Tamper Proof Electronic Voting Machine Implementation on FPGA

Mr. Sharan Kumar Electronics Department T.K.I.E.T Warananagar

Ms. Rama C. Mane. Electronics Department T.K.I.E.T Warananagar

Ms.R. R. Naik. Electronics Department T.K.I.E.T Warananagar

1. ABSTRACT

In the past, people go to polling place and take the blank ballots, then punch a hole or append the seal. If the seal is not clear enough, or the vote is damaged by soiling, it may bring some debate on the result. In order to resolve these situations, the technology of electronic voting machine came into existence. In the existing machine there is a possibility of tampering due to memory is present externally. Rigging also possible because of the control of successive votes is with polling officer. In order to resolve these situations, in this paper it is proposed to enhance the existing technology with the use of GSM and SMARTCARD. Proposed system can cast and count votes with higher convenience and efficiency, even make the electoral procedures simple and reduce the mistake rate of ballot examination.

The proposed EVM having the following features:

- GSM based voting - allows the citizens to vote using mobile phones from anywhere in the country.
- Smart card based voting using RFID - allows voters to use a smart card to verify their identity and authorizes them to cast vote. This feature has been included to exploit the advantages of the UID (Unique Identification) card or the "AADHAAR" scheme which the government proposes to introduce in a few years that will allow each citizen to be uniquely identified based on a single smart card.
- Tamper proof – in addition to the existing security features the proposed scheme provides password protection at various stages, auto-locking features, scalability and non-volatility of vote count.

The proposed EVM has been implemented on FPGA which is a rapid prototyping platform. The hardware-weightedness, reconfigurability and reusability of FPGA have made it a suitable choice for proposed design.

2 Voting Techniques

In India all earlier elections be it state elections or centre elections a voter used to cast his/her vote to his/her favorite candidate by putting the stamp against his/her name and then folding the ballot paper as per a prescribed method before putting it in the Ballot box. This is a long, time-consuming process and very much prone to errors.

This method wanted voters to be skilled voters to know how to put a stamp, and methodical folding of ballot paper. Millions of paper would be printed and heavy ballot boxes would be loaded and unloaded to and from ballot office to polling station. All this continued till election scene was completely changed by electronic voting machine. No more ballot paper, ballot boxes, stamping, etc. all this condensed into a simple box called ballot unit of the electronic voting machine.

The marking system of voting was introduced in 1962 to make it possible for a

substantial number of illiterate voters to indicate easily their preferences in choosing their representatives. Over the years, there was a pronounced increase in the volume of work: crores of ballot papers had to be printed and lakhs of ballot boxes had to be prepared, transported, and kept in storage; and a great amount of time was taken up by the conduct of elections. To overcome these difficulties, the Election Commission of India (ECI) thought of electronic gadgets. The Electronics Corporation of India Ltd. (ECIL), Hyderabad, and Bharat Electronics Ltd. (BEL), Bangalore, developed the electronic voting machine in 1981.

2.1 The Electronic Voting Machine

The complete EVM consists mainly of two units - (a) Control Unit and (b) Balloting Unit with cable for connecting it with Control unit. A Balloting Unit caters upto 16 candidates. Four Balloting Units linked together catering in all to 64 candidates can be used with one control unit. The control unit is kept with the Presiding Officer and the Balloting Unit is used by the voter for polling.

The Balloting Unit of EVM is a small Box-like device, on top of which each candidate and his/her election symbol is listed like a big ballot paper. Against each candidate's name, a red LED and a blue button is provided. The voter polls his vote by pressing the blue button against the name of his desired candidate.

How the Vote is cast with this EVM?

