Global Journal of Computer and Engineering Technology (GJCET)

Vol. 3, No. 1, January, 2023 ISSN: 2767-1933

DESIGNING A VOTING SYSTEM TO DETECT FRAUDULENT VOTERS

S.K. Peer, KSRM College of Engineering, India (skpeer@ksrmce.ac.in)
Rakesh K. Sharma, University of Maryland Eastern Shore, USA (rksharma@umes.edu)
Julius A. Alade, University of Maryland Eastern Shore, USA (ajalade@umes.edu)

ABSTRACT

A fraudulent voter refers to a person involved in the impersonation or proxy of a voter during the casting of votes through the specified voting system. The use of Electronic Voting Machine (EVM) accompanying Voter-verified paper audit trail (VVPAT) is in practice in major democratic countries like India. The election commission of India used EVM (Electronic Voting Machine) accompanying VVPAT (Voter-verified paper audit trail) on a pilot trial basis in the 2014 general elections. This system has been used in every assembly and general election in India since 2019 as per the directions of the supreme court of India. It is an M3 version of EVM with VVPAT capability compared to the previous M1 and M2 versions. It has embedded hardware and software that enables only a particular control unit to work with a particular voting unit to avoid tampering. An EVM consists of two units, a control unit, and a balloting unit. The control unit is operated by one of the polling booth officers, while the balloting unit is operated by the voter in privacy. The officer confirms the voter's identification and then electronically activates the ballot unit to accept a new vote. Once the voter enters the vote, the balloting unit displays the vote to the voter, records it in its memory and transfers the vote to the printing unit. The voter places the print copy of the vote in a ballot box, which may be used for cross-verification in case of a dispute. A "close" command issued from the control unit by the polling booth officer registers the vote and relocks the unit to prevent multiple votes. The process is repeated when the next voter with a new voter ID arrives before the polling booth officer. This system is not equipped with a measure to avoid electoral fraud of impersonation or proxy which can reduce voters' confidence in democracy. Hence, there is a need to develop a system that determines fake voters and rejects them from voting. The proposed system is equipped with a device and software to incorporate the features to read and match identification numbers and biometric measures of the voter with that of the database of the system, to identify the fake voter. This system is useful in increasing voters' confidence in democracy in democratic countries as many more popular countries are moving towards a democratic system.

Keywords: EVM with VVPAT, Control unit, Balloting unit, Fraudulent voter, Impersonation of the voter, Proxy voter, Personal identification number, Thumb impression, Iris impression, Tampering-proof layers, EVM tracking system.

1. INTRODUCTION

The electronic voting system replaced the paper ballot and manual counting of votes in the majority of countries across the world. Political party loyalists used to capture the polling booths to exercise fraudulent voting and stuffed them with pre-filled fake ballots in case of a paper balloting system. The paper balloting system is also more expensive as it involves printed paper ballots and requires substantial post-voting resources to count hundreds of millions of individual ballots (Verma, 2005; Madhavan, 2019). Electronic voting was proposed to face the challenges of paper-based voting to ensure accurate and bias-free elections (Daramola et al., 2020). The features of embedded EVM such as the mechanism to confirm the identity of the voter and control the rate of casting votes (Verma et al., 2005), etc. contribute to reducing electoral fraud and abuse, eliminating booth capturing and creating more competitive and fairer elections (Debnath et al., 2017). India is a major democratic country and its election commission used EVM (Electronic Voting Machine) accompanying VVPAT (Voter-verified paper audit trail) on a pilot trial basis in the 2014 general elections (The Times of India. 20 January 2012, and Daily News and Analysis. 27 April 2014). This system has been used in every assembly and general election in India since 2019 as per the directions of the Supreme Court of India. It is an M3 version of EVM with VVPAT capability compared to the previous M1 and M2 versions. It has embedded hardware and software that enables only a particular control unit to work with a particular voting unit to avoid tampering. Indian EVMs are stand-alone non-networked machines (The Times of India. 6 March 2017). The literature related to the application of technology in the development of smart, secure, and versatile public voting

systems is reviewed, to outline research gaps for recommending new approaches to the existing systems (Chandra, et al., 2020).

