Advanced Security System of Electronic Voting Machine using the Self-destruction Circuit

Pritha Roy, Surinder Singh Arora

Abstract--- The objective of this project is to develop a protection circuit for the electronic voting machine. The main aim of the system is to develop a timer controlled self-destructing circuit for reducing the chances of tampering whether it be data tampering or circuit tampering within the EVM [1]. The Electronic voting machine is used for counting the total number of votes polled in the particular polling booth during the elections and in those scenarios the tampering of the EVM is quite often to be found. In our project we will be using the circuit destroyer module which is controlled by a timer circuit that will trigger on when the data is once taken as input for the polling and the box is enclosed. As the box is once closed the timer circuit is triggered and whenever the box is tried to open or tampered before the stipulated time period the relay switches on the power signal to the self-destructive circuit which in turn destructs the circuit of the electronic voting machine so the data collected is transferred to a hard drive for data extraction and the machine can neverbe used again by tampering. Thereby ensuring the voters vote security and lessening the violation of the rights of the particular citizen.

I. INTRODUCTION

The advance security of the EVM concerns with secured voting medium where the voters cast their vote without any difficulty.

The existing VVPAT system concerns with ballot paper system which shows the vote casted on the EVM but the system is too costly which the SEC does not mandates to count during vote calculation as it is too time consuming. It can also prove to be a hoax as the paper which is to be printed after the vote is casted can also be a digital illusion or the circuit system for the vote calibration and the printing of the casted votes can be separately operated to keep the peopleaway from the reality of the data manipulation EVM can be tampered by different electrical & data manipulation systems.

This system ensures the security of the circuitry and the data by destroying the main circuit in case of any manipulation with the system.

There are two existing designs which is the normal electronic voting machines which have been used till date and the newly designed system the VVPAT[6] (Voter Verified Paper Audit Trial) where the voters gets to see the print of the vote casted The tampering can be done in the internal circuitry of the system by separating the link between the paper audit trial and the counted votes in the software.

[8]There are many tampering methods such as data manipulation methods that are found to be improvised in this such as the dishonest display which adds a separate hidden microcontroller that gets the data of the total votes casted using the PIC16F914 microcontroller & KC Wire free KC 22 Bluetooth module and substitutes it with manipulated & fraudulent results by replacing the hardware component.

[5]Next the clip on memory manipulator attack system in which at any time between the start of the polling and till the counting, dishonest election insiders and criminals could use the clip-on device to change the data recorded in the EVM.

So as to prevent the particular acts the prevention technique has beenproposed in this project.

In addition to the software it also might get tampered by the manufacturer which cannot be easily be detected as the software have been issued by the manufacturer before it was installed in the CPU of the particular system.

He or she can substitute the version without being caught by the outsiders using the back door procedures as they are the sole manufacturers. They can even substitute with the look alike CPUs.

Tabulation for the threats on EVM

No.	Type of attacks	Brief
1.	**Dishonest display attack**	It adds a separate hidden layer of microcontroller that gets the data from the total votes casted using the PIC16F914 microcontroller & KC Wire free KC 22 Bluetooth module and substitutes it with manipulated & fraudulent results by replacing the hardwarecomponent
2.	**Clip on memory attack**	It is used to change thedata recorded within the system .[4]

Fig. 1: Table for the details of the attacks

The particular models of evm which are till now made into use are all can be tampered very easily by these following methods, so as to ensure the security of the voters the proposed model is stated.

Manuscript receivedJune 10, 2019 .

Pritha Roy, B. Tech in Electrical and Electronics Department, SRMIST Ramapuram.Chennai, T.N, India.(e-mail: roy.prit.1997@gmail.com)

Surinder Singh Arora, B. Tech in Electrical and Electronics Department, SRMIST Ramapuram.Chennai, T.N, India.(e-mail: amit.arora271@gmail.com)

Block Diagram

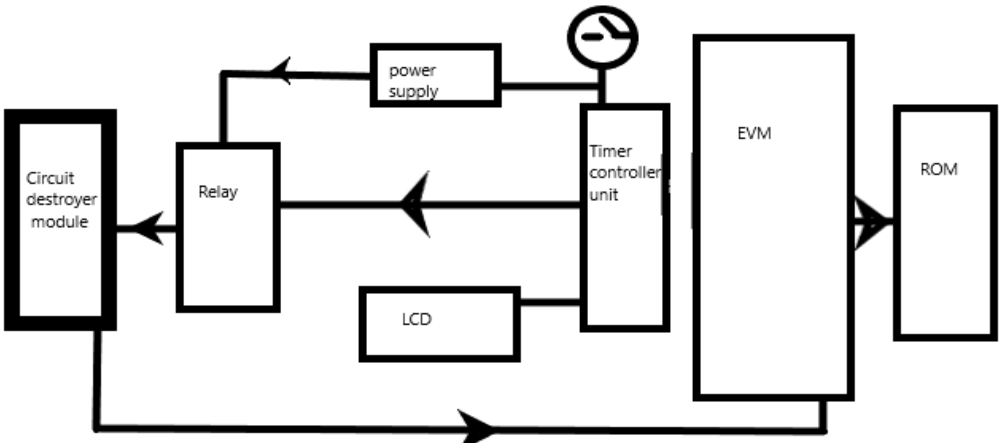

Fig. 2: Block diagram of the timer controlled circuit of the of the circuit destruction module for the EVM

Algorithm

Step 1: For opening the box the push button switch is pressed which in turn signals the lock to open.

