Available online at www.ijpe-online.com

International Journal of Performability Engineering

vol. 15, no. 10, October 2019, pp. 2570-2577
DOI: 10.23940/ijpe.19.10.p2.25702577

Secure Electronic Voting Machine using Multi-Modal Biometric Authentication System, Data Encryption, and Firewall

Jasdev Bhatti*, Satvik Chachra, Ansh Walia, and Abhishek Vishal

Chitkara University Institute of Engineering and Technology, Chitkara University, Punjab, 140401, India

Abstract

Electronic voting machines have replaced paper ballot systems, which were being used in early Indian elections. But, with the advancement of technology, a series of security issues have been raised regarding the present voting system, such as EVM tampering in order to register fraudulent votes. The proposed system attempts to solve the problem of bogus voting by introducing a multi-modal biometric authentication system. It makes the voting system more secure by using data encryption and firewalls to protect the voter database. It increases accessibility by allowing voters to cast their vote in the elections of their respective constituency from any polling booth across the country. It also increases transparency in the election process by notifying voters on successful casting of their vote. This paper proposes a Biometric Voting Machine with a robust system architecture that is able to withstand malicious attacks and fraudulent behaviours.

Keywords: biometric voting machine; electronic voting machine; data encryption; two-step authentication system; electronic voting; secure system; ballot; polling booth; OTP verification; SMS notification

(Submitted on August 26, 2019; Revised on October 15, 2019; Accepted on October 30, 2019)

1. Introduction

Free and fair elections are the bedrock of the world's largest democracy, and the Election Commission of India is the constitutional authority responsible for ensuring this. ECI does so by administering the election process and safeguarding the democratic values stated in the Constitution of India. After the Universal Adult Suffrage Movement, every Indian citizen over the age of 18 years who had a valid ID, became eligible to vote. Elections gave citizens a way to voice their opinion and bring a constructive change in the way the system worked. Thus, each citizen became a catalyst of change.

Each vote influences how a district, city or a state is governed. Since each vote has the power to influence how the whole nation would be run, each vote is significant and each vote counts. Therefore, upholding the integrity of the election process is of utmost importance. As the electoral system involved, ECI has faced many challenges. One of the major challenges was 'Bogus Voting'. In 1988, to counter this problem, voters' fingers were marked with indelible ink. Over time, the voting system evolved. It began with a ballot box per contestant, which was then substituted by a single ballot box. Then, with the advancement of technology, electronic voting machines were brought into use.

In the Pioneer, 05 June 2013, the Electoral Office of Delhi admitted many dubious/bogus voters listed on the electoral rolls and decided to remove around 12 lakh (nearly 10 percent) of such voters. On 14 December 2017, the New Indian Express reported that 45,830 bogus voters pertaining to the RK Nagar Assembly Constituency were found. The latest claim was made by Congress, where around 9 lakh bogus voters may have snuck into the city's electoral rolls, which was reported by The Times of India on the 16th of January 2019. Also, it was reported in the Hindustan Times on the 9th of August 2013 that Patna's election authorities detected 76 lakh 'ghost' voters on the electoral rolls of 243 assembly constituencies in Bihar.

These news reports most certainly justify that the present voting system has its limitations and drawbacks. The present system needs some major reforms to deal with its shortcomings. The conventional system, due to its manual nature,

* Corresponding author.
E-mail address: jasdev.bhatti@chitkara.edu.in

involves a great deal of human error, be it in the process of registering a citizen as a voter or verifying a voter at the Election Booth. Our proposed system solves that by utilizing the latest technology to our advantage and making the whole process digital. In 2004, research on modernising the voting system had been initiated by some researchers and industries. Kohno et al [1] and Bannet et al [2] proposed an analysis of an electronic voting system with Hack-a-vote security issues in 2004. Wolchok [3] and Kumar [4] extensively analysed the existing electronic voting machine used in elections in India and found major security issues with the current voting system. In 2014, Thakur [5] proposed the transformation with the voting paradigm, studying the shift from inline through online to mobile voting. Pomares [6] discussed in his paper about voting experience and trust in the first full E-election, which was held in Argentina.

