International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 07 Issue: 04 | Apr 2020 www.irjet.net p-ISSN: 2395-0072

IoT based EVM

Arun Kumar S[1], Logesh D[2], Mageshwaran B[3], Kavitha Balamurugan[4]

[1, 2, 3] *Students, Dept. of ECE, KCG College of Technology, Chennai - 97*
[4] *Associate Professor, Dept. of ECE, KCG College of Technology, Chennai, Tamil Nadu, India*

Abstract - *Currently used Electronic Voter Machines [EVM] have vulnerabilities, which led to many cases that testified the security of both Electronic Voter Machine (EVM) and the Voter Verified Paper Audit (VVPAT) system. Some cases infer that these machines are tampered and the votes are hacked from one party to another. There are several problems in the existing voter machine such as no transparency to the voter, limited storage capacity, Separate ballot and control unit and chance for bogus voting as authentication purely depends on the officer in the polling booth. Our idea solves these problems by bringing transparency in the voting process, using Internet of Things (IoT) based technology to store votes in a cloud server with a new protocol called Random Code Transmission Protocol, making each machine an independent unit and reducing bogus voting with biometric authentication. Our idea is to provide an electronic voting machine which is a highly secure and efficient voting system to our country.*

Key Words: Electronic Voter Machine, Internet of Things (IoT), Transparency, Bogus Voting, Cloud Server, Biometric Authentication

1. INTRODUCTION

The Indian electronic voting machine (EVM) was developed in 1989 by Election Commission of India in collaboration with Bharat Electronics Limited (BEL) and Electronics Corporation of India Limited (ECIL). Since then the electronic voting machines have been used in all general and state assembly elections of India since 2004. Out of 120 countries that follow democracy, only 31 countries use EVM for either for small elections or nationwide. Other countries still use paper voting system as they have no trust in EVMs. Some cases were filed in the Supreme Court of India testified the security of these EVM which are still left unanswered. There is no transparency to the voter about the voting process and the process inside the machine. Even BEL, ECIL and Election Commission of India cannot read the software inside the EVM. There is only limited storage capacity. Each EVM is separated into two units, a ballot unit and a control unit. It brings complexity to the system. Also, the chance for bogus voting is high as the authentication purely depends on the officer in the polling booth. The voting process involves a lot of man power which can be reduced. Hence a solution that uses modern technological advancements to resolve these problems becomes necessary. This paper proposes such a solution that solves the problems in the existing machine and provides an efficient voting system that is highly safe and secure.

2. PROPOSED ARCHITECTURE

Our idea proposes an EVM that uses IoT based technology to transmit the votes from the machine to the cloud server through Wi-Fi. This EVM includes a QR code scanner to scan the QR code present in the AADHAR card of the voter. The QR code is used to obtain the details of the voter such as fingerprint and name from the AADHAR Database. These details are compared with the fingerprint obtained using a Biometric sensor during voting process. Only after the validation of the voter, the vote is taken into count. This prevents bogus voting and assures that only the voter casts the vote himself/herself. The EVM brings transparency by displaying the entire program running inside the machine when the concerned button to display the program is pressed. Since all the functions are incorporated into a single unit, this EVM doesn't require any control unit. The section below describes the voting process involved during an election with our EVM.

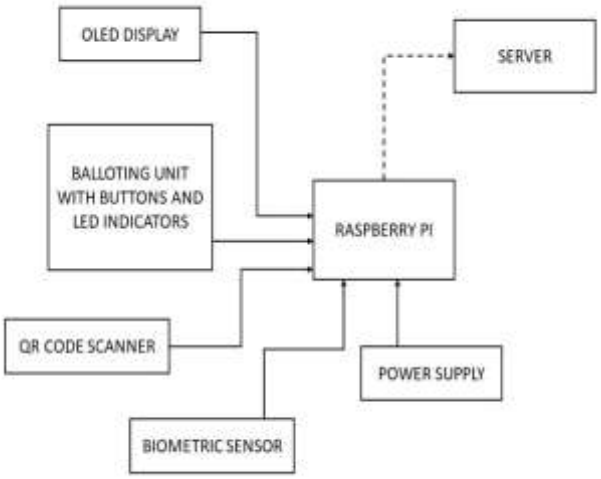

Fig -1: Internal Architecture of the proposed EVM

The Raspberry Pi has an inbuilt Wi-Fi module which is here used to transmit the votes through the internet. An Organic Light Emitting Diode (OLED) is used to display the status of the voting. The balloting unit consists of a number of buttons and LEDs corresponding to the candidate's name and party. The LEDs serve as an indicator to the button pressed respective to the candidate. A Battery of 3000 mAH is used as the power supply to the EVM in order to last long for one day. A provision for direct power supply will also be available for emergency purpose.

