Modernized Voting Machine using Finger Print Recognition

Jeya Priyanka.D[#1], Prathibha.M[#2], Shanmuga Priya.R[#3]

[# 1, 2, 3] *EEE Department, UG Students*

Kalasalingam Institute of Technology
Anand Nagar, Krishnankoil-626126.

[1]djeyapriyanka@gmail.com

[2]m.prathibha90@gmail.com

[3]priya.rjune3@gmail.com

ABSTRACT— Nowadays, providing preventive measures is one of the challenging matters in the world. Among the several field, providing preventive measures system for voting are the tedious and expensive one. In order to provide inexpensive solutions to the above, this project will be implemented with 3 security measures namely, finger print scan, magnetic coated stripe scan, and password scan. These scans are used to ensure the security to avoid fake, repeated voting etc. Then these polled votes are stored in local database in each poll booth and then they are connected to the main database by encrypted form in order to avoid any malicious threats. Thus the first aim of avoiding fake and repeated voting has been avoided then to reduce the time of finding the Winning party with majority of votes we make use of this main database, thus the result of polled votes are checked and the winning party can be announced within few hours after the polling.

I. INTRODUCTION

Electronic Voting Machines ("EVM") are being used in Indian General and State Elections to implement electronic voting in part from 1999 elections and in total since 2002 elections. The EVMs reduce the time in both casting a vote and declaring the results compared to the old paper ballot system. The EVMs were devised and designed by Election Commission of India in collaboration with two Public Sector undertakings viz., Bharat Electronics Limited, Bangalore and Electronics Corporation of India Limited, Hyderabad. The EVMs are now manufactured by the above two undertakings. EVMs were first used in 1982 in the by-election to Parur Assembly Constituency of Kerala for a limited number of polling stations (50 polling stations).

II. EXISTING SYSTEMS

1. ANALYSIS OF AN ELECTRONIC VOTING SYSTEM

With significant U.S. federal funds now available to replace outdated punch-card and mechanical voting systems, municipalities and states throughout the U.S. are adopting paperless electronic voting systems from a number of different vendors. a security analysis of the source code to one such machine used in a significant share of the market. The analysis shows that this voting system is far below even the most minimal security standards applicable in other contexts. Several problems including unauthorized privilege escalation, incorrect use of cryptography, vulnerabilities to network threats, and poor software development processes. The voters, without any insider privileges, can cast unlimited votes without being detected by any mechanisms within the voting terminal software. In the face of such attacks, the usual worries about insider threats are not the only concerns; outsiders can do the damage. The insider threat is also quite considerable, showing that not only can an insider, such as a poll worker, modify the votes, but that insiders can also violate voter privacy and match votes with the voters who cast them. This voting system is unsuitable for use in a general election. Any paperless electronic voting system might suffer similar flaws, despite any "certification" it could have otherwise received. The best solutions are voting systems having a "voter-verifiable audit trail," where a computerized voting system might print a paper ballot that can be read and verified by the voter.

2. HOW TO TRUST DRE VOTING MACHINES PRESERVING VOTER PRIVACY

While many experts believe that the e-voting system offers prominent advantages over plain paper voting system, others express concerns about the potential for large-scale fraud. Many current e-voting systems are not based on the cryptographic technologies and require voters to trust them. Voters cannot be assured that the votes cast accurately reflect their intent because the mechanism for recording votes is hidden in the code for the machine. In this paper, the author proposed a practical voter-verifiable e-voting scheme using a paper receipt based on cryptographic technologies.

3. THE DESIGN OF A TRUSTWORTHY VOTING SYSTEM

After the voting debacle in the Florida Presidential election of 2000 with its now-fabled hanging chads and pregnant chads, many voting jurisdictions turned to electronic voting machines. This transition has had at least as many problems as punch-card systems and added the additional one of making recounts impossible. As a result, many jurisdictions have gone back to paper ballots in despair. The electronic voting can have many benefits including accessibility and usability but requires regarding voting as a system of which the voting machine is only a (small) part. This paper describes all the components of an electronic voting system that is

practical and difficult to tamper with. It emphasizes the importance of systems aspects, defense in depth, and being paranoiac.