In 2016, Das [7] studied the three tiers of the secured state-of-the-art EVM design using pragmatic fingerprint detection annexed with an NFC enabled voter-ID card. Usmani [8] proposed a technique in 2017 favouring the security of voting machines. In 2017, Rezwan [9] came up with the new idea of introducing a simple user-friendly offline voting system based on biometrics. Bhuvanpriya [10] proposed a smart voting system with the key point being generation of voter ID at the polling booth itself if the citizen had an AADHAAR Card and was over 18 years of age. Illakiya [11] devised a ready to use multi-purpose online voting platform for the government with the significant feature being the use of encryption to protect election data. Lakshmi [12] discussed in his paper about a secure and transparent voting system using biometrics in 2018. Roy [13] discussed the American voting system and its future. In 2018, Patil [14] proposed an E-smart voting system with secure data identification using cryptography.

Thus, all previous works as discussed had only focused on the security aspect of the voting machine, whereas this paper proposes a system that focuses on both security and transparency aspects of the voting machine while making sure it is compatible with today's digital world. This system overcomes the challenges faced by the existing system in:

- Authentication
- Casting
- Counting
- Recounting

It works on restoring trust of voters in the voting machines and accomplishes it by showcasing properties, namely:

- **Eligibility:** Only biometrically authenticated voters will be able to cast their vote and can vote once only.
- **Accuracy:** The vote can't be altered as the data is encrypted. Each vote will be counted in the final count and tallied through each database ensuring no bogus vote is casted and no vote is missed.
- **Secrecy:** No vote can be linked back to the voter as the AES encryption key changes during the transition from the authentication system to the voting interface.
- **Convenience:** Voters can cast their vote (once only) from any polling booth since location specific databases get updated during the authentication of the voter.
- **User Friendly and Accessibility:** The system is designed to assist differently abled people to ensure a good and hassle-free user-experience by including features like a screen reader.

Thus, by means of this paper, we are proposing a secure electronic voting machine that uses a multi-modal biometric authentication system, data encryption and firewall.

2. Present Voting System

The present voting system is not "infallible" or "tamper proof" as claimed by the ECI. There are three classes of vulnerabilities, namely:

- Converting genuine votes to bogus votes by replacing original components with duplicate components to display a different result (requires physical access).
- Recording bogus votes by tampering with the memory storage of the unit (requires physical access).
- Outsider attacks by modifying the source code burnt into the chip.

2.1. Converting Genuine Votes to Bogus Votes by Replacing Original Components with Duplicate Components to Display a Different Result

The contemporary EVM is not a secure device because simple candle-wax and string are used for sealing it. Furthermore, it

basically has paper-stickers and over screws to collect any evidence of tampering [3]. The biggest worry in this system is that one can make a duplicate display board that can consist of a micro-controller and a bluetooth-radio module hidden between the CPU and the display where the microcontroller would help in displaying a different election outcome and the bluetooth-radio module would help in choosing the winning candidate and the winning fraction of bogus votes through a mobile phone.

2.2. Recording Bogus Votes by Tampering with the Memory Storage Unit

One can tamper with the two EEPROM memory chips whose electrical interface I2C makes it easy to communicate with. Also, the software used is not encrypted or protected by any kind of cryptography for that matter. It just stores a 1-byte record for each vote that is casted. It can be accessed easily as it is indirectly a matter of public record. This class is an electronic form of bogus voting, as it bypasses the rate-limiting condition of the software [3]. By just rewriting the array of bytes with respect to candidates, one can change the election result. All it takes is a small clip-like device with a knob on its top, which by rotating, one can select the preferred candidate.