EVMs in India manufactured by Bharat Electronics Limited, Bangalore and Electronics Corporation of India Limited, Hyderabad are powered by an ordinary 6-volt alkaline battery (ECI Voting Equipment, 2019). These units have many tamper-proof protocols. Their hardware, by design, can only be programmed once at the time of their manufacture and they cannot be reprogrammed (The Hindu, March 10, 2019). An EVM is consisting of two units, viz., a control unit, and the balloting unit that are connected by a five-meter cable. The control unit controls the ballot units, stores voting counts and displays the results on 7-segment LED displays, whereas a balloting unit facilitates voting by a voter via labelled buttons. One of the important features of the controller unit is that once the controller is manufactured, no one, including the manufacturer can change the program, etched permanently in silicon at the time of manufacturing.

The balloting unit is placed inside the voting compartment and operated by the voter in privacy. The balloting unit presents the voter with blue buttons (momentary switch) horizontally labelled with the corresponding party symbol and candidate names. The balloting unit has an internal real-time clock and a protocol by which it records every input-output event with a timestamp whenever they are connected to a battery pack. An EVM can record a maximum of 3840 (now 2000) votes and can cater to a maximum of 64 candidates. There is provision for 16 candidates in a single balloting unit and up to a maximum of 4 balloting units with 64 candidate names and the respective party symbols can be connected in parallel to the control unit (Shrivastava et al., 2016). After a 2013 upgrade, an Indian EVM can cater to a maximum of 384 candidates plus "None of The Above" option (NOTA) (India Today March 15, 2019).

On the other hand, the control unit is operated by the presiding officer or polling booth officer. The voting process starts with the verification and validation of voter's identification by the polling booth officer. The control Unit provides the officer-in-charge with a "Ballot" marked button to proceed to the next voter, instead of issuing a ballot paper to them. Once the polling booth officer confirms the voter's identity, then the ballot unit is activated electronically to accept a new vote and the voter is permitted to enter the vote. This activates the ballot unit for a single vote from the next voter in the queue. The voter has to cast his vote by once pressing the blue button on the balloting unit against the candidate and symbol of his choice. As a result, the symbol of the vote is displayed on the balloting unit displays for the voter and recorded in memory of balloting unit. It transfers the symbol to the display unit for the confirmation of voter and the same symbol is transferred to printer. The voter places the print copy in the ballot box for its verification, in case of discrepancy. Then the polling booth officer issues a "close" command from the control unit to register the vote and relocks the unit to prevent multiple votes. This process is repeated for the next voter with a new voter arriving with ID before the polling booth officer (Shrivastava, 2016; Tere, 2016).

This system of voting is not included with mechanism to curb fraudulent voter and it is required to design EVM with VVPAT to identify and reject fraudulent voter. This paper presents a model of advanced version of EVM with VVPAT to identify and reject fraudulent and impersonal voters. Next section of the paper presents designing the model of the proposed system. Section 3 presents working procedure of the proposed system. The benefits and use of the proposed system are explained in section 4 and the conclusions on the proposed voting system are presented in section 5. Finally, the paper ends with the scope for future generation technology for voting system to increase the confidence in democracy.

2. DESIGNING THE PROPOSED SYSTEM

The electronic voting machines of M3 with VVPAT facility version are built and encoded with read-only masked memory software. These machines are in use at present rather, the older versions of M1 and M2 versions of machines. They are placed at the state-owned and high-security premises of the Bharat Electronics Limited and the Electronics Corporation of India Limited (India Today, March 15, 2019) in India. The various features included in M3 machine are: (1) It is embedded with unique hardware and software that enables only a particular control unit to work with a particular balloting unit. (2) These EVMs are not connected in network and stand-alone machines (Bhagia, 2019). (3) These are equipped with real-time EVM Tracking Software (ETS) for tracking the inventory of election EVMs with its digital verification identity and physical presence. These features incorporate three-layer tamper proofing capability in M3 version VVPAT EVMs.
Design of the proposed EVM includes two units, such as control unit operated by polling booth officers and balloting unit operated by the voter in privacy are joined by a five-meter cable. A voter makes use of balloting unit for voting

through labeled buttons. Control unit controls the ballot units, stores voting counts and displays the results on 7 segment LED displays. Operating program is permanently etched in silicon of controller used in EVMs at the time of manufacturing. The upgrade of EVMs that followed modified the EVM software and a printer was attached to the machine. With the VVPAT system, when a vote is cast, it is recorded in its memory and simultaneously a serial number and vote data are printed out. The print copy of a vote cast is placed in the ballot box by the voter. Later, these printouts are used for cross-checking the voting data stored in the EVMs, in case of discrepancies.