Step 2: The push button switch signals the timer circuit to initiate a loop within it.

Step 3: The system derives power from the 5v battery source.

Step4: When the switch is pressed again the input initiated is checked with the timer condition, if the signal is found to be initiated after the timer loop is over then the signal wont initiate the power supply to the relay.

Step 5: Else if it satisfies the timer condition it will initiate the relay to switch the self-destruction unit

.Step 6: A high voltage will be supplied satisfying the condition of the timer control unit

Step 7: the data will be stored in a readable disc for data recovery.

Circuited block diagram

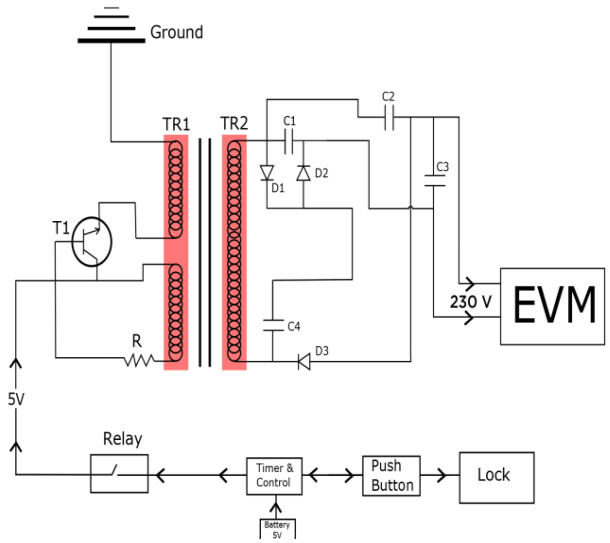

Fig. 3:Circuit diagram for the timer controlled protection system of EVM

Working

The particular diagram describes the working of the particular system. The data which is stored is secured by the timer integrated circuit (Multifunctional delay time module switch control relay cycle timer) which tends to trigger when the lock is opened with the push button switch and the destruction circuit triggers the high voltage AC signal to the particular EVM as the timer control unit checks whether the data which is received form the push button switch is under the timer count or if the data satisfies the above time limit or not , if it does so the relay control unit of the above device closes the connection thereby destroying it and the present data gets transferred into a ROM for data recovery in emergency cases there by solving the problem of threat to tampering of the above EVM.The above destruction module receives 12 volt dc from the battery source and converts into ac output of about 200 volts which as result destroys the CPU, the controlling of the system is done using the adjustable timer unit with relay control which senses the data of the relay control switch and compares the present time with the time left for the timer to run depending on that the above circuit and closes the circuit connection depending on the device status and thereby the power from the destruction module is transferred through the USB port which destroys the internal system of the circuit in seconds.The above data gets directly stored in the ROM while the votes are counted in a separate area which is only a readable unit which cannot me rewritten or manipulated which helps in securing the data when the device gets destroyed in any emergency tampering faced situation.

II. SIMULATION DIAGRAM & RESULTS

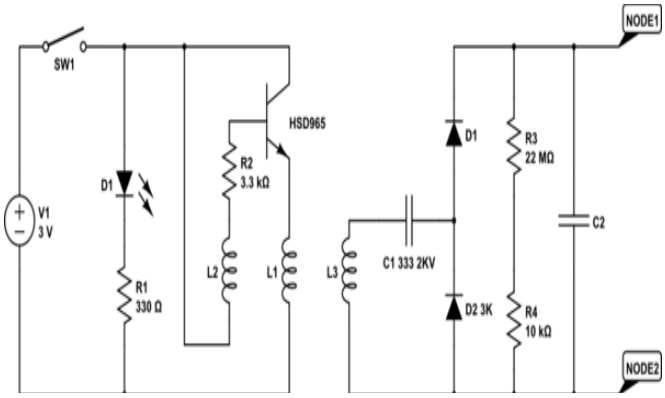

Fig. 4: Simulation circuit for self destructoin circuit

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

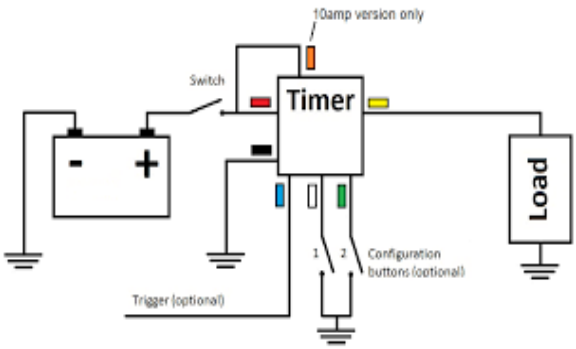

Fig. 5: Multifunciontimer relay cercuit diagram that controls the switching operation of the circuit