2.3. Outsider Attacks by Modifying the Source Code Burnt into the Chip

The source code written by BEL (Bharat Electronics Limited) and ECIL (Electronics Corporation of India Limited) is burnt into the chips, which are imported from Japan and USA. This means we have to believe that no foreign government would tamper with the chips to affect the election result and consequently, with the electoral system of India. Thus, EVMs are tamper-able and vulnerable to fraudulences.

3. Proposed System

In this paper, we have designed a system involving a machine with a voting security mechanism. The machine is secured from any physical damages by being sealed. It is also locked using a USB security key, which we named "SANGRAKSHAN KEY". This provides an extra layer of security to the machine. After using the security key, an OTP will be sent to the Election Official of that booth for verification. Once verified, the official needs to press the Ballot Button. Once it is pressed, the session begins. The initiating process of the voting machine is designed as Figure 1.

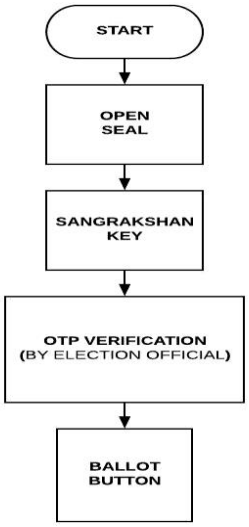

Figure 1. Initiating the voting machine

The proposed system uses a biometric authentication system (shown in Figure 2) and is based on three pillars:

- Fingerprint Scanning
- Iris Scanning
- Facial Recognition

It uses the Aadhaar Database at the backend to uniquely identify an individual and verify him/her as a registered voter.

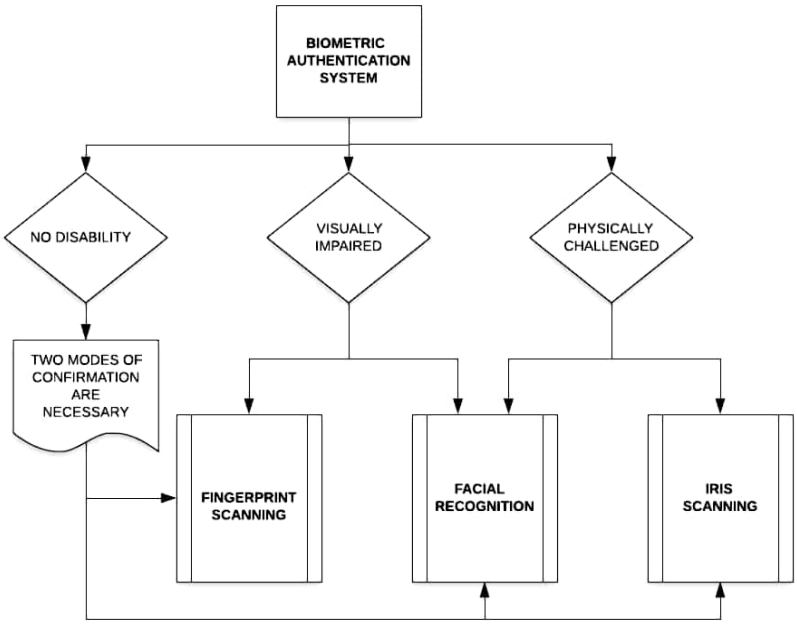

Figure 2. Multi-mode authentication system

This system can be broadly divided into 3 phases:

- Authentication and Verification Phase
- Voting Phase
- Counting and Tallying Phase

4. Authentication and Verification Phase

As for any voting system, the most important phase is its authentication and verification phase, which the present voting system is lacking. So, the parameters involved in this phase are divided into three different stages for verification:

- Database Check
- AADHAAR Card Number Check
- Age limit and Eligibility Check

4.1. Database Check

In every data centric system, the flow and storage of data is very important, and it is crucial to the success of our proposed system. There are 4 components of the database used in the proposed system-architecture:

- National Database
- State Database
- District Database
- Local Database

The hierarchy of the database in our system is described in Figure 3.

