www.ijecs.in

International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume – 5 Issue -03 March, 2016 Page No. 16033-16037

Advanced Secure Voting System with IoT

Ms. Nithya.S[1], *Mr.Ashwin.C*[2], *Mr.Karthikeyan.C*[3], *Mr.Ajith kumar.M*[4]

[1]Assistant professor, ECE, KPR Institute of Engineering and Technology, Coimbatore.
nithyakpr@gmail.com

[2,3,4] Students , ECE, KPR Institute of Engineering and Technology, Coimbatore
ashwinchinnadurai@gmail.com karthi28avi@gmail.com ajithmbe@gmail.com

ABSTRACT: ***It has always been an arduous task for the election commission to conduct free and fair polls in our country, the largest democracy in the world. Crore of rupees have been spent on this to make sure that the elections are riot free. But, now-a-days it has become common for some forces to indulge in rigging which may eventually lead to a result contrary to the actual verdict given by the people. This paper aims to present a new voting system employing biometrics in order to avoid rigging and to enhance the accuracy and speed of the process. The system uses thumb impression for voter identification as we know that the thumb impression of every human being has a unique pattern. Thus it would have an edge over the present day voting systems. As a pre-poll procedure, a database consisting of the thumb impressions of all the eligible voters in a constituency is created. During elections, the thumb impression of a voter is entered as input to the system. This is then compared with the available records in the database. If the particular pattern matches with anyone in the available record, access to cast a vote is granted. But in case the pattern doesn't match with the records of the database or in case of repetition, access to cast a vote is denied or the vote gets rejected. Also the police station nearby to the election poll booth is informed about the identity of the imposter. All the voting machines are connected in a network, through which data transfer takes place to the main host. The result is instantaneous and counting is done finally at the main host itself. The overall cost for conducting elections gets reduced and so does the maintenance cost of the systems.***

Keywords: finger print scanner, PIC 16F877A, Gsm Module, Cloud Storage.

.

1. Introduction

As the modern communications and Internet, today are almost accessible electronically, the computer technology users, brings the increasing need for electronic services and their security. Usages of new technology in the voting process improve the elections innatural. 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 growing in everyday usage. In computing, services and information security it is necessary to ensure that data, communications or documents (electronic or physical) are enough secure and privacy enabled. Advances in cryptographic techniques allow pretty good privacy on e-voting systems. Security is a heart of e-voting process. Therefore the necessity of designing a secure e-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. There are different levels of e-voting security. Therefore serious measures must be taken to keep it out of public domain. Also, security must be applied to hide votes from publicity. There is no measurement for acceptable security level, because the level depends on type of the information. An acceptable security level is always a compromise between usability and strength of security method. The authenticating voters and polling data security aspects.

2. ISSUES OF EXISTING VOTING SYSTEM:

Elections are a defining feature of democratic government, but all too frequently, we take the actual mechanics of the election for granted. We speak at length of such issues as who is allowed to vote, how campaigns are conducted, and how they are financed, but no one gives priority to the understanding of the actual voting process. Electronic Voting Machines ("EVM"), Idea mooted by the Chief Election Commissioner in 1977.The EVMs were devised and collaboration with Bharat Electronics Limited (BEL), Bangalore and Electronic Corporation of India Limited (ECIL),Hyderabad. The EVMs are now manufactured by the above two undertakings. An EVM consists of two units, i) Control Unit, ii)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.

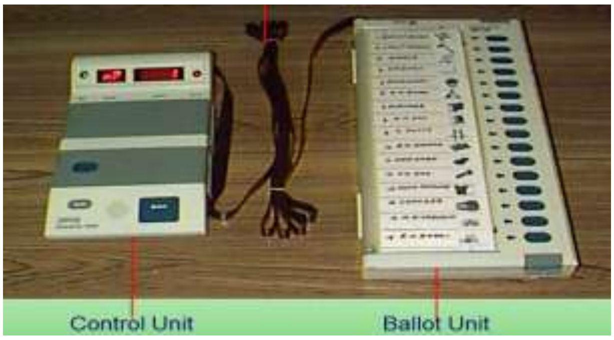


Fig 1

. It ensures that vote casting cannot be altered by unauthorized person. The voter authentication in online e-voting process can be done by formal registration through administrators and by