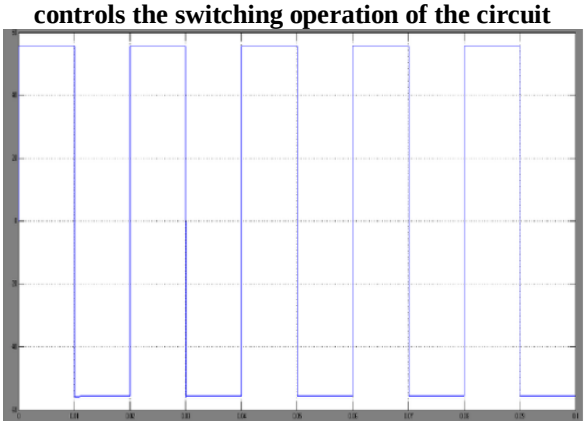

Fig. 6:Simulation result for the output wave form of the particular destruction circuit.

III. RESULT

The particular simulation shows the output waveform of the destruction circuit which is the amplified waveform of the particular inverter circuit embedded in the circuit module. It is the amplified signal which gets stored in the capacitor bank of the particular module.

IV. ADVANTAGES

- It does not allows the intruders to manipulate with the design or the order in which the vote is to be casted as the circuit is being protected using the self-destruction module.
- The circuit cannot be manipulated by any external link as the circuit is not connected to any Wi-Fi network system
- The circuit gets automatically destroyed during any forceful intervention.
- A back up data storage is created using readable storage.

V. CONCLUSION

The proposed design is made for preparing the protection system for the hardware and the software from the illegal piracy of data that can be stored in the evm. The data which was previously stored is redirected automatically to a readable memory compartment for later retrieval of the data for emergency situation which cannot be manipulated, As the device provides with a processor destruction circuit that act as a high voltage generator which is integrated with the timer control unit of the project, helps to provide the security status to the EVM by destroying the circuit module of the particular within seconds. This in turn provides the user to have a trust worthy device for voting ensuring them that no-one will ever try to tamper it coz if they try to manipulate the results the voting would me ceased for that particular device.

REFERENCES

1. D. Ashok kumar&T.UmmalSaritaBegum,"Electronic voting machine".[International Conference on Pattern Recognition", Informatics and Medical Engineering (PRIME-2012)];
2. Sahibzada Muhammad Ali,"Micro controller based smart evm",[IEEE International Conference on Electro/Information Technology];
3. A.K.Wang,"EVM Simulation and analysis techniques"[MILCOM 2006 - 2006 IEEE Military Communications conference];
4. P. Vidyasree, S. ViswanandhaRaju, "Desisting the Fraud in India's Voting Process through Multi Modalbiometrics",[2016 IEEE 6th International Conference on Advanced Computing (IACC)];
5. R. Geambasu, T. Kohno, A. Levy, H.M. Levy, Vanish,"Increasing data privacy with self-destructing data", [Proc. of the 18th USENIX Security Symposium, 2009].
6. DnyaneshP.Lengure,Dines V.Rojatkar, "Hacking free system in EVM",[InternationalJournal of Electrical andElectronics Research];
7. Zuheir Desai, Alexander Lee, "Technology,Choice,and Fragmentation The Political effects of Electronic Voting" [India2016 IEEE 6th International Conference on Advanced Computing (IACC)];
8. Hari K. Prasad, J Alex Halderman, RopGonggrijp, "Security analisys of India's EVM" ,[Proc. 17th ACM Conference on Computer and Communications Security (CCS '10), Oct. 2010];
9. A. Aviv, P. Cerný, S. Clark, E. Cronin, G. Shah, M. Sherr, and M. Blaze. "Security evaluation of ES&S voting machines and election management system".[InProc.USENIX/ACCURATE Electronic Voting Technology Workshop (EVT), San Jose, CA, July 2008].
10. W. Appel, M. Ginsburg, H. Hursti, B. W. Kernighan, C. D. Richards, G. Tan, and P. Venetis. "The New Jersey voting-machine lawsuit and the AVC Advantage DRE voting machine". [In Proc. Electronic Voting TechnologyWorkshop; Elections (EVT/WOTE),Montréal, Canada, Aug. 2009].
11. Election Commission of India. Information under RTI on EVMs. [July 2009. No. RTI/2009-EMS/39. Election Commission of India. Electronic voting machines–Regarding. Aug. 8, 2009. No. PN/ECI/41/2009].
12. R. G. Johnston. Tamper-indicating seals. In American Scientist, pages 515–523, [November–December 2006].
13. C. R. Kasarbada, P. V. Indiresan, and S. Sampath."Report of the expert committee for the technical evaluation of the electronic voting machine".[Apr.1990.ExpertCommittee-Report-on-EVM, pages 21–37].
14. T. Kohno, A. Stubblefield, A. D. Rubin, and D. S. Wallach. "Analysis of an electronic voting system".[In Proc. IEEE Symposium on Security and Privacy,Oakland, CA, pages 27–40, May 2004].
15. R. Mehta. How 100,000 EVMs can be tampered by just 10–12 people at top.[evm1.pdf, 2009].
16. Press Trust of India."Compulsory voting not practical", [CEC. Apr. 26, 2010].