4. MANAGING REQUIREMENTS FOR E-VOTING SYSTEMS: ISSUES AND APPROACHES

This paper discusses on structuring and maintaining requirements for an e-voting system built and deployed for elections. Issues related to integrating laws and recommendation for e-voting systems, managing different elections and configurations, supporting a spiral development, yielded problems and approaches to help maintain integrity of requirements and a coherent view of the system. Moreover, the relationship between requirements and system architecture is based on finite state machines that bridge the gap between the laws and the actual behavior of the machine.

5. AN OPEN-SECRET VOTING SYSTEM

Electronic voting machines allow software configuration of the ballots, adapt to a voter's first language, and offer a touch-screen interface's ease of use. These machines also make it easy to change a selection before pressing a final accept button. But as a means for counting votes, computer-based devices raise suspicions as to what exactly is going on inside the black box. It's not hard to imagine all kinds of software irregularities, intended or otherwise, that might cause machine tallies to be skewed. Thus, mistrust of such machines runs rampant. The Internet's strengths include easy access and broad public acceptance, but like the touch-screen voting machine, Internet software raises questions about security and integrity

6. ENSURING VOTERS AND CANDIDATES' CONFIDENTIALITY IN E-VOTING SYSTEMS

A new method based on cryptography to ensure voters and candidates' confidentiality in the Internet E-Voting, referred to as the Name and vOte separaTed E-voting (NOTE) system, is proposed. In NOTE, an impartial party, the Election Commission (EC) will be responsible for part of the vote counting duties besides collecting and verifying the voter ID. The votes and the candidates' names are separated into two parts during the counting process. EC will hold the candidates' names secret before the tally comes up; the Vote Counting Committee (VCC) only counts the votes and is not involved in unveiling the vote tally by virtue of the anonymity of the candidates. Only EC can disclose the final tally after VCC has counted all votes without knowing who the votes are for during the vote counting procedure. This scheme will effectively ensure voters and candidates' confidentiality, and thus improving election security and fairness.

III. ELECTRONIC VOTING MACHINE

Electronic Voting Machine (EVM) retains all the characteristics of voting by ballot papers, while making polling a lot more expedient. Being fast and absolutely reliable, the EVM saves considerable time, money and manpower. And, of course, helps maintain total voting secrecy without the use of ballot papers. The EVM is 100 per cent tamper proof. And, at the end of the polling, just press a button and there you have the results. The EVM consists of two units that can be inter-linked. One, a ballot unit which a voter uses to exercise his vote. And the other, a control unit – used by the polling officials.

THE BALLOT UNIT : AN ELECTRONIC BALLOT BOX.

A simple voting device, it displays the list of candidates. A facility to incorporate party names and symbols is in-built. All the voter has to do is press the desired switch located next to the name of each candidate. The main advantage is the speed, apart from the simplicity of operation, which requires no training at all. A single ballot unit takes in the names of 16 candidates. And thus, by connecting four ballot units the EVM can accommodate a total of 64 candidates in a single election.

THE CONTROL UNIT : IN TOTAL CONTROL OF THE POLLING

Conduction of polling, display of total votes polled, sealing at the end of the poll, and finally, declaration of results – these are the various accomplishments of just one gadget : the control unit. In total control of the polling, this electronic unit gives you all necessary information at a press of a few buttons. For instance, if you need to know the total number of votes, you just have to press the Total switch. Candidates-wise results can be had only at the end of polling.