DOI: 10.18535/ijecs/v5i3.31

entering OTP Certificate. In Offline e-voting process authentication can be done using facial recognization, fingerprint sensing and RFID(smart cards) which enables the electronic ballot reset for allowing voters to cast their votes. Also the voted data and voters details can be sent to the nearby Database Administration unit in a timely manner using GSM System with cryptography technique. The criteria are Registration through Administrator, Voter identification and verification process is done through GSM with one time password. The second Offline e-voting process includes Facial Reorganization; Fingerprint sensing, RFID and Polling data processing using Cryptography Technique with RC4 Algorithm. The final process concludes the analysis of polling data in real time and immediate resulting system of e-voting system. There are two types of problems with EVM which is currently in use:

1. Security Problems-One can change the program installed in the EVM and tamper the results after the polling. By replacing a small part of the machine with a look-alike component that can be silently instructed to steal a percentage of the votes in favor of a chosen candidate. These instructions can be sent wirelessly from a mobile phone.

2. Illegal Voting (Rigging)-The very commonly known problem, Rigging which is faced in every electoral procedure. One candidate casts the votes of all the members or few amount of members in the electoral list illegally. This results in the loss of votes for the other candidates participating and also increases the number votes to the candidate who performs this action. This can be done externally at the time of voting.

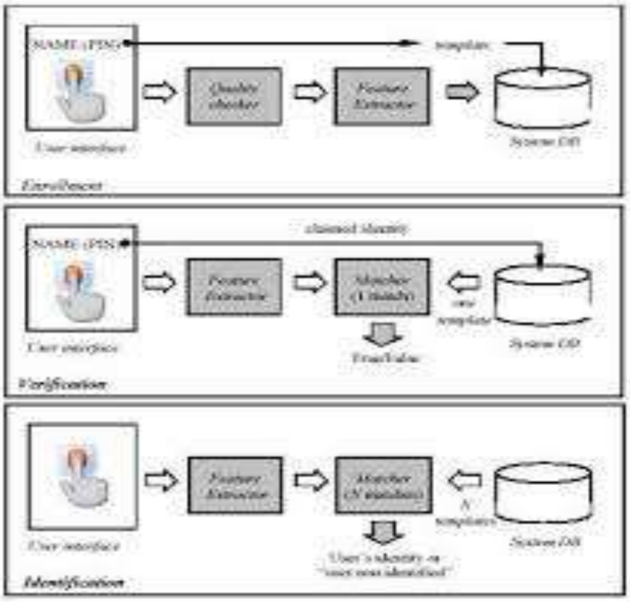
3. REMEDIES:

The above mentioned security problems can be solved by other means such as taking more care in keeping the EVMs safe and secure until the time of declaring the results, which can be done manually. By placing Jammers at the Ballot vault to avoid the tampering using wireless communication (Cell Phones). Results should be declared immediately after polling. The problem of rigging can be eradicated by giving a unique to every user so that one person can cast his vote only once. That unique id can be ―Fingerprint of each individual.

4. BIOEMTRIC SYSTEM (FINGERPRINT RECOGNITION):

A biometric system is essentially a pattern recognition system that operates by acquiring biometric data from an individual, extracting a feature set from the acquired data, and comparing this feature set against the template set in the database. Depending on the application context, a biometric system may operate either in verification mode or identification mode. In addition, different from the manual approach for fingerprint recognition by experts, the fingerprint recognition here is referred as AFRS (Automatic Fingerprint Recognition System), which is program-based. In such a system, an individual who desires to be recognized claims an identity, usually via a personal identification number (PIN), a user name, or a smart card, and the system conducts a one-to-one comparison to determine whether the claim is true or not (e.g., ―Does this biometric data belong to Bob?‖). Identity verification is typically used for positive recognition, where the aim is to prevent multiple people from using the same identity. In the identification mode, the system recognizes an individual by searching the templates of all the users in the database for a match. Therefore, the system conducts a one-to-many comparison to establish an individual‘s identity (or fails if the subject is not enrolled in the system data-base) without the subject having to claim an identity (e.g., ―Whose biometric data is this?‖). Identification is a critical component in negative recognition applications where the system establishes whether the person is who she (implicitly or explicitly) denies to be. The purpose of negative recognition is to prevent a single person from using multiple identities. Identification may also be used in positive recognition for convenience (the user is not required to claim an identity). While traditional methods of personal recognition such as passwords, PINs, keys, and tokens may work for positive recognition, negative recognition can only be established through biometrics. Throughout this paper, we will use the generic term recognition where we do not wish to make a distinction between verification and identification. The block diagrams of a verification system and an identification system are depicted in Fig. 1; user enrollment, which is common to both of the tasks, is also graphically illustrated.