In this phase, a user's fingerprint is scanned twice/thrice using a fingerprint scanner. Then, this captured template is matched on one–to–many bases at the local database server. If the fingerprint data is not found in the local database, it is searched for in the cached copies in the state database. If not found in the state database, it is searched for in the cached copies of the national database. If the biometric data of the user is not found in any of the databases, a buzzer beeps to alert the polling booth officer and an exit screen is displayed on the machine and the machine gets locked. It can be unlocked only by the election official present at the polling booth as the machine is secured using the USB security key i.e.

Sangrakshan Key, which is present only with the election official. After that, a one-time password is generated and sent to the election official's mobile number. When the OTP verification process is concluded, the machine is unlocked.

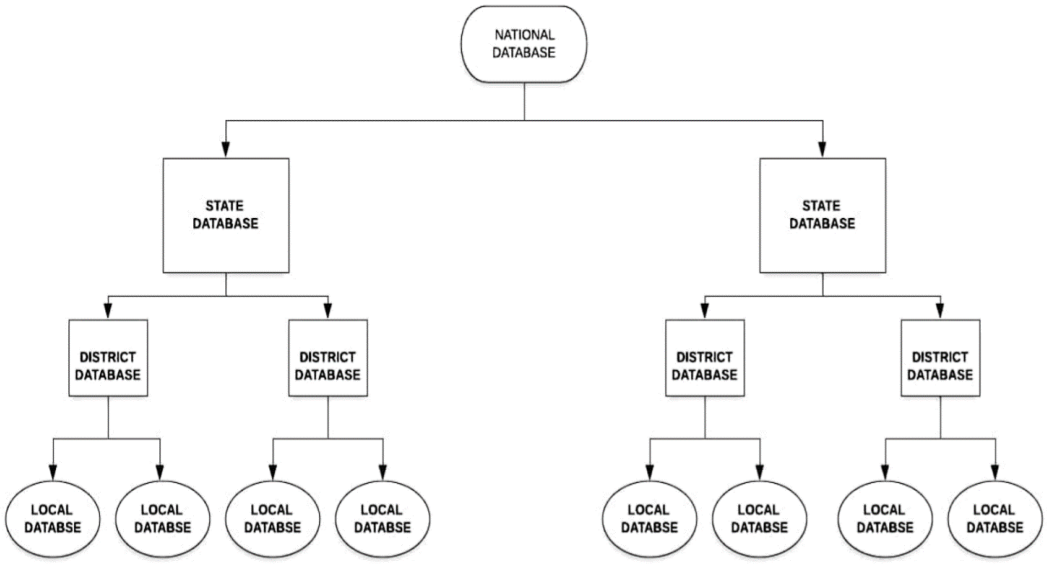

Figure 3. Database hierarchy

The databases are secured by a combination of 2 types of firewall:

- Host – Based Firewall
- Network – Based Firewall

The host-based firewall will be installed on each server to control incoming and outgoing traffic, while the network-based firewall will be built into the infrastructure of the cloud. An anti-malware software will be installed in conjunction with the firewall. The detection and prevention systems operating on the network-based firewall will keep a check on suspicious traffic generated by a Trojan as it crosses the network barrier and will prevent the attack while raising an alert. Even if an attacker can circumvent the network barrier, he will have to try and breach the host-based firewall as well to cause any form of damage.

To protect data both in transit and at rest, the network perimeter will be continuously managed and controlled. Voters will not only be given controlled access to the machine, but also the activity log will be audited by the completely autonomous voting machine itself every few seconds to keep track of any unusual activity. The complete query response system to authenticate a voter in the process of database check is described in Figure 4.

4.2. AADHAAR Card Number Check

After the database check is complete, it is of paramount importance to verify the voter's identity through the Aadhaar card number check. So, under this process, if the biometric data is found in any of the database, that particular database starts getting updated. When the Aadhaar Card number of the voter is found to exist in the database, an age limit check is also imposed to check the eligibility of the user to cast a vote.