Polling booth officers use the control unit first to verify the voter identification number (Adhar card number in India) as shown in Figure1. Once the identification number is matched with that of in the database of the system, then bio-metric (thumb or Irish) identification of the voter is verified in the second stage of authentication as shown in Fig.1. Otherwise, a voter is identified as a fraudulent voter and he is not permitted to move for further identification. A fraudulent voter can handle authenticated identification number of a voter and the same identification number handled by a fraudulent voter will get matched with that of in the database of the system in the first stage of the authentication verification process. Hence, it is required to implement biometric verification in the second stage of the authentication verification process. Then, it is checked whether the bio-metric identification with that of the system for a voter is matched. Once it is matched, then the officer electronically activates the ballot unit to accept a new vote. Once the voter enters the vote, the balloting unit displays the vote to the voter and records it in its memory. A "close" command issued from the control unit by the polling booth officer registers the vote and relocks the unit to prevent multiple votes. With the VVPAT system, when a vote is cast, it is recorded in its memory and simultaneously a serial number and vote data are printed out. The printouts placed in the ballot box by the voters are used later to cross-check the voting data stored in the EVMs, in case of discrepancies. The process is repeated when the next voter with a new voter ID arrives before the polling booth officer. If the biometric identification of a voter is not matched in the second stage of verification, then he is identified as a fraudulent voter and is not permitted to cast his vote.

EVMs are equipped with battery power to avoid the use of power cables as the power cables may interfere with the reliable functioning of an EVMs due to a lack of power supply and/or erratic power supply. Hence, the manufacturers of EVMs in India, BEL, Bangalore as well as ECIL, Hyderabad use an ordinary 6-volt alkaline battery to power EVMs. Earlier, each balloting unit of EVM was provided with the symbols and names of 16 contesting candidates and up to a maximum of 4 balloting units with 64 candidate names and the respective party symbols were connected in parallel to the control unit. If the number of contesting candidates exceeds 64, then the conventional ballot paper/box method of polling was used. Later, an EVM is upgraded to a maximum of 384 candidates plus the "None Of The Above" (NOTA) option to record a maximum of 3840 votes. After the completion of the polling on a particular election day, the separated balloting units and the control unit are placed at different locations in highly secured premises.

Both the control unit and balloting unit are equipped with numerous tamper-proof protocols. The hardware programmed at the time of manufacturing of the balloting unit and control unit cannot be reprogrammed. Further, these units are not equipped with any wireless communication components or an internet interface. The balloting unit has an internal real-time clock and a protocol by which it records every input-output event with a timestamp whenever they are connected to a battery pack. Both the balloting unit and control unit cannot work without each other during the voting process.