IV. ARCHITECTURE OF THE PROPOSED SYSTEM

The major parts of the voting system is listed below,

1. Arm Processor
2. Finger Print Sensor
3. RFID tag reader
4. Peripheral Interfacing
   - LCD
   - LED
   - MAX 232
   - RS232

1) ARM PROCESSOR

The NXP (founded by Philips) LPC2148 is an ARM7TDMI-S based high-performance 32-bit RISC Microcontroller with Thumb extensions 512KB on-chip Flash ROM with In-System Programming (ISP) and In-Application Programming (IAP), 32KB RAM, Vectored Interrupt Controller, Two 10bit ADCs with 14 channels, USB 2.0 Full Speed Device Controller, Two UARTs, one with full modem interface. Two I2C serial interfaces, Two SPI serial interfaces Two 32-bit timers, Watchdog Timer, PWM unit, Real Time Clock with optional battery backup, Brown out detect circuit General purpose I/O pins. CPU clock up to 60 MHz, On-chip crystal oscillator and On-chip PLL.

2) FINGER PRINT SENSOR

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 image generate a 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.

DESCRIPTION

- **Power** DC 3.6V-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) RFID TAG READER

RFID stands for Radio Frequency Identification. RFID is one member in the family of Automatic Identification and Data Capture (AIDC) technologies and is a fast and reliable means of identifying objects. There are two main components: The Interrogator (RFID Reader) which transmits and receives the signal and the Transponder (tag) that is attached to the object. An RFID tag is composed of a miniscule microchip and antenna. RFID tags can be passive or active and come in a wide variety of sizes, shapes, and forms. Communication between the RFID Reader and tags occurs wirelessly and generally does not require a line of sight between the devices. An RFID Reader can read through most anything with the exception of conductive materials like water and metal, but with modifications and positioning, even these can be overcome. The RFID Reader emits a low-power radio wave field which is used to power up the tag so as to pass on any information that is contained on the chip. In addition, readers can be fitted with an additional interface that converts the radio waves returned from the tag into a form that can then be passed on to another system, like a computer or any programmable logic controller. Passive tags are generally smaller, lighter and less expensive than those that are active and can be applied to objects in harsh environments, are maintenance free and will last for years. These transponders are only activated when within the response range of an RFID Reader. Active tags differ in that they incorporate their own power source, where as the tag is a transmitter rather than a reflector of radio frequency signals which enables a broader range of functionality like programmable and read/write capabilities.

RFID FREQUENCIES

Radio waves are the carriers of data between the reader and tags. The approach generally adopted for RFID communication is to allocate frequencies depending on application. The frequencies used cover a wide spectrum.

These specified bands are

Very long wave 9 - 135 kHz
Short wave 13.56 MHz
UHF 400-1200 MHz
Microwave 2.45 and 5.8 GHz

NSK EDK 125 KHZ RFID

This is a Passive RFID (Sensitivity Range is about 6cm from antenna)

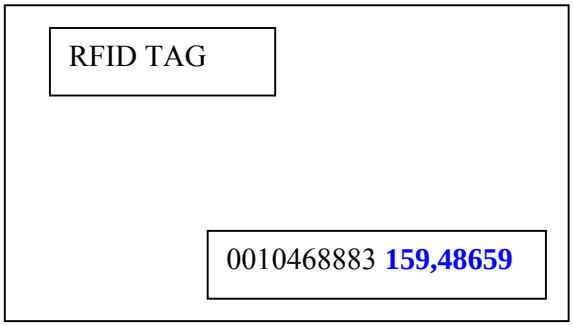
Hardware:

This RFID Reader is having 3 stages

- RFID Reader Chip
- Pic Microcontroller to decode the data into Serial o/p and wigend O/p
- Rs232 to Convert signal into TTL to RS232

DATA TRANSMISSION IN ASCII STANDARD

Data read from the tag is Manchester encoded. The Manchester encoded data is decoded to ASCII standard. Decoded data is sent to the UART serial interface for wired communication with the host systems. ASCII data format is shown below:



For Example If The card Shown Above is Placed on the Reader ,

UART Data Will be 159 48659

Parity |---8BIT--|-------16BIT----------|Parity

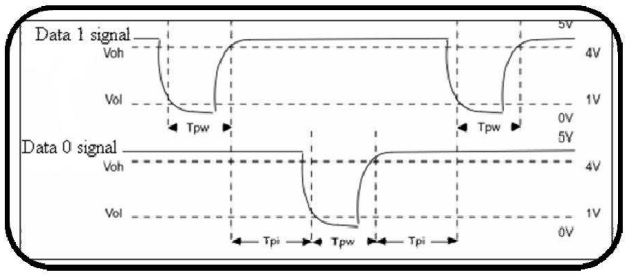
Wigend O/p Will be

1 1001 1111 1011 1110 0001 0011 0

DATA TRANSMISSION IN WIEGAND26 STANDARD

The reader module supports the Wiegand standard that gives the Wiegand encoded output. This output comprises 3 bytes of data. It will be indicated as low pulse on data line if it is a Data 1 signal and low pulse on the zero line if it is a Data 0 signal. The pattern of data bits sent by the reader is shown.

This timing pattern falls within the Wiegand guidelines as prescribed by the SIA's Access Control Standard Protocol for the 26-bit Wiegand Reader Interface (a Pulse Width time between 20 μS and 100 μS, and a Pulse Interval time between 200 μS and 20 mS). The Data 1 and Data 0 signals are held at logic high level (above the Voh level) until the reader is ready to send a data stream. The reader places the data as asynchronous low-going (negative) pulses (below the Vol level) on the Data 1 or Data 0 lines to transmit the data stream to the access control panel (the "saw-teeth" in Figure 2).The Data 1 and Data 0 pulses do not overlap or occur simultaneously. The composition of the open existing industry standard 26- bit Wiegand format contains 8 bits for the facility code field and 16 bits for the ID number field. Mathematically these 8 facility code bits allow a total of 256 (0 to 255) facility codes, while the 16 ID number bits allow a total of only 65,536 (0 to 65,535) individual ID's within each facility code.



…….NSK RFID EDK 125KHZ ……

4) PERIPHERAL INTERFACING

This section explains interfacing peripherals with processor, which is necessary for making any application. The following section explains the various peripherals like LED, LCD, Keyboard interfacing with any embedded controller.

LED

A light-emitting diode (LED) is a semiconductor light source. LEDs are used as indicator lamps in many devices and are increasingly used for other lighting. Introduced as a practical electronic component in 1962, early LEDs emitted low-intensity red light, but modern versions are available across the visible, ultraviolet, and infrared wavelengths, with very high brightness.

When a light-emitting diode is forward-biased (switched on), electrons are able to recombine with electron holes within the device, releasing energy in the form of photons. This effect is called electroluminescence and the color of the light (corresponding to the energy of the photon) is determined by the energy gap of the semiconductor. LEDs are often small in area (less than 1 mm^2), and integrated optical components may be used to shape its radiation pattern. LEDs present many advantages over incandescent light sources including lower energy consumption, longer lifetime, improved robustness, smaller size, and faster switching. LEDs powerful enough for room lighting are relatively expensive and require more precise current and heat management than compact fluorescent lamp sources of comparable output.

Light-emitting diodes are used in applications as diverse as aviation lighting, automotive lighting, advertising, general lighting, and traffic signals. LEDs have allowed new text, video displays, and sensors to be developed, while their high switching rates are also useful in advanced communications technology. Infrared LEDs are also used in the remote control units of many commercial products including televisions, DVD players, and other domestic appliances.

Therefore, when interfacing an LED to a TTLoutput, the maximum current through the LED is16 mA. The features of LEDs are listed below

· Lower power consumption
· Require series resistors to limit the current
· Displaying decimal digits

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. Its low electrical power consumption enables it to be used in battery-powered electronic equipment. It is an electronically modulated optical device made up of any number of segments filled with liquid crystals and arrayed in front of a light source (backlight) or reflector to produce images in color or monochrome. 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.

No. Of characters × Lines: 8×1, 16×1, 16×2, 16×4, 20×4, 40×4,…

Dots × Dots: 122×32, 128×64, 240×128, 320×240,….

Color: Yellow, Green, Gray, Blue….

Graphics LCDs are also available with different sizes and colors.

UART

A Universal Asynchronous Receiver/Transmitter, abbreviated UART is a type of "asynchronous receiver/transmitter", a piece of computer hardware that translates data between parallel and serial forms. UARTs are commonly used in conjunction with communication standards such as EIA RS-232, RS-422 or RS-485.