4.3. Age Limit and Eligibility Check

Under the AADHAAR card verification checking process as discussed above, if the user is found to be not over 18 years of age, a buzzer goes off and an exit screen is displayed on the machine. If the user is found to be over 18, a voter-list check is imposed.

Thus, for any voting system the above three validation processes are best to overcome the issue of bogus voting as they are unsurpassable.

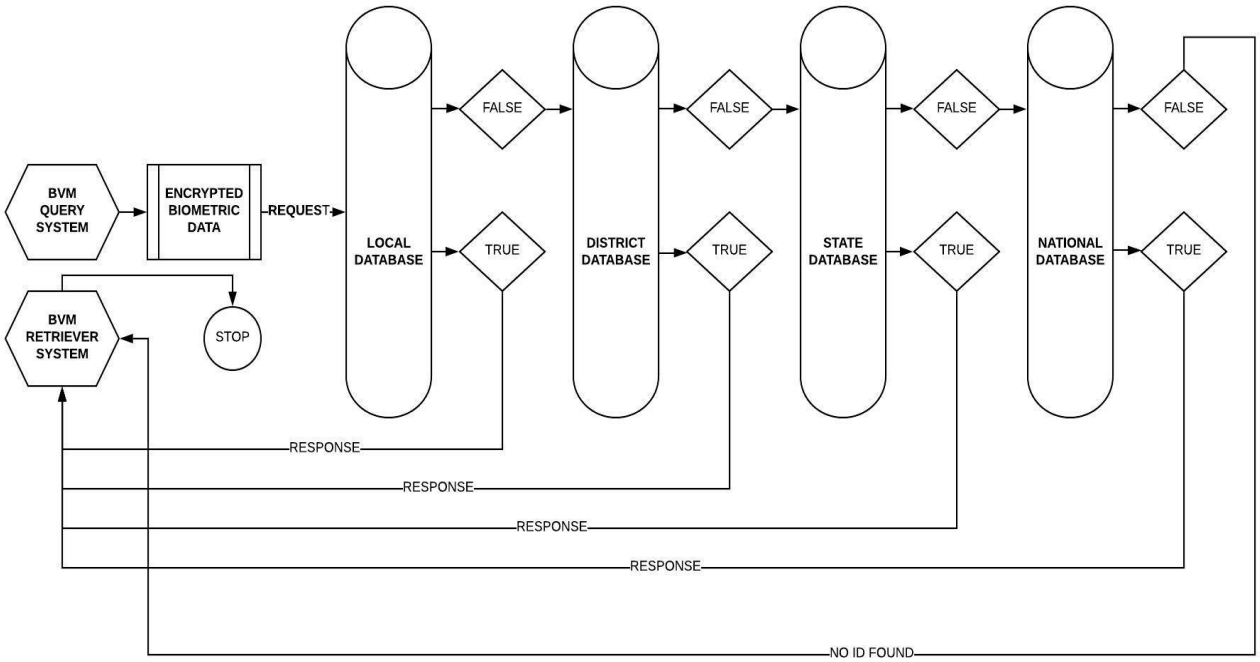

Figure 4. Query-response system to authenticate voters

5. Voter-List Check

There are 4 types of elections that are being conducted in India, including the General Elections (Lok Sabha), State Assembly Elections, Rajya Sabha Elections (Upper House) and Local Body Elections. So, in such elections, if the user is found on the voter list of the local or state database, the respective databases starts getting updated, allowing the voter to cast his/her vote from any polling booth in the country at his/her own convenience. If they are not found on the database, a notification is displayed asking the voter to fill the Form-6 to register themselves in the voter list. All of this logging data is protected by AES encryption.

The query-response system for checking voter-list is shown in Figure 5.