The entire process is very easy to understand:

- Like in earlier system, your name is called and you are asked to sign or put your thumb impression in a register.
- After your identification is done by Election Officer, an ink mark is put on your finger, same as earlier.
- Then the Election Officer gives you a slip that bears the Voter register number where you signed or put your thumb impression.
- You hand over this slip to the presiding officer who confirms the serial number and permits you to vote by pressing the button of the Control Unit of EVM.
- You are not given any ballot thereafter, and are sent to the EV Machine placed behind a card board in a corner. The machine is placed in such a way that your polled vote will be a secret.
- On the Balloting Unit of EVM, you press the blue button placed in front of your favorite candidate and release.
- As soon as the button is pressed, the red LED indicator lights up and a whistle sound comes from the machine. This signifies that your vote has been casted rightly. Now you can come out.
- In case of red LED not working, press the Blue button firmly again. If finding it difficult, consult the Presiding Officer.
- Your vote is complete safe and secret and there is no room for error as well. You can rest assured that your vote is not going to be invalid in any case.
- The Voting Machine is attached to the 'Control Unit'. When the user presses the button, his vote is registered in the control unit and the number of votes for the respective candidates is calculated automatically.

What Happens after Voting is over?

After the hour fixed for the close of the poll and the last voter has recorded his vote, the EVM is closed so that no further recording of votes in the machine is possible.

At the counting place, only the control unit is required for ascertaining the result of poll at the polling station at which the EVM was used. The balloting unit is not required. All this used to happen every time election were held.

2.2 Booth Capture

A remarkable advantage is that rigging is not possible with the EVMs. In the ballot paper system, the intruders can mark hundreds of ballots and put them into the ballot box in a matter of a few minutes. This is not possible in voting machines as the machine is designed to be capable of recording a maximum of five votes per minute. (The pace of polling can be set to any predetermined number before manufacturing). Thus, even for recording about 100 bogus votes it would take the booth captors 20 to 25 minutes, during which time the law and order officials may intervene to stop the rot. Moreover, as soon as the presiding officer apprehends any mischief, he can stop the poll by pressing the special switch after which no votes can be recorded.

The presiding officer of the polling station is empowered to close the control unit of the voting machine to ensure "that no further vote can be recorded". There is no possibility of any bogus votes being polled after the close of the poll and during the transit of the machines from the polling booth to the counting centre. A vote once recorded in an EVM cannot be tampered with, whereas in the ballot paper system the votes marked and put into the box can be pulled out and destroyed. The EVMs are capable of retaining the memory of the votes recorded for a period of three years. If the machine is tampered with in any respect either during the poll time or at any time before the counting of votes, which will be easily detectable so that a fresh poll can be ordered.

The EVMs have following advantages:

- The saving of considerable printing stationery and transport of large volumes of electoral material,
- Easy transportation, storage, and maintenance,
- No invalid votes,
- Reduction in polling time, resulting in fewer problems in electoral preparations, law and order, candidates' expenditure, etc. and
- Easy and accurate counting without any mischief at the counting centre
- Eco friendly.

As a matter of interest, “Diebold Accuvote System”, is a smarter system over conventional EVMs used in India.

It is a new system of voting adopted by US government is DIEBOLD. Diebold system works on Microsoft software; it has no seals on locks and panels to detect a tempering. It has a keyboard interface (!!!) and the server was tested to have “Blaster” virus. One report on Wired says a lady stumbled upon some files from Diebold, and found that the votes were stored in MS Access files. It also has a PCMCIA Scandisk card for local storage. A touch screen GUI and a network connection to send the results to a server after encrypting it with DES.

3. Existing System

The conventional electronic voting machines used in india are microcontroller/ microprocessor based manually operating machines which have many flaws. Present

electronic voting machine as shown below is having following features.