A UART is usually an individual (or part of an) integrated circuit used for serial communications over a computer or peripheral device serial port. UARTs are now commonly included in microcontrollers.

(UART) takes bytes of data and transmits the individual bits in a sequential fashion. At the destination, a second UART re-assembles the bits into complete bytes. Each UART contains a shift register which is the fundamental method of conversion between serial and parallel forms.

MAX232

The MAX220–MAX249 family of line drivers/receivers is intended for all EIA/TIA-232E and V.28/V.24 communications interfaces, particularly applications where ±12V is not available. These parts are especially useful in battery-powered systems, since their low-power shutdown mode reduces power dissipation to less than 5µW. While connecting the hardware serially with the PC using RS232, it is necessary to use a driver to make the data accessible to both the modules since, their operating powers are different. Here we are using MAX232 as the driver.

The MAX232 contain four sections:

- Dual charge-pump DC-DC voltage converters
- RS-232 drivers
- RS-232 receivers
- Receiver and transmitter enable control inputs

ABSOLUTE MAXIMUM RATINGS

Supply voltage (V_{CC}) -	-0.3V to +6V
Input voltages:	
T_{IN} -	-0.3V TO (V_{CC}-0.3V)
R_{IN} -	±30V
Output voltages:	
T_{OUT} -	±15V
R_{OUT} -	-0.3V TO (V_{CC}+0.3V)
Storage temperature -	-65ºC to +160ºC
Lead temperature (soldering) -	+300ºC

RS-232

In telecommunications, RS-232 (Recommended Standard 232) is a standard for serial binary data signals connecting between a DTE (Data Terminal Equipment) and a DCE (Data Circuit-terminating Equipment). It is commonly used in computer serial ports. A similar ITU-T standard is V.24.

SCOPE OF THE STANDARD

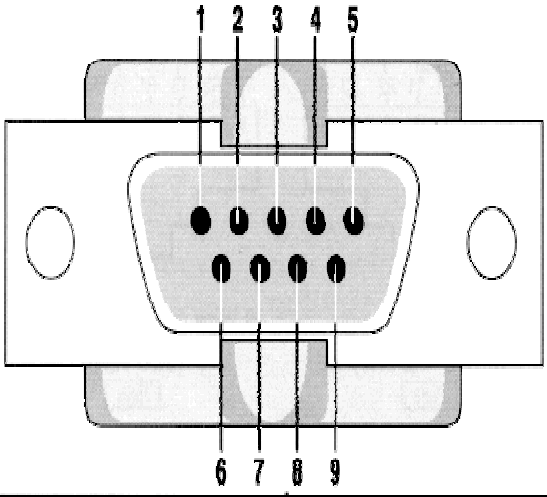
The Electronics Industries Association (EIA) standard RS-232-C as of 1969 defines:

Electrical signal characteristics such as voltage levels, signaling rate, timing and slew-rate of signals, voltage withstand level; short-circuit behavior, and maximum load capacitance.

Interface mechanical characteristics, pluggable connectors and pin identification.

Functions of each circuit in the interface connector. Standard subsets of interface circuits for selected telecom applications.

PIN DIAGRAM



Pin	Signal	Pin	Signal
1	Data Carrier Detect	6	Data Set Ready
2	Received Data	7	Request to Send
3	Transmitted Data	8	Clear to Send
4	Data Terminal Ready	9	Ring Indicator
5	Signal Ground		

Figure.1 RS232 PIN DIAGRAM

V. WORKING OF THE PROPOSED SYSTEM

At the time of polling, the voter has to place the smart card on the RFID reader. Later it verifies whether he/she is handicapped or not. After conforming, the normal person should produce his/her finger print at the scanner. Then it is verified in the database and his/her details will be displayed. Now they can enter their corresponding vote. For exceptional cases, he/she should enter the password for password scanning and later it is verified and can enter their corresponding vote. Else if he/she is an invalid person, the machine becomes disabled and hence he can't vote. After voting a party all the polling buttons get disabled so that no repeated polling will be done. The party to whom the voter polled will be immediately updated in the database. Then the system will automatically reset and hence the next person can poll. As soon as a person polls, his/her id will be disabled and hence he/she can't poll again hence avoiding malpractices.