2.1 Voting Process

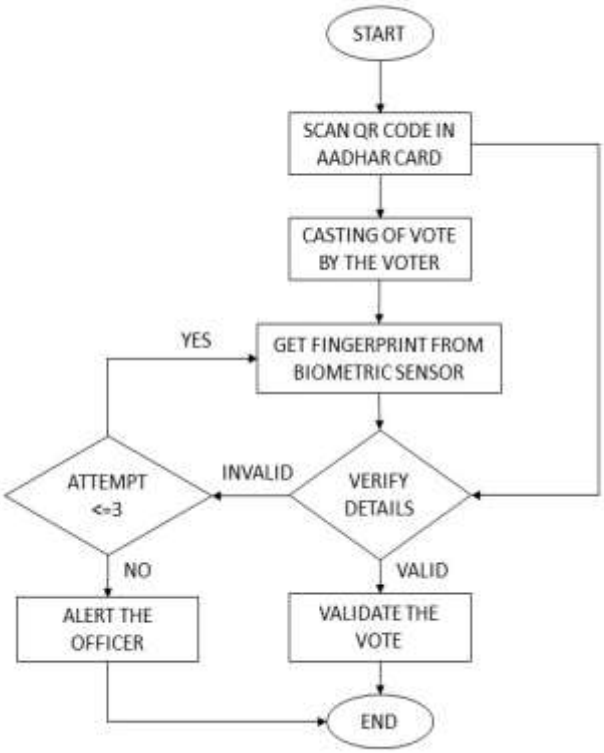

Fig -2: Flow chart of the voting process with our proposed architecture

The voting process starts with the scanning of QR code in the AADHAR Card. The voter details are fetched from the database. Then the voter has to cast the vote followed by placing his/her thumb on the biometric sensor. The fingerprints are compared and only then the votes are taken. If the vote is taken into count, it is indicated with a beep from the buzzer. If the fingerprint didn't match, the voter is given three more chances to validate the fingerprint. Else the officer in the polling booth will be alerted through the rapid beep sound from the buzzer. From the beginning of the process till end, the voting status is displayed in the LED Display. Whenever a vote is validated, the vote is transmitted to the server through internet. Like VVPAT system, the candidate and party name to which the voter has voted will be displayed for 7 seconds in the LED display.

2.2 Transmission Protocol

To make the system more secure, we implement our new protocol called Random Code Transmission Protocol (RCTP). This protocol runs over TCP/IP uses 64-bit data segment for transmission. The protocol uses Transport Layer Security (TLS) for encryption. The data format of the protocol, below the fixed header will be random and different for each transmission of data. This format is decided by the sequence number and format offset bits in the fixed header of the data packet. The server (receiver) has to decode the data based on this sequence number and offset. If there is a change in the format, it indicates that either the data is manipulated or there is some error in the transmission. Hence the data manipulation can be easily identified. This protocol provides additional security to ensure secure transmission of votes to the server. The data format of the protocol is given below in the 'Fig-3' and the 'Table-1' describes the fields in the data format.

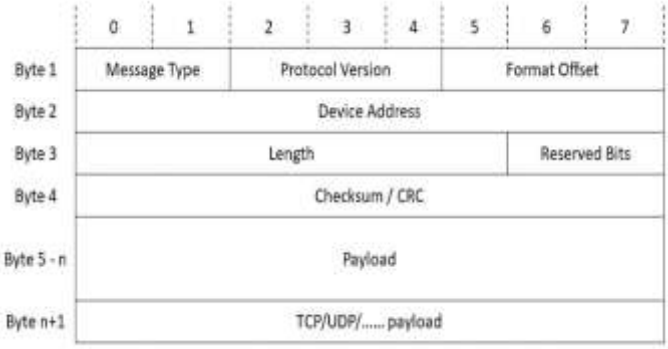

Fig -3: Data Format of RCTP

Table -1: Fields in the Data Format of RCTP

Field	Description
Message Type	It indicates the type of the message, whether it is a post or get message.
Length	It defines the header length
Protocol Version	It indicates the version of the protocol used
Format Offset	These two fields are used to define the format of the data packet below fixed header
Device address	This field contains the address of the EVM
Reserved Bits	This field can used for future purposes.
Checksum / CRC	It is used for cyclic Redundancy check or checksum of the payload
Payload	It contains the data (votes) to be transmitted
TCP/UDP Payload	It contains the payload from TCP/UDP/other protocols