Figure 3.1 EVM used in India

- EVMs are powered by an ordinary 6 volt alkaline battery. This design enables the use of EVMs throughout the country without interruptions because several parts of India do not have power supply and/or erratic power supply.
- Currently, an EVM can record a maximum of 3840 votes, which is sufficient for a polling station as they typically have no more than 1400 voters assigned.
- Currently, an EVM can cater to a maximum of 64 candidates. There is provision for 16 candidates in a Balloting Unit. If the total number of candidates exceeds 16, a second Balloting Unit can be linked parallel to the first Balloting Unit and so on till a maximum of 4 units and 64 candidates.
- It is not possible to vote more than once by pressing the button again and again. As soon as a particular button on the Balloting Unit is pressed, the vote is recorded for that particular candidate and the machine gets locked. Even if one presses that button further or any other button, no further vote will be recorded. This way the EVMs ensure the principle of **"one person, one vote"**.
- The EVMs cannot be pre-programmed to favor a party or a candidate because the order in which the name of a candidate/party appears on the balloting unit depends on the order of filing of nominations and validity of the candidature, this sequence cannot be predicted in advance

4. Proposed system

The proposed EVM having the following features:

- GSM based voting - allows the citizens to vote using mobile phones from anywhere in the country.
- Smart card based voting using RFID - allows voters to use a smart card to verify their identity and authorizes them to cast vote. This feature has been included to exploit the advantages of the UID (Unique Identification) card or the "AADHAAR" scheme which the government proposes to introduce in a few years that will allow each citizen to be uniquely identified based on a single smart card.
- Tamper proof – in addition to the existing security features the proposed scheme provides password protection at various stages, auto-locking features, scalability and non-volatility of vote count.

The proposed EVM has been implemented on FPGA which

5. IMPLMENTATION OF THE PROPOSED SYSTEM

5.1 Basic Block Diagram

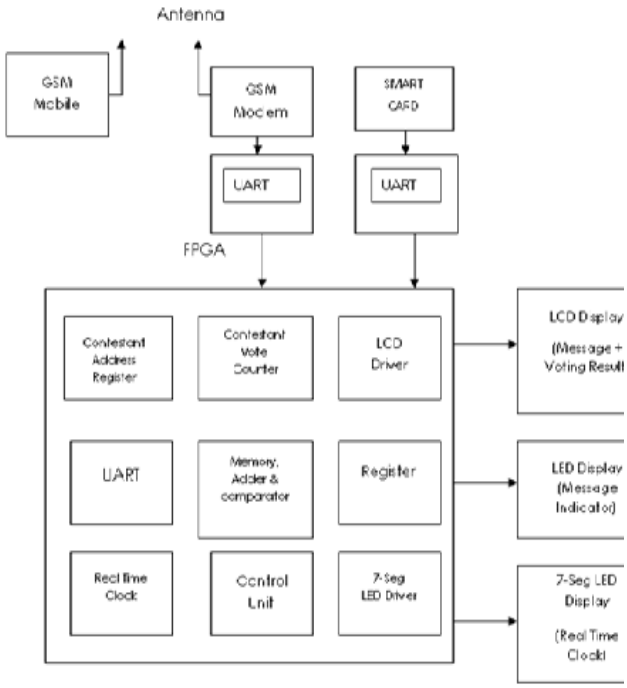


Figure 5.1 Basic Block Diagram

This shows the basic block diagram of the project. The main components being used are fpga (Spartan-2 kit in the project), gsm mobile & modem, smart card, and various display boards for displaying voting result, real time clock and indicating message. Let us see the working of this block diagram.

5.2 Description of Data Flow Diagram: -

1. Machine is initialized by admin.
2. Voting counters are open by resetting Real Time Clock.
3. Assigning the voting duration, a real time clock denoting Hours, Minutes & Seconds will be displayed in 7-seg display which will be driven by RTC module and 7-seg display driver module to be implemented in FPGA.
4. Public need to choose the type of voting method to cast their vote to their favorite candidate either by manually using smart card or by GSM mobile by sending SMS.
5. After the selection of the mode the verification process is done that voting has not been done before by any of the modes.
6. GSM modem or the smart card receives these votes; LEDs will indicate the voting number or contestant number. Votes will get added for each vote & for each contestant.
7. GSM modem sends the vote data to FPGA module through UART / MAX 232.
8. UART on FPGA module receives the data and sends it to memory and comparator to eliminate dual voting by same SIM ID.
9. If the same voter has not voted till now, the Control unit will register vote by enabling the Contestant Address Register & Contestant Vote Counter.
10. LCD driver will drive LCD to display that the Vote is validated.
11. Control Unit will send Acknowledgement through UARTs & GSM modem an Acknowledgement message.
12. After Voting time is over, the Control unit will disable the Voting counters & UART.
13. Results will be declared upon admin / Voting officer sending his PASSWORD through SMS to EVM, after voting period.
14. LCD will display the result in the format:

A=XX; B= XX & C = XX

15. For UART, we will be using MAX232 IC to interface GSM modem with FPGA module.

5.3 Functionality of Modules

The functionality of entire proposed system can be divided into two parts.

1) GSM MODEM
2) SMART CARD READER(RFID READER)

GSM MODEM and SMART CARD READER are interfaced to FPGA through UART.

The messages received from the mobile voter and the unique identification numbers (UIN) from RFID tag are displayed on the LCD which is interfaced to FPGA.

5.3.1Gsm Modem

This section explains the how GSM MODEM receiving the message from mobile voter and how it sending the acknowledgement to the mobile voter and in what way the message is displayed on LCD. The working of GSM MODEM contains two sections, UART receiver and the UART transmitter section, the UART receiver, receives the message from the mobile voter. UART transmitter sends an acknowledgement to the mobile voter.

GSM Modem Receiver Section

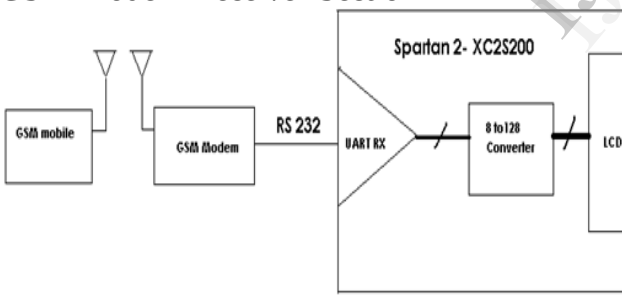


FIGURE 5.2 GSM MODEM RECEIVER SECTION

The GSM Modem receives the messages sent by the mobile voter. The GSM Modem just receives the message but to read that particular message one AT command is needed, and that AT command to read that particular message is AT+CMGR=loc ⏎ .

The modem is interfaced to the FGPA kit is through UART (RS232 cable), The UART receiver on the FPGA module receives the upcoming serial data (message) and converts it into parallel 8-bit data. In this proposed system the upcoming data (message) is displayed on the LCD display which is interfaced to FPGA board. This LCD display having the capability of displaying 16 characters at a time; it means up to 128 bits (16*8) can be displayed. For that reason one 8-bit to 128 bit converter is required and it is implemented in this proposed system.

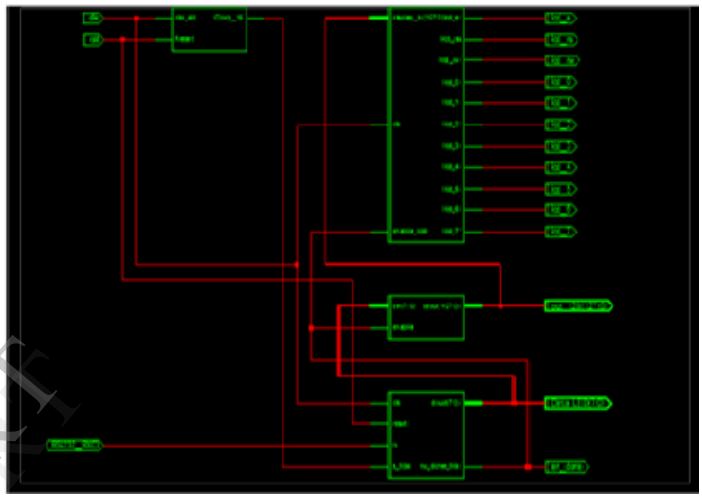


FIGURE 5.3 RTL SCHEMATIC OF THE GSM MODEM RECEIVER

This RTL Schematic shows the entire working of GSM MODEM Receiver section .First baud generator taking the available 4 MHz clock of spartan2 FPGA kit and converting it into 16 clock pulses and which is giving to UART receiver as clock. Then UART receiver takes serial data (message) from GSM MODEM through RS232 cable and converts it into 8-bit parallel data and which is applied to 8 to 128 converter. The 8 to 128 converter converts the upcoming 8-bit parallel data into 128 bits and then it is giving to LCD as input. Then LCD will display the result (message).