Fig: 2



A biometric system is designed using the following four main modules. 1) Sensor module, which captures the biometric data of an individual. An example is a fingerprint sensor that images the ridge and valley structure of a user‘s finger. 2) Feature extraction module, in which the acquired biometric data is processed to extract a set of salient or discriminatory features. For example, the position and orientation of minutiae points (local ridge and valley singularities) in a fingerprint image are extracted in the feature extraction module of a fingerprint-based biometric system. 3) Matcher module, in which the features extracted during recognition are compared against the stored templates to generate matching scores. For example, in the matching module of a fingerprint-based biometric system, the number of matching minutiae between the input and the template fingerprint images is determined and a matching score is reported. The matcher module also encapsulates a decision making module, in which a user‘s claimed identity is confirmed (verification) or a user‘s identity is established (identification) based on the matching score. 4) System database module, which is used by the biometric system to store the biometric templates of the enrolled users. The enrollment module is responsible for enrolling individuals into the biometric system database. During the enrollment pause, the biometric characteristic of an individual is first scanned by a biometric reader to pro-duce a digital representation of the characteristic. The data capture during the enrollment process may or may not be supervised by a human depending on the application. A quality check is generally performed to ensure that the acquired sample can be reliably processed by successive stages. In order to facilitate matching, the input digital representation is further processed by a feature ex-tractor to generate a compact but expressive representation, called a template. Depending on the application, the template may be stored in the central database. Of the bio-metric system or be recorded on a smart card issued to the individual. Usually, multiple templates of an individual are stored to account for variations observed in the biometric trait and the templates in the database may be up-dated over time. A biometric verification system makes two types of errors: 1) mistaking biometric measurements from two different per-sons to be from the same person (called false match) and 2) mistaking two biometric measurements from the same person to be from two different persons (called false non-match). These two types of errors are often termed as false accept and false reject, respectively.

1) PIC Microcontroller-The PIC (founded by Microchip) 16F877A is an CMO-FLASH based high-performance 8-bit RISC Microcontroller. This powerful (200 nanosecond instruction execution) yet easy-to-program (only 35 single word instructions) microcontroller packs Microchip's powerful PIC® architecture into an 40 pin packag. The PIC16F877A features 256 bytes of EEPROM data memory, self programming, an ICD, 2 Comparators, 8 channels of 10-bit Analog-to-Digital (A/D) converter, 2 capture/compare/PWM functions, the synchronous serial port can be configured as either 3-wire Serial Peripheral Interface (SPI™) or the wire Inter-Integrated Circuit (I²C™) bus and a Universal Asynchronous Receiver Transmitter (USART). All of these features make it ideal for more advanced level A/D applications in automotive, industrial, appliances.

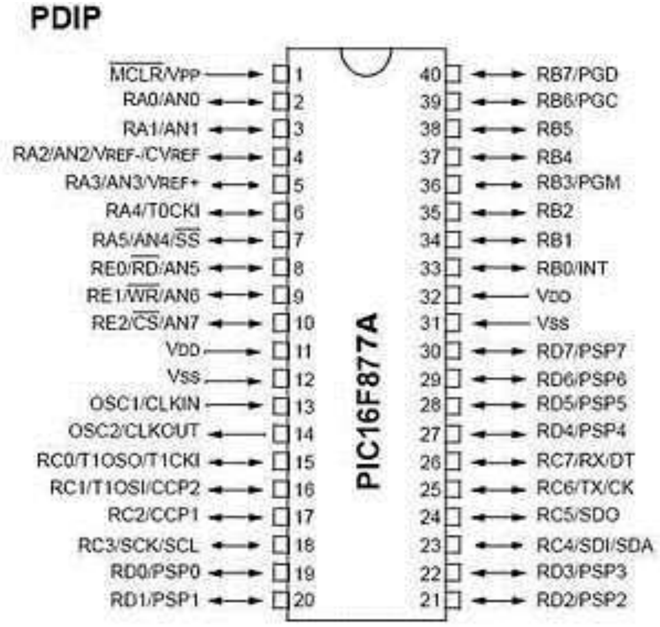


Fig:3

2) Fingerprint Identification Module-Fingerprint processing includes two parts: fingerprint enrollment and fingerprint matching (the matching can be 1:1 or 1:N).When enrolling, user needs to enter the finger two times. The system will process the two time finger images, generate template of the finger based on processing results and store the template. When matching, user enters the finger through optical sensor and system will generate a template of the finger and compare it with templates of the finger library. For 1:1 matching, system will compare the live finger 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.

