is in open drain configuration and as a result, pull up resistors should be provided for its normal operation. The contrast of this LCD display is adjusted by changing the value of a resistor which is grounded at the other end. The EEPROM memory is used to store the details relating to the voter and indicating whether a voter has already voted or not.R305 device operates at 57600 baud rate. This circuit requires three serial port connections which is accomplished by one hardware and two software communications. The pins are configured accordingly. A 16*4 LCD is also interfaced with Arduino board.SIM800 GSM module is used for message transfer to the registered mobile.

The Fingerprint is one of the safest way to detect and identify the Authorized person,We know that fingerprint is unique even identical twins do not have identical fingerprints. By using this we can make pretty sure about security needs. To add fingerprint verification we can use the optical fingerprint sensor-scanner (R305). It makes fingerprint detection and verification super simple. In the circuit shown, the power and ground pins are connected accordingly and the transmit and receive pins of both the Arduino and fingerprint module is interconnected. Using the software support, we can enroll the valid fingerprints which can be used to create database and further can be used for detection and verification in real time. The fingerprints are stored in the form of addresses and this address can be retrieved while verification.

VI. Acknowledgment

We acknowledge our sincere thanks to the management of N.S.S College of Engineering for providing assistance for our Project. We would like to express our gratitude to Dr.T SUDHA, Principal, N.S.S College Of Engineering, Palakkad. We take this opportunity to express our profound gratitude to Prof.KALA L, Head of the Department of ECE and all staffs of the department for their valuable feedback. We express our sincere gratitude to Prof.ANOOP S PILLAI, our project guide and Prof.VIJITHA S, our staff in charge, for their guidance and valuable support towards the project.

Above all we thank Almighty for guiding our steps.

References

[1] Intelligent Electronic Voting Machine with Image Processing by Mr. S. Gowri Shankar and Ms. D. Vijayalakshmi,JECET, March 2015-May 2015, Sec. A Vol.4.No.2, pages 219-225.

[2] Design of Secured Wireless Electronic Voting Machine for Data Acquisition by Subhadeep Chakraborty, Dip Laha, Payel Kundu, Indrajit Ghosh, September 2015, Vol.5, Issue 9, pages 222-227

[3] Electronic Voting System in India by Murugan Mahalingam, Article in IEEE Circuits.

[4] Iris Recognition based Voting System by J Nithya, International Conference on Science and Technology.

[5] Palm Vein Technology by K. R. Deepti, Dr. R. V. Krishnaiah, International Journal of Computer Engineering and Applications, Vol. II, Issue I/III, ISSN 2321-3469.

[6] Integrity of Electronic Voting System: Use of Cryptography by Computer science and Engineering Department, University of Connecticut.