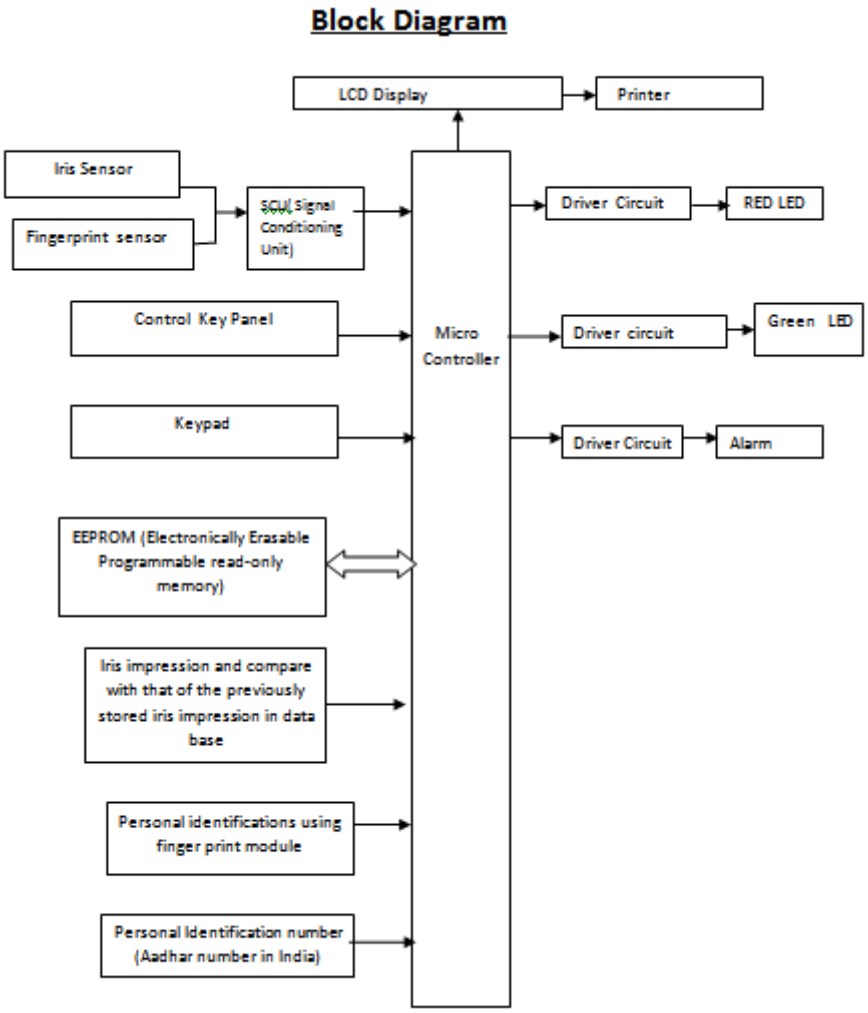

Figure 1: Block Diagram To Describe Voting Process

3. PROCEDURE TO USE THE PROPOSED EVM

The control unit is with the presiding officer or a polling officer and the balloting unit is placed inside the voting compartment. The balloting unit presents the voter with blue buttons (momentary switch) horizontally labelled with the corresponding party symbol and candidate names. The Control Unit, on the other hand, provides the officer-in-charge with a "Ballot" marked button to proceed to the next voter, instead of issuing a ballot paper to them. This activates the ballot unit for a single vote from the next voter in the queue. The voter has to cast his vote by pressing the blue button once on the balloting unit against the candidate and symbol of his choice.

Polling booth officers use the control unit to verify the personal identification number (Adhar card number in India) of a voter as shown in Figure 2 in the first phase of the verification process. Then, it is checked whether the personal identification number matches that in the system for a voter. Once the identification number is matched with that of in the database of the system, the bio-metric (thumb or Irish) identification of the voter is verified in the second phase of authentication as shown in Figure 2. Authenticated identification number of a particular voter handled by a fraudulent voter will get matched with that of in the database of the system in the first phase of the authentication verification process. Hence, it is required to implement biometric verification in the second phase of the authentication verification process. In case the thumb impression is matched with that of in the database, the voter is permitted to cast his vote as shown in Fig.2. Otherwise, an iris impression of a voter is verified for authentication as shown in Fig.2

as thumb impressions are subjected to change by age. If the iris impression of a voter is matched with that of in the database, then the voter is permitted to cast his vote as shown in Figure 2. Otherwise, a voter is identified as a fraudulent voter and is not permitted to move for further identification to cast the vote. Once, the voter is permitted to cast his vote, then the officer electronically activates the ballot unit to accept a new vote. Once the voter enters the vote, the balloting unit displays the vote to the voter, records it in its memory and simultaneously a serial number and vote data are printed out. The printouts placed in the ballot box by the voters are used later to cross-check the voting data stored in the EVMs, in case of discrepancies. A "close" command issued from the control unit by the polling booth officer registers the vote and relocks the unit to prevent multiple votes. The process is repeated when the next voter with a new voter ID arrives before the polling booth officer. If the biometric identification of a voter is not matched in the second stage of verification, then he is identified as a fraudulent voter and is not permitted to cast his vote.