Fig:4

DESCRIPTION

- Power DC 4.5V-6.0V
- Interface UART(TTL logical level)/ USB 1.1
- Working current Typical: 100mA Peak:150mA
- Matching Mode 1:1 and 1:N
- Image acquiring time <0.5s
- Template size 512 bytes
- FAR <0.001%
- FRR <0.1%
- Average searching time < 0.8s (1:880)
- Window dimension 18mm*22mm

3) LCD -A liquid crystal display (LCD) is a flat panel display, electronic visual display, or video display that uses the light modulating properties of liquid crystals (LCs). LCs do not emit light directly. They are used in a wide range of applications, including computer monitors, television, instrument panels, aircraft cockpit displays, signage, etc. They are common in consumer devices such as video players, gaming devices, clocks, watches, calculators, and telephones. LCDs have replaced cathode ray tube (CRT) displays in most applications. They are available in a wider range of screen sizes than CRT and plasma displays, and since they do not use phosphors, they cannot suffer image burn-in. LCDs are, however, susceptible\ to image persistence. LCDs are more energy efficient and offer safer disposal than CRTs

DOI: 10.18535/ijecs/v5i3.31

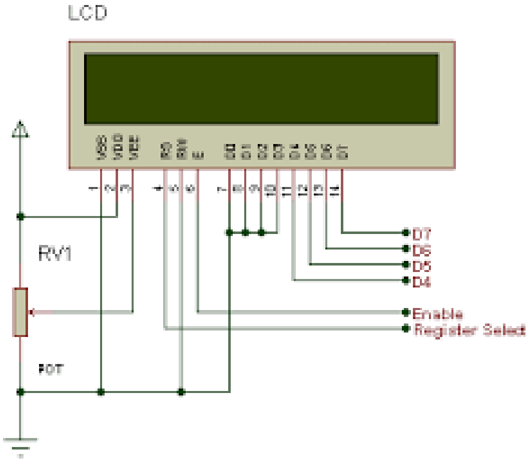


Fig:4

The most flexible ones use an array of small pixels. The earliest discovery leading to the development of LCD technology, the discovery of liquid crystals, dates from 1888. By 2008, worldwide sales of televisions with LCD screens had surpassed the sale of CRT units. LCDs available in two models: Character LCD and Graphics LCD. The character LCD displays ASCII values and graphics LCD displays graphics. Character LCDs are available in various kinds of models.

5. POWER SUPPLY:

-Power supply unit consists of the following units:
1. Step down transformer.
2. Rectifier unit.
3. Input filter.
4. Regulator unit.
5. Output filter.

5.1 STEP DOWN TRANSFORMER:

It is used to step down the main supply voltage by using step down transformer. It consists of primary and secondary coils. The o/p from the secondary coil is also AC wave form. So we have to convert the easy wave form into dc voltage by using rectifier unit.

5.2 RECTIFIER UNIT:

We have to convert AC voltage to DC using rectifier. Bridge rectifier is used. This o/p voltage often rectifier is in rippled form, so we have to remove ripples from DC voltage.

5.3 INPUT FILTER:

Capacitor acts as filter. The principle of the capacitor is charging and discharging. It charges in the positive half cycle of the AC voltage and it will discharge in the negative half cycle. So this allows only AC voltage and does not allow the DC voltage. This filter is fixed before the regulator.