2.3 Server End Process

The votes are stored in the server using blockchain technology. Since by design, the blockchain technology is resistant to data modification, the votes are stored securely. Our solution includes a software running in the server which segregates the votes and provides the overall result of the election. The votes are stored and classified by the constituency which makes easier to identify the EVM and the number of votes from it. The total number of votes from each constituency, total number of votes from each polling booth,

total number of votes to a party in a state and analysis on overall percentage of votes acquired during the election can be accessed from the software in the server. This reduces the workload to make analysis and eliminates the need for a day of counting process.

3. RESULTS

Fig -4: Prototype of our proposed architecture

Fig -5: Internal architecture of our prototype

Fig -6: Screenshot of software displaying the vote results in server

Fig -7: Screenshot of Data Packet of RCTP protocol received in the server

Our proposed architecture is demonstrated with the prototype as shown in Fig-4 & Fig-5. The box case of the prototype is made up of 6mm plywood as it weighs lighter. The box case has a closable board on top, which can be screwed and sealed. The Fig-6 shown above is the screenshot of the software that displays the votes from the EVM taken in the PC that acts as the server here. The Fig-7. shows the data packet of our protocol 'RCTP'. In Fig-7, to demonstrate the security of our protocol we added an option to replace the packet received for decoding. Even if a small part of the packet is manipulated, the checksum will not match with manipulated packet. Hence manipulation of data can be easily identified. The software will notify if such type of manipulation occurs.

4. CONCLUSIONS

Expected outcome of our proposed architecture is an easy, efficient and secure voting system through our EVM. Our solution makes the whole election process more easy and secure. It also reduces the overall manpower involved in the election process. We believe that this system will create an impact in the society as it brings transparency between a voter and the voting machine, so that people will have trust in the voting system.

REFERENCES

[1] J.Deepika, S.Kalaiselvi, S.Mahalakshmi, S.Agnes Shifani , "Smart Electronic Voting System Based on Biometric Identification-Survey", Third International Conference on Science Technology Engineering & Management (ICONSTEM), 2017.

[2] Anandaraj.S, Anish.R, Devakumar.P.V, "Secured Electronic Voting Machine using Biometric", IEEE Sponsored 2nd International Conference on Innovations in Information, Embedded and Communication systems (ICIIECS), 2015.

[3] B.Madan Mohan Reddy, D. SrihariRFID, "Based Biometric Voting Machine Linked to Aadhaar For Safe and Secure Voting", International Journal of Science, Engineering and Technology Research (IJSETR), Volume 4, Issue 4, April 2015.

[4] Ansif Arooj, Mohsin Riaz, "Electronic voting with biometric verification Offline and Hybrid EVMS solution", The Sixth International Conference on Innovative Computing Technology , 2016.

[5] Gomathi B, Veena Priyadarshini S, "Modernized Voting Machine using Finger Print Recognition", International Journal of Scientific & Engineering Research, Volume 4, Issue 5, May-2013.

[6] Ankit Anand, Pallavi Divya, "An Efficient Online Voting System", IJMER Vol.2 Issue. 4 July-Aug-2012.

[7] Himanshu Agarwal, G.N.Pande, "Online voting System for India based on AADHAAR ID", IEEE (ITC&KE), 2013 11th International Conference 20-22, Nov-2013.

[8] David Jefferson, Aviel D. Rubin, Barbara Simons, and David Wagner, "Analyzing Internet voting security", Communications of the ACM, vol. 47(10), Oct. 2004, pp. 59-64.

[9] Mohan M, Nagamanikantha E, Naresh V, Naveen Kumar H.V, Raji, "Next Generation Electronic Voting Machine using Biometric and Voice Feedback" , IEEE sponsored International Conference on Communication and Signal Processing (ICCSP), 2018.