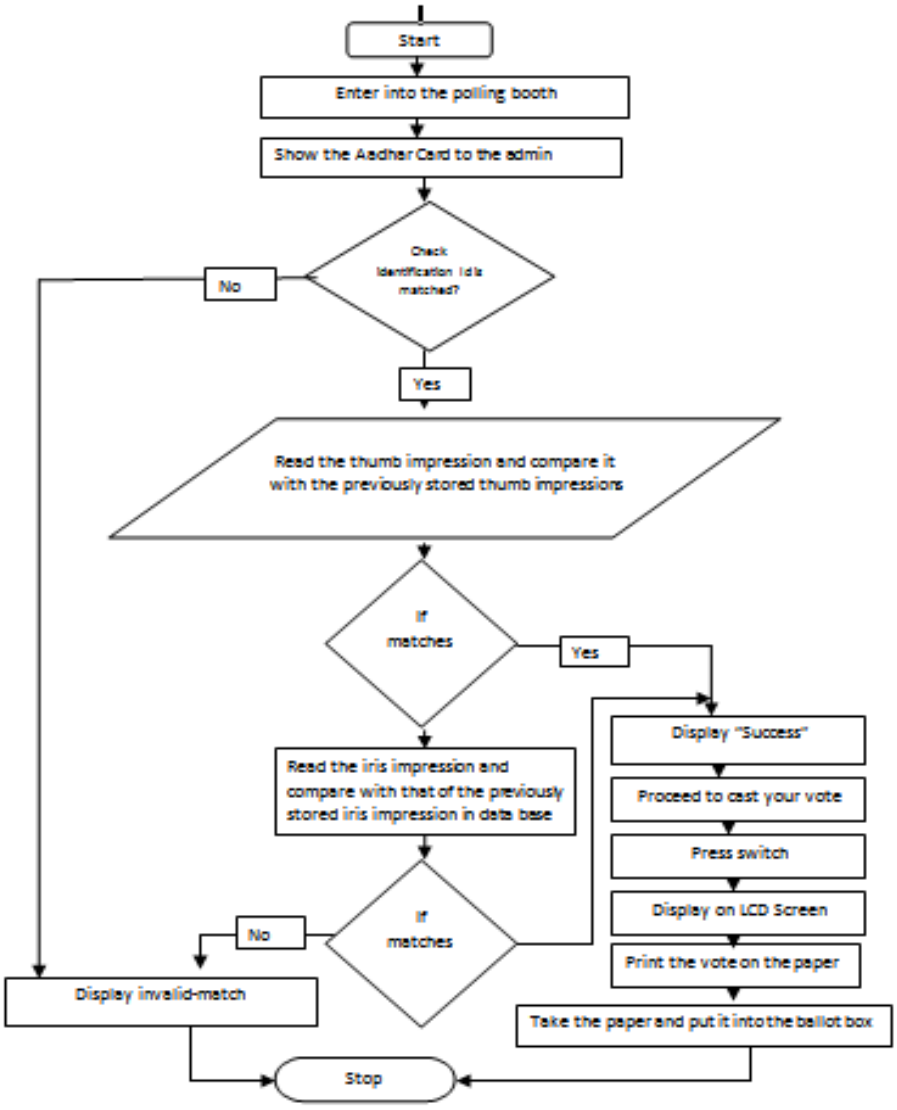

Figure 2 : Flowchart to Describe the Process of Casting Vote Using the Proposed Advanced Version of Evm with Vvpat

As soon as the last voter has voted, the polling officer in charge of the control unit will press the 'Close' button. Thereafter, the EVM will not accept any votes. Further, after the close of the poll, the balloting unit is disconnected from the control unit to keep them separate. Votes can be recorded only through the balloting unit. Again, the presiding officer, at the close of the poll, will hand over to each polling agent present an account of the votes recorded. At the time of counting of votes, the total will be tallied with this account and if there is any discrepancy, this will be pointed out by the counting agents. During the counting of votes, the results are displayed by pressing the 'Result' button. There are two safeguards to prevent the 'Result' button from being pressed before the counting of votes officially begins. (a) This button cannot be pressed till the 'Close' button is pressed by the polling officer-in-charge at the end of the voting process in the polling booth. (b) This button is hidden and sealed; this can be broken only at the counting center in the presence of a designated office.

Even though the initial investment was heavy, it has since been expected to save costs of production and printing of crores of ballot papers, their transportation and storage, substantial reduction in the counting staff and the remuneration paid to them. For each national election, it is estimated that about 10,000 tons of ballot paper are saved. EVMs are easier to transport compared to ballot boxes as they are lighter, more portable, and come with polypropylene carrying cases. Vote counting is also faster. In places where illiteracy is a factor, illiterate people find EVMs easier than the ballot paper system. Bogus voting is greatly reduced as the vote is recorded only once. The unit can store the result in its memory before it is erased manually. The battery is required only to activate the EVMs at the time of polling and counting and as soon as the polling is over, the battery can be switched off. The shelf life of Indian EVMs is estimated at 15 years (The Indian Express. 25 October 2015. Retrieved 10 January 2019).