This below figure shows the overall basic block diagram of our proposed system.

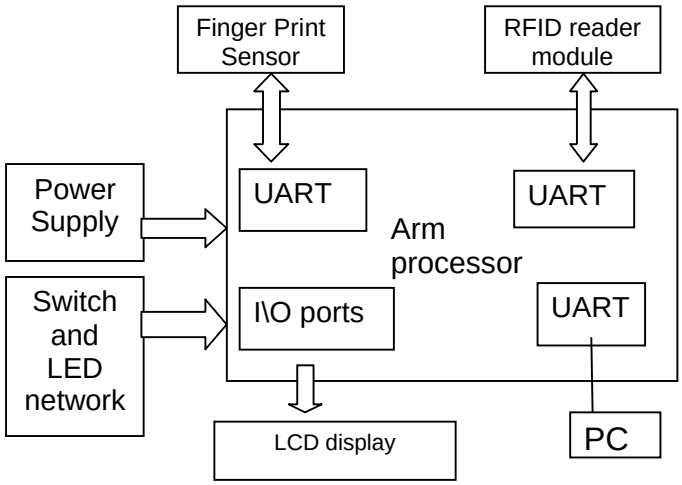


Figure 2. BLOCK DIAGRAM

VI. BEFORE POLLING

The following is the flow chart for the process before polling. First, we should obtain each and every persons details like name, residential address, age, sex, date of birth and their photo. Verify the person is handicapped. If so give authenticated password to the corresponding persons. If not, then collect their finger prints and save it in the according databases. Store all these details in an encrypted format and provide it in the smart card to the voters.

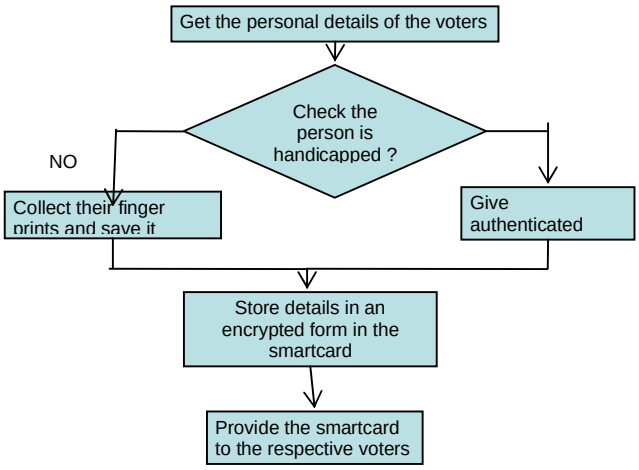


Figure 3. Before polling

VII. DURING POLLING

Initially, the voter places his/her smart card which is provided at the time of polling. After verifying whether he/she is handicapped or not. After conforming, the normal person should produce his/her finger print at the scanner. Then it is verified in the database and his/her details will be displayed. Now they can enter their corresponding vote. For exceptional cases, he/she should enter the password for password scanning and later it is verified and can enter their corresponding vote. Else if he/she is an invalid person, the machine becomes disabled and hence he can't vote. After voting a party all the polling buttons get disabled so that no repeated polling will be done. The party to whom the voter polled will be immediately updated in the database. Then the system will automatically reset and hence the next person can poll.