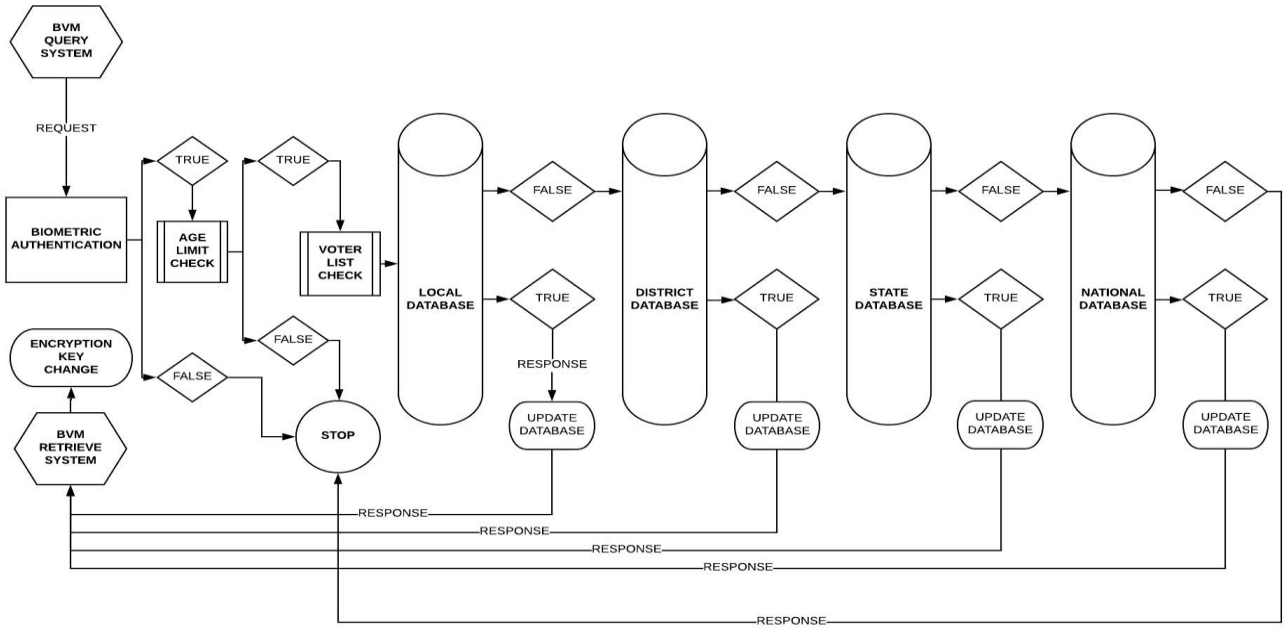

Figure 5. Query-response system for voter-list check to determine constituency of the voter

After the authentication and verification phase is completed, the user is recognised as a voter. A simple and user–friendly voting interface is displayed on the screen with candidate names and party symbols next to each other. The voter must choose a candidate to cast his/her vote. After selecting the candidate and the respective party, the voter clicks on the vote button. A pop-up message is displayed asking the voter to confirm his/her preferred choice. If the voter does not confirm the message, he/she can make a change in his/her choice.

Once the vote has been casted, the value of the voter flag gets set to true or 1, and a serial ID is generated simultaneously. This is done to prevent the voter from casting a vote more than once. The serial ID generated gets stored in the state and the national databases. This voting interface is open for a specific duration of time. After the vote is casted successfully, an exit screen is displayed. To add another layer of security, all this voting data is protected by a different AES encryption key. After the voting process has ended, the voter will receive the serial ID of his vote in form of a confirmation SMS. This special confirmation SMS is used to increase the transparency of the voting process. The complete voting phase is described in Figure 6.