4. CONCLUSION

Electronic voting machine (EVM) has embedded hardware and software that enables only a particular control unit to work with a particular voting unit to avoid tampering. The M3 version of EVM with VVPAT capability consists of two units, such as the control unit and the balloting unit. A polling booth officer makes use of a control unit to confirm the identification of a voter and to activate the balloting unit electronically to enter a new voter. A voter makes use of a balloting unit to get display the vote cast. The balloting unit is used to record the vote cast and transfer it to the print unit to get the print to place it in a box for its cross-verification, in case of a dispute. Then, the polling booth officer makes use of the control unit to issue a close command to register the vote cast and relock the unit, to avoid multiple casting of votes. A fraudulent voter makes use of the existing system to cast multiple votes with various voter identification numbers which lead to losing confidence in a democratic system.

The proposed electronic voting system is included features to read and match personal identification numbers (Aadhar numbers in India) and biometric measures of the voter with that of the database of the system, to identify fake voters and avoid them from casting votes. Polling booth officers use the control unit to verify the personal identification number (Aadhar card number in India) of a voter in the first phase of the verification process. Once the identification number is matched with that of the database of the system, the bio-metric (thumb or Irish) identification of the voter is verified in the second stage of authentication. Personal identification numbers of other voters handled by fraudulent voters will get matched with that in the database of the system in the first phase of the authentication verification process. Hence, it is required to implement biometric verification in the second phase of the authentication verification process. In case the thumb impression is matched with that of in the database, the voter is permitted to cast his vote. Otherwise, an iris impression of a voter is verified for authentication as thumb impressions are subjected to change by age. If the iris impression of a voter is matched with that of in the database, then the voter is permitted to cast his vote. Otherwise, a voter is identified as a fraudulent or bogus voter and he is not permitted to move for further identification to cast the vote.

The proposed system of electronic voting machines can identify fraudulent voters to avoid them to cast a vote, and to increase confidence in a democratic system. It reduces the cost involved in producing, printing, transporting, and storing ballot papers. It also reduces the number of counting staff and their remuneration. It is quite easy to transport EVMs compared to ballot boxes containing paper ballots. Accurate and early electoral results can be published due to the fast counting of votes with EVMs. Invalid votes can be reduced to a large extent as illiterate people also find the EVMs easier than the ballot paper system to cast their votes. Bogus or fraudulent voters are avoided to cast votes as only one vote is recorded for each personal identification number and bio-metric impression. It consumes less electricity as the battery is required only to activate the EVMs during polling and counting.

5. SCOPE FOR FUTURE GENERATION VOTING SYSTEM

Blockchain-enabled voting (BEV) systems were proposed as the next generation of modern electronic voting systems because the immutable feature of the blockchain has made it a decentralized distributed ballot box (Zhang et al., 2020). With BEV, individual votes will be publicly available, while voters are masked behind an encrypted key. It offers greater privacy and security than traditional ballot boxes and could reduce voter suppression. Bad actors can't identify voters and therefore can't target them(Hall, 2018). The blockchain's audit trail ensures that no vote has been changed or removed and that no fraudulent and illegitimate votes have been added (Sandre, 2018). Blockchains enable the creation of tamper-proof audit trails for voting (Nir et al., 2018). Black chain Enabled e-Voting (BEV) employs an encrypted key and tamperproof personal IDs. Eligible voters cast a ballot anonymously using a computer or smartphone. To address voter tampering, blockchains generate cryptographically secure voting records. Votes are recorded accurately, permanently, securely, and transparently (Prico, 2018). So, no one can modify or manipulate votes (Lear, 2017). Ten different official documents including driver's licenses, state IDs, and passports may be accepted to verify voter identity (Kuebler, 2018). This online-voting process might be complicated for some voters. It's not easy to know whether a vote was cast as intended or whether it was counted as cast (Lohrmann, 2017). As we already noted, blockchain results are publicly auditable.

Blockchains' complexity might hinder mainstream public acceptability of BEV(Boucher, 2016). Broadband access and digital user skills are also concerns. BEV will shift power away from central actors such as electoral authorities and government agencies (Boucher, 2016). Thus, the technology is likely to face resistance from political leaders who benefit from the status quo (Ooijen, 2017). Also, there exists a major threat to a voter in casting his vote as the loyalists of political parties can interfere in the privacy of the voter to hijack his voting credentials. This technology may be adapted and provided with measures to protect the voting credentials of a voter to enhance confidence in democracy.

REFERENCES

Verma, A. (2005). Policing Elections in India. *India Review*. **4** (3–4): 354–376.