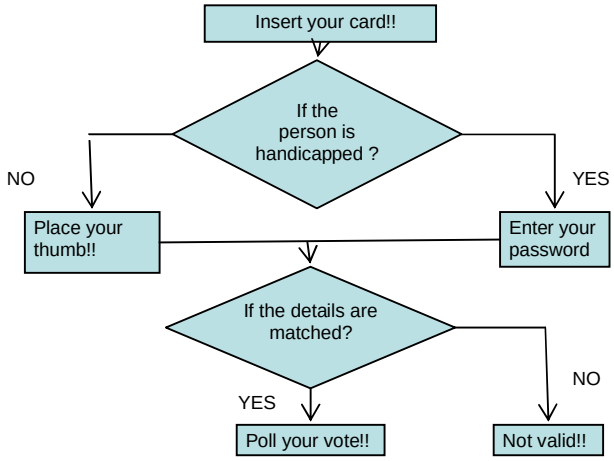


Figure4. After polling

VIII. ADVANTAGES

- **Independent & Reliable**
  The EVM is compact and comes in its reusable carry pack. Further, the EVM works/operates on a battery power source. Making it independent and totally reliable.
- **Hi-tech Simplicity**
  To commence polling, the polling officer activates the "Ballot" switch on the control unit. The voter then has to press the button of his choice on the ballot unit. This is followed by a short beep sound, indicating that the vote has been cast. Once again, the polling officer has to press the "Ballot" switch to clear the machine for the next voter to cast his vote.

- **Super-sensitive circuitry : No invalid votes**
  Inside the control unit, hidden from you, is an extremely sensitive circuitry that takes care of common election errors or malpractices like vote duplication. For instance, if one were to press two or more buttons simultaneously, then no vote would be cast. Even if there was a micro-second difference in the pressing of the switches, the EVM is sensitive enough to trace and identify the twitch that was press first.
- **Instant results**
  Once polling is completed, the election results can be known instantly at the counting station by pressing the ‘‘Result'’ switch. This switch is located in a sealed compartment of the control unit.
- **Tamper proof design**
  The EVM is designed to be totally tamper proof. Each EVM comes with a sophisticated programme in assembly language: software fully seated against outside influence. And the programme is itself fused on to a customised micro processor chip at the manufacturer’s end. This ensures that the program is rendered tamper proof and inaccessible.
- **Result Printout**
  Normally, an EVM displays results on the display panel of the control unit. But a printout option is available with the use of a Download Adaptor Unit (DAU). The DAU has to be connected to the control unit and any standard printer. Further, with the help of a modem, the DAU can also enable transmission of voting information to a distant centralised computer.
- Increased Security
- Publication of results as soon as possible
- Reduces criminal activities
- Reduces Man power

IX. CONCLUSION

In olden days, polling is done more manually using ballot boxes and papers. As the world got modernized and automation came in to effect, it has been changed to Electronic Voting Machines. NXG EVM may be considered as its updation. Yet more improvements can be made as science advances.

REFERENCES

[1] Tadayoshikohno_ Adamstubblefield Avield Rubidans.Wallach “Analysis of an Electronic Voting system”, IEEE symposium on Security and Privacy 2004.

[2] Yunho Lee; Seungjoo Kim; Dongho Won; Sch. of Inf. & Commun. Eng., Sungkyunkwan Univ.,Suwon. “How to Trust DRE Voting Machines Preserving Voter Privacy” IEEE International Conference ICEBE’08,e-Business Engineering, 2008.

[3] Paul, N.; Tanenbaum, A.S.; Vrije Univ., Amsterdam, Netherlands.” The Design of a Trustworthy Voting System ” , ACSAC’09 Computer Security Applications Conference, 2009.

[4] Weldemariam, K.; Mattioli, A.; Villafiorita, A.; Center For Inf. Technol., FBK-IRST, Trento, Italy “Managing Requirements for E-Voting Systems: Issues and Approaches”, First international workshop Requirements Engineering for e-Voting Systems (RE-VOTE), 2009

[5] 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.

[6] Haijun Pan; Hou, E.; Ansari, N.; Dept. of Electr. & Comput. Eng., New Jersey Inst. of Technol., Newark, NJ, USA “Ensuring voters and candidates' confidentiality in E-voting systems”, 34th IEEE Sarnoff Symposium, 2011.

[7] www.rfidjournal.com

[8] www.aimglobaltechnologies.org\lpc2148

[9] http://www.keil.com/dd/chip/3880.html