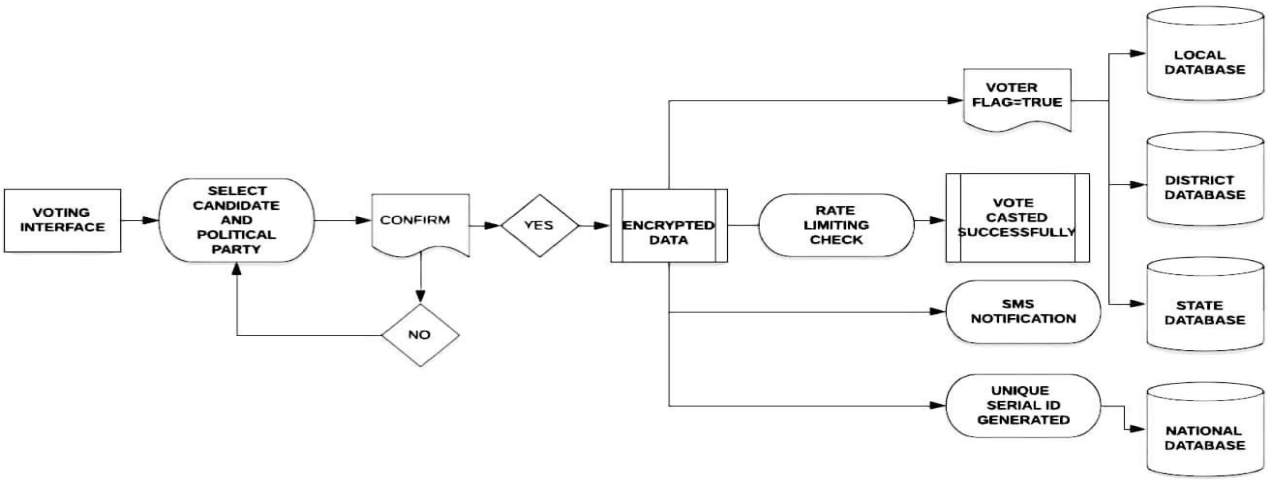

Figure 6. Voting phase

6. Counting and Tallying Phase

As in any system related to data collection, the most important and difficult task is to count and tally the data without any data loss or information breach. Therefore, the major advantage through our paper is that we introduce a new technique for counting and tallying the voting record in a safe and secure manner. In our system, the counting and tallying voting phase involves:

- Local Database Update
- State Database Update
- National Database Update
- SMS Notification on registered mobile number of the voter

Counting the votes is done across all the databases. Then, the tallying process begins. If any bogus votes are found, they are eliminated automatically using the difference in serial IDs generated and updates in the local database. Voting data is only present at the local and state database. At the national database, there are 4 types of encrypted data as mentioned below:

- Logging data
- Voting Data
- Voter Data Analysis
- Logging Data Analysis

Also, whether the voter has voted or not will be stored in the form of true or false form for analysis in the form of bar graphs and pi-charts to see voter participation per constituency. In the proposed system, a rate-limiting function is also included where no more than 3 votes can be cast in a minute to neutralize physical challenges such as booth-capturing.

7. Conclusions

This paper proposes a new voting system that provides five major specific advantages over the existing voting machine:

- Transparency
- Accessibility
- Security
- Speed
- Accuracy

It restores the integrity of the electoral process and makes the voting system more reliable by comprising unique features to overcome different challenges faced by the classical system. It has a rate-limiting feature that sets a limit of the number of votes that can be casted per minute to solve the issue of booth capturing. It works on making the system more transparent by sending an SMS notification to the voter on his/her registered mobile number. It uses a multi-modal biometric authentication system, voting data encryption, and a firewall system to prevent any malicious attacks on the voter database, thus making it more secure, transparent and accurate. A unique serial ID is generated for every successful vote that is cast, and they are stored in the national database, making the process of counting, tallying, auditing, and in special circumstances, recounting votes, faster and easier. Thus, the proposed system discussed in this paper will be beneficial by providing a better and safe electronic voting machine to users.