Madhavan S. (2019). *India's electoral democracy: How EVMs curb electoral fraud*. Brookings Institution, Washington DC.

Debnath, S., Kapoor, M. & Ravi, S. (2017). The Impact of Electronic Voting Machines on Electoral Frauds, Democracy, and Development: 1–59. SSRN 3041197.

The Times of India. 20 January 2012. Archived from the original on 22 January 2012. Retrieved 20 January 2012.

Daily News and Analysis. 27 April 2014. Retrieved 10 January 2019.

The Times of India. 6 March 2017**.** Election Commission plans to replace all pre-2006 EVMs with advanced M3 machines.

Vishesh S. & Girish T. (2016). An Analysis of Electronic Voting Machine for its Effectiveness. *International Journal of Computing Experiments*. 1 (1), 8–12.

ECI Voting Equipment's. *Election Commission of India*. Retrieved 10 January 2019.

A look inside the electronic voting machine, The Hindu (March 10, 2019).

Vishesh S. & Girish T. (2016). "An Analysis of Electronic Voting Machine for its Effectiveness". *International Journal of Computing Experiments*. 1 (1), 8–12.

Lok Sabha elections 2019: Check FAQs related to EVMS, India Today March 15, 2019

Shelf-life of 50% EVMs ending, have to buy 14 lakh for 2019: EC. *The Indian Express*. 25 October 2015. Retrieved 10 January 2019.

Lok Sabha elections 2019: Check FAQs related to EVMS, *India Today* (March 15, 2019).

Pallava, B. (2019). Zero Complaints Came Up After Lok Sabha Polls, Claims Expert Behind EVMs. March 28.

Daramola, O., & Thebus, D. (2020). Architecture-Centric Evaluation of Blockchain-Based Smart Contract E-Voting for National Elections. *Informatics*, 7 (16).

Zhang, S., Wang, L., & Xiong, H. (2020). Chaintegrity: Blockchain-enabled large-scale e-voting system with robustness and universal verifiability. *Int. J. Inf. Secur*., 19, 323–341.

Sandre, A. (2018). Blockchain for Voting and Elections. Hackernoon, 14 Jan.; https://hackernoon.com/blockchain-for-voting-and-elections-9888f3c8bf72.

Kshetri, N., & Voas, J. (2018). Blockchain-Enabled E-voting. *IEEE Software* 35(4), 95-99

Prico, G. (2018) Sierra Leone Pilots Blockchain-Based Voting for Political Elections. 22 Mar.; https://www.nasdaq.com/article/sierra-leone-pilots-blockchain-based-voting-for-political-elections-cm938309.

Leary, K. (2017). Blockchain Might Be About to Change the Way We Vote. *World Economic Forum*, 13 Sept.; https://www.weforum.org/agenda/2017/09/blockchain-could-be-about-to-change-how-you-vote,2017.

Kuebler, E. (2018). Making Voting, Elections Both Secure and Accessible with Blockchain Technology. *Bitcoin Magazine*, 11 Jan; https://bitcoinmagazine.com/articles/making-voting-elections-both-secure-and-accessible-blockchain-technology.

Lohrmann, D. (2017). Can Blockchain Technology Secure Your Vote? *Government Technology*, 29 Apr.; http://www.govtech.com/blogs/lohrmann-on-cybersecurity/can-blockchain-technology-secure-your-vote.html.

Boucher, P. (2016). What If Blockchain Technology Revolutionised Voting? *European Parliamentary ResearchService*,http://www.europarl.europa.eu/thinktank/en/document.html?reference5EPRS_ATA(2016)581918.

van Ooijen, C. (2017). How Blockchain Can Change Voting: The Colombian Peace Plebiscite. *Forum Network*, 20 Dec.; https://www.oecd-forum.org/users/76644-charlotte-van-ooijen/posts/28703-how-blockchain-can-change-voting-the-colombian-peace-plebiscite.

Hall, J. (2018). Can Blockchain Technology Solve Voting Issues? *Bitcoin Magazine*, 7 Mar.; https://www.nasdaq.com/article/can-blockchain-technology-solve-voting-issues-cm931347.

Vinayachandra, C., Geetha. P. K., Rajeshwari M, & Krishna P. K. (2020). Role of Technology in the Development of Smart and Secure Public Voting Systems – a Review of Literatures. *International Journal of Management, Technology, and Social Sciences.* June 30.