GSM Modem Transmitter

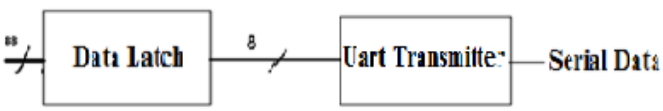


Figure 5.4 GSM Modem Transmitter section

The AT(attention) commands sent from the FPGA to GSM modem is in blocks of 88bit. Hence this module aids in serial transmission via RS232 standards.The function of the Data Latch module is to convert block of 88 bits and transmit them in blocks of 8 bits to the UART transmitter. The UART transmitter then converts the 8 bit parallel data into serial data . Then after the entire this process mobile voter will get acknowiledgement.

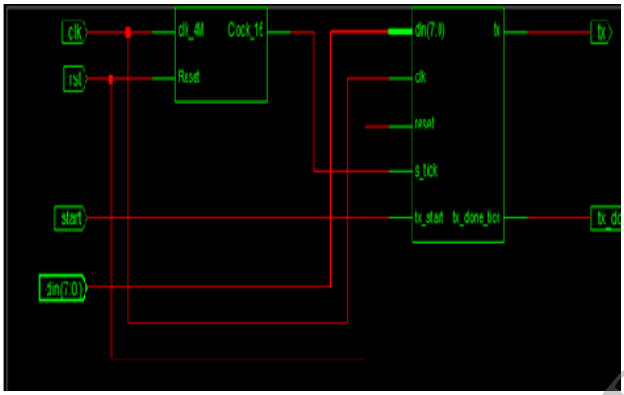


FIGURE 5.5 RTL SCHEMATIC GSM MODEM TRASMITTER

This RTL Schematic shows the entire working of GSM MODEM Transmitter section. First baud generator taking the available 4 MHz clock of spartan2 FPGA kit and converting it into 16 clock pulses and which is giving to UART transmitter as clock. Then the transmitter takes the 8 bit parallel data and converts it into serial data then through this entire process mobile voter will get the acknowledgement.

5.3.2 RFID Reader

This section explains how the RFID READER reads the unique identification number (UIN) of the RFID (Smart cards) tag and in what way the unique identification number displayed on LCD which interfaced to FPGA. The RFID reader is interfaced to the FPGA module through UART, the UART receiver on the FPGA module converts the upcoming serial data into 8-bit parallel data. The RFID tag is used in this system has the 8 character UIN (8*8=64 bits), each character has a start bit and a stop bit, totally 80 bits. Decoder converts the 8-bit parallel data into 80 bits and is displayed on LCD on the FPGA board.