References

1. T. Kohno, A. Stubblefield, A. D. Rubin, and D. S. Wallach, "Analysis of an Electronic Voting System," in *Proceedings of IEEE Symposium on Security and Privacy*, pp. 27-40, 2004
2. J. Bannet, D. W. Price, A. Rudys, J. Singer, and D.S. Wallach, "Hack-a-Vote: Security Issues with Electronic Voting Systems," *IEEE Security and Privacy*, Vol. 2, No. 1, pp. 32-37, 2004
3. S. Wolchok, E. Wustrow, J. A. Halderman, H. K. Prasad, A. Kankipati, S. K. Sakhamuri, et al., "Security Analysis of India's Electronic Voting Machines," in *Proceedings of 17th ACM Conference on Computer and Communications Security* (*CCS*), pp. 1-14, 2010
4. D. A. Kumar and T. U. S. Begum, "Electronic Voting Machine — A Review," in *Proceedings of International Conference on Pattern Recognition, Informatics and Medical Engineering* (*PRIME-2012*), pp. 41-48, 2012
5. S. Thakur, O. O. Olugbara, R. Millham, H. W. Wesso, and M. Sharif, "Transforming Voting Paradigm — The Shift from Inline through Online to Mobile Voting," in *Proceedings of 2014 IEEE 6th International Conference on Adaptive Science and Technology* (*ICAST*), pp. 1-7, 2014
6. J. Pomares, I. Levin, R. M. Alvarez, G. L. Mirau, and T. Ovejero, "From Piloting to Roll-out: Voting Experience and Trust in the First Full E-Election in Argentina," in *Proceedings of 2014 6th International Conference on Electronic Voting*: *Verifying the Vote* (*EVOTE*), pp. 1-10, 2014
7. A. Das, M. P. Dutta, and S. Banerjee, "VOT-EL: Three Tier Secured State-of-The-Art EVM Design using Pragmatic Fingerprint Detection Annexed with NFC Enabled Voter-ID Card," in *Proceedings of 2016 International Conference on Emerging Trends in Engineering, Technology and Science* (*ICETETS*), pp. 1-6, 2016
8. Z. A. Usmani, K. Patanwala, M. Panigrahi, and A. Nai, "Multi-Purpose Platform Independent Online Voting System," in *Proceedings of 2017 International Conference on Innovations in Information, Embedded and Communication Systems* (*ICIIECS*), pp. 1-5, 2017
9. R. Rezwan, H. Ahmed, M. R. N. Biplob, S. M. Shuvo, and Md. A. Rahman, "Biometrically Secured Electronic Voting Machine," in *Proceedings of 2017 IEEE Region 10 Humanitarian Technology Conference*, pp. 510-512, 2017
10. R. Bhuvanapriya, R. S. Banu, P. Sivapriya, and V. K. G. Kalaiselvi, "Smart Voting," in *Proceedings of 2017 2nd International Conference on Computing and Communications Technologies* (*ICCCT*), pp. 143-147, 2017
11. T. Illakiya, S. Karthikeyan, U. M. Velayutham, and N. R. Devan, "E-Voting System using Biometric Testament and Cloud Storage," in *Proceedings of 2017 Third International Conference on Science Technology Engineering and Management* (*ICONSTEM*), pp. 336-341, 2017
12. Ch. J. Lakshmi and S. Kalpana, "Secured and Transparent Voting System using Biometrics," in *Proceedings of 2018 2nd International Conference on Inventive Systems and Control* (*ICISC*), pp. 343-350, 2018
13. L. R. CarrIII, A. Newtson, and J. Joshi, "Towards Modernising the Future of American Voting," in *Proceedings of 2018 IEEE 4th International Conference on Collaboration and Internet Computing* (*CIC*), pp. 130-135, 2018
14. S. Patil, A. Bansal, U. Raina, V. Pujari, and R. Kumar, "E-Smart Voting System with Secure Data Identification using Cryptography," in *Proceedings of 2018 3rd International Conference for Convergence in Technology* (*I2CT*), pp. 1-4, 2018