5.4 REGULATOR UNIT:

Regulator regulates the o/p voltage constant depends on upon the regulator. It is classified as follows.
1. Positive regulator
a. Input pin
b .Ground pin
c. Output pin
It regulates the positive voltage
2. Negative regulator
a. Ground pin
b. input pin
c. output pin
It regulate the negative voltage

5.5 OUTPUT FILTER:

Capacitor acts as filter. The principle of the capacitor is charging and discharging. It charges in positive half cycle of the AC voltage an it will discharge in negative half cycle. So it allow only allows AC voltage and does not allow the DC voltage. This filterer fixed after the regulator. The IR Sensor Set,SN-IRS-01consists of transmitter and an IR receiver mounted side by side on a tiny PCB. With minimum interface and 5VDC power, it can be used as a reflective type IR sensor for mobile robot or low cost object detection sensor.IR Transmitter will always transmit IR light (Infrared), it is not visible to human eyes. Since the transmitter and receiver is being arrange side by side, theoretically, the receiver should not receive any or in most cases, it will receive small amount of infrared emitted by the IR transmitter. The working concept of IR receiver is similar to transistor or LDR (Light Dependent Resistor). Referring to above diagram, the IR Receiver is like a transistor with the‗base' controlled by the IR light received. When there is no IR light receive, the‗collector' of transistor does not allow current to sink to‗emitter' further to ground of circuit. It is like very high resistance from‗collector' to‗emitter', blocking current going to ground. In this case, the voltage at Output node will be high, near to 5V.When the IR receiver receives more IR light, it changes the resistance at‗collector' and allow more current to sink to ground, and this is similar to low resistance at the lower part of the circuit. So, the voltage at Output will drop. We utilize this voltage changes to IR light to ―know‖ whether there is obstacle or not. Because when there is obstacle, IR light get reflected to IR receiver further changes the voltage, monitoring the voltage changes will get you an obstacle detection sensor. With the help of this we can easily detect any kind of tampering with the machine and will program the machine to stop the process till it is rechecked and then reset the machine.

ADVANTAGES

1. The system is highly reliable, tamper-proof and secure.
2. In the long run the maintenance cost is very less when compared to the present systems.
3. Illegal practices like rigging in elections can be checked for.
4. It is possible to get instantaneous results and with high accuracy.
5. This unique fingerprint voter ID card can be used for Identification purpose in Govt. /Semi-Govt. bodies E.g.: When applying Passport, Driving license, etc.
.

FUTURESCOPE:

1. This system can be implemented in a few years, with recent development in technology, a fingerprint scanner is neither too expensive nor too complicated to use on daily basis.
2. Memory of finger print module can be expanded .We can use a 1mb flash memory finger print module for increasing the capacity.
3. External memory can be provided for storing the finger print image, which can be later accessed for comparison.
4 .Audio output can be introduced to make it user friendly for

illiterate voters. Unique Identification Numbers (Aadhar cards) have already been introduced in India that contains an individual‗s fingerprints and iris scan. Soon every Indian citizen can have a similar identity card and all the government will have all the necessary information required to bring such a system in play.

CONCLUSION:

For over a century, fingerprints have been one of the most highly used methods for human recognition; automated biometric systems have only been available in recent years. This work is successfully implemented and evaluated. The arrived results were significant and more comparable. It proves the fact that the fingerprint image enhancement step will certainly improve the verification performance of the fingerprint based recognition system. Because fingerprints have a generally broad acceptance with the general public, law enforcement and the forensic science community, they will continue to be used with many governments‗ legacy systems and will be utilized in new systems for evolving applications that require a reliable biometric. Thus the advent of this biometric voting system would enable hosting of fair elections in India. This will preclude the illegal practices like rigging. The citizens can be sure that they alone can choose their leaders, thus exercising their right in the democracy.

REFERENCE:

[1] Schurmann, C.; IT Univ. of Copenhagen, Copenhagen, Denmark. ―Electronic Elections: Trust Through Engineering‖, First international workshop Requirements Engineering for e-Voting Systems (RE-VOTE), 2009.

[2] A. Villafiorita and K. Weldemariam, and R. Tiella, "Development, Formal Verification, and Evaluation of an E-Voting System with VVPAT," IEEE Transactions on Information Forensics and Security, vol. 4, no. 4, 2009

[3].Jossy P. George Saleem S Tevaramani And K B Raja Performance Comparison Of Face Recognition Using Transform Domain Techniques World Of Computer Science And Information Technology Journal (WCSIT) ISSN: 2221-0741 Vol. 2, No. 3, 82-89, 2012

[4] Molnar, D. ; California Univ., Berkeley, CA ; Kohno, T. ; Sastry, N. ; Wagner, D.,Tamper-evident, history-independent, subliminal free data structures on PROM storage -or- how to store ballots on a voting machine, Security and Privacy, 2006 IEEE Symposium, 21-24 May 2006.