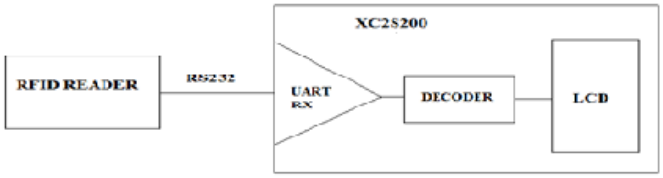


FIGURE 5.6 RFID RECEIVER SECTION

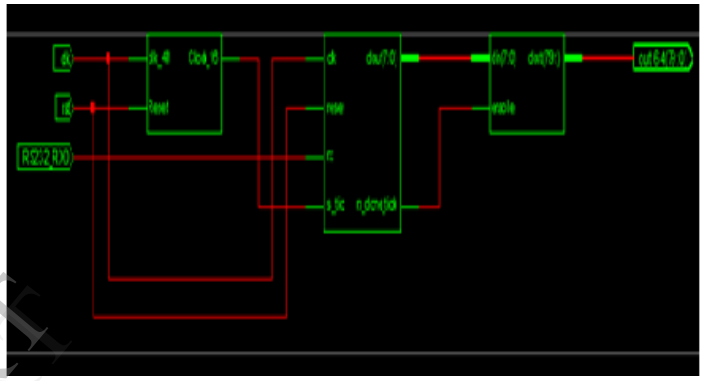


FIGURE 5.7 RTL SCHEMATIC OF THE RFID RECEIVER

This RTL Schematic shows the entire working of RFID Receiver section .First baud generator taking the available 4 MHz clock of spartan2 FPGA kit and converting it into 16 clock pulses and which is giving to UART Receiver as clock. Then the UART Receiver takes the unique identification number (UIN) from the RFID Reader through RS232 cable in a serial way then converts it into 8 bit parallel data. Then the decoder converts the 8 bit data into 80 bit parallel data. Then the 64 bits data will be giving to LCD as input. Then unique identification number of RFID tag will be displayed on the LCD which is interfaced to FPGA.

5.4 Modes of Operation

Tamper proof EVM can be operated in three different modes for the ease of operator and the user.

5.4.1 EVM in Initialization mode:

1. Candidates will be assigned Voting counters like

Congress	- A - 1001
BJP	- B - 1002
JD (U)	- C - 1003

2. Timer can be adjusted to set the Voting hours or time – a real time clock will be running inside FPGA to track the voting time.
3. Voting counters will operate only in the above set duration – say 10 mins, 1 hour or 24 hours etc.

5.4.2 EVM in voting mode:

1. Real Time starts as set in previous mode.
2. Select the option of casting vote by one of the two modes.
   a. Smart card voting mode.
   b. Mobile voting mode.
3. After the selection of the mode the verification process is done that voting has not been done before by any of the modes.
4. Using Radio Frequency Identification Tags (RFID Tags) public can cast their vote to their favorite contestant by an ID check done by Radio Frequency based smart card reader and then cast the vote.
5. Using any GSM mobile public can cast their votes to their favorite contestant by way of SMS.
6. Voter will get the voting message acknowledgement by SMS delivery message.
7. Voter's GSM id will be kept in memory to stop double voting by same voter for the same contest

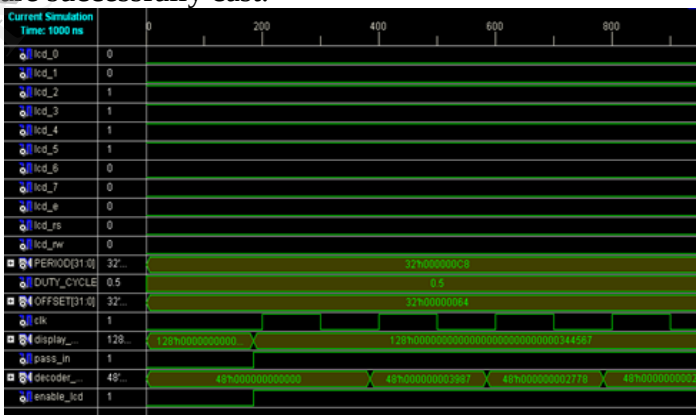
5.4.3 EVM in Counting / Result mode:

1. After set voting time, the EVM will need a password from the Voting Officer or the administrator to declare the results.
2. Admin / Voting Officer will send his password in SMS to EVM & immediately the results will get declared.

6. SIMULATION RESULTS

SIMULATION RESULT 1: LCD DISPLAY with enable being applied periodically

This module displays the vote count as well as the necessary confirmation when votes are successfully cast.



Lcd_0 to lcd_7: 8 bit data input to LCD controller

enable_lcd: is used to enable the LCD and provide delay between enabling the display characters

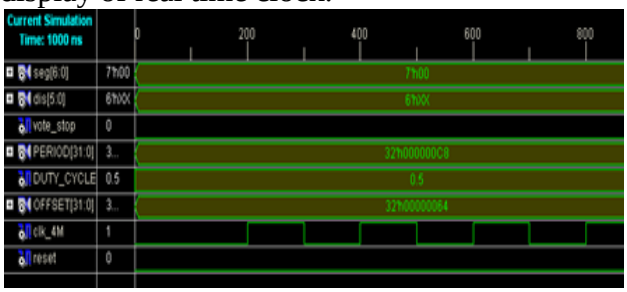
pass_in: indicates password has been sent. The vote count can be displayed. If this signal is low it will not display the results.

Lcd_rs : rgister select control signal for lcd

Display_128: 128 bit input (16 characters of LCD * 8bit each character = 128 bits to be displayed)

SIMULATION RESULT 2: Seven segment display

Seven segment display is used for the display of real time clock.



Vote_ stop: input signal indicates that the voting process time is over. When this signal goes high the system enters the auto locking mode.

Clk_4M: is the reference input clock signal. authorized mobile phone. It also takes in the smart card ID and verifies its authenticity by comparing it with its database.

7. CONCLUSION

The tamper proof EVM aid in making the voting system more secure, reliable, mobile, flexible and scalable. With the features of mobile voting and smart card voting the proposed system is cited to increase the percentage of vote count recorded in India. There is no chance that a vote for one candidate to be transferred to another candidate. The policy of ONE PERSON- ONE VOTE, with no possibility of duplication has been strictly implemented. There is no chance for a vote to disappear. The system can easily aid in reliable recounts. The system supports voter-verifiability. A remarkable fact is that it preserves voter anonymity at the same time. In addition we propose these possible enhancements in future.

8. REFERENCES

1. Muhammad Raisul Alam, Md. Masum, Md. Mostafizur Rahman and Md. Arifur Rahman "Design and Implementation of Microprocessor Based Electronic Voting System" Proceedings of 11th International Conference on Computer and Information Technology (ICCIT 2008)25-27 December, 2008, Khulna, Bangladesh.
2. Jeremy Clark, Aleks Essex and Carlisle Adams "Secure and Observable Auditing of Electronic Voting Systems using Stock Indices" 0840-7789/07/$25.00 ©2007 IEEE
3. Leyou Zhang, Yupu Hu, Xu'an Tian and Yang Yang "Novel Identity-based Blind Signature for ElectronicVoting System" 978-0-7695-3987-4/10 $26.00 © 2010 IEEE DOI 10.1109/ETCS.2010.198
4. Ying Qiu and Huafei Zhu "Somewhat Secure Mobile Electronic-voting Systems Based on theCut-and-Choose Mechanism" 978-0-7695-3931-7/09 $26.00 © 2009 IEEE DOI 10.1109/CIS.2009.39
5. Arunkumar.N and Arunkumar.P.L "Analysis, Design & Real-Time Implementation of Electronic Voting Machine".
6. J. Paul Gibson, Eric Lallet, and Jean-Luc Raffy "Engineering a Distributed e-Voting System Architecture: Meeting Critical Requirements" H. Giese (Ed.): ISARCS 2010, LNCS 6150, pp. 89–108, 2010.c_Springer-Verlag Berlin Heidelberg 2010.
7. Rui Joaquim, André Zúquete and Paulo Ferreira "REVS – A ROBUST ELECTRONIC VOTING SYSTEM"
8. Mohammad Hajjar, Bassam Daya, Anis Ismail and Haissam Hajjar "AN E-VOTING SYSTEM FOR LEBANESE ELECTIONS" Journal of Theoretical and Applied

Information Technology© 2006 JATIT. All rights reserved.

9. Wei-Chi Ku and Chun-Ming Ho "An e-Voting Scheme with Improved Resistance to Bribe and Coercion.