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

Jasdev Bhattia\*, Satvik Chachrab, Ansh Waliac, Abhishek Vishald

*a, b,c,d Chitkara University Institute of Engineering and Technology, Chitkara University, Punjab, India*

Abstract

Electronic Voting Machines have replaced the paper ballot system which was earlier being used in 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 multi-modal biometric authentication system. It makes the voting system more secure by using data – encryption and firewalls to protect voter database. It increases accessibility, by allowing voters to cast 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 vote. This paper proposes a Biometric Voting Machine with a robust system architecture, which is able 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 12, 2019; Accepted on October 19, 2019)

© 2019 Totem Publisher, Inc. All rights reserved.

1. Introduction

Free and fair elections are the bedrock of world’s largest democracy -India and the Election Commission of India, is the constitutional authority responsible for ensuring the same. 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 proof, became eligible to vote in the elections. Elections gave citizens a way to voice their opinion and bring a constructive change in the way 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 becomes significant and each vote counts. Therefore, upholding integrity of the election process is of utmost importance. As the electoral system involved, ECI 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 from a ballot box per contestant, which was then substituted by a single ballot box, and then with the advancement in technology, Electronic Voting Machines were brought into the sphere.

In the Pioneer, 05 June 2013, Electoral Office of Delhi admitted many dubious/bogus voters listed in electoral rolls and decided to remove around 12 lakh (nearly 10 percent) such voters from the electoral rolls. On 14 December 2017, the New Indian Express reported that 45,830 bogus voters, in electoral rolls pertaining to RK Nagar Assembly Constituency were found. The latest claim was made by Congress, which around 9 lakh bogus voters may have sneaked 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, 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 and our proposed system solves that by utilizing latest technology to our advantage and making the whole process digital. In 2004, the research on modernising the voting system had been initiated by some researchers and industries. Kohno et al [1] and Bannet et al [2] had proposed an analysis of an electronic voting system with Hack-a-vote security issues in 2004. Wolchok [3] and Kumar [4] analysed the existing electronic voting machine used in elections in India, extensively and found major security issues with the current voting system. In 2014, Thakur [5] had proposed the transformation with voting paradigm studying the shift from inline through online to mobile voting. Pomares [6] had discussed in his paper about voting experience and trust in the first full E-election which was held in Argentina. In 2016, Das [7] had studied three tiers secured state-of-the-art EVM design using pragmatic fingerprint detection annexed with NFC enabled voter-ID card. Usmani [8] had proposed the technique in 2017 favouring the security of voting machines. In 2017, Rezwan [9] had comed with 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 has an AADHAAR Card and is over 18 years of age. Illakiya [11] devised a ready to use multi-purpose online voting platform for the government with a significant feature being use of encryption to protect election data. Lakshmi [12] had discussed in his paper about secured and transparent voting system using biometrics in 2018. Roy [13] had discussed about modernising structure American voting system and its future. In 2018, Patil [14] proposed E-smart voting system with secure data identification using cryptography in his paper. Thus, all previous works as discussed had only focused on security aspect of the voting machine. But by this paper we have proposed a system that focuses on both security and transparency aspects of it which is compatible with today digitalize world. This system overcomes the challenges faced by the existing system in:

* Authentication
* Casting
* Counting
* Recounting

of the votes as well as the above-mentioned systems. 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 vote once only.
* **Accuracy:** 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 transition from authentication system to voting interface.
* **Convenience:** Voters can cast their vote (once only) from any polling booth, since location specific databases get updated during authentication of the voter.
* **User Friendly and Accessibility:** System is designed to assist the especially abled people to have a good and successful user-experience by including features like a screen reader.

Thus, by mean of this paper, we tried to discuss a new voting system involving a secure and digitalize an electronic voting machine by using multi-modal biometric authentication system, data encryption and firewall

1. Present Voting system

Thepresent 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 unit (Requires Physical Access).
* Outsider attacks by modifying the source code burnt into the chip.
  1. *Converting genuine votes to bogus votes by replacing original components with duplicate components to display a different result*

The EVM system or machine using in present voting is not a secure device because simple candle-wax and string are used for sealing it and it basically has paper-stickers, over screws, to collect any evidence of tampering [3]. The biggest problem in this system is that one can make a duplicate display board which 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, while the Bluetooth-radio module would help in choosing the winning candidate and the winning fraction of bogus votes through a mobile phone.

* 1. *Recording bogus votes by tampering with the memory storage of unit*

One can tamper with the two EEPROM memory chips whose electrical interface I2C is making 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 and that too in an order, which 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 – limit condition of the software [3]. By just rewriting the array of bytes with respect to candidates, one can change the election result and all it will take, is a small clip-like device with a knob on its top, which by rotating, one can select the preferred candidate, clipped to the memory chips.

* 1. *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 electoral system of India. Thus, EVMs are tamper-able and vulnerable to fraudulences.

1. Proposed System

In this paper, we had designed a system involving machine with voting security mechanism. The machine is secured from any physical damages by sealing it. It is also locked using a USB type key. After using the key, an OTP will be sent to the Election Official of that booth, for verification. Once, verified the official need to press the Ballot Button. Once it is pressed, the session begins. The initiating process of voting machine is designed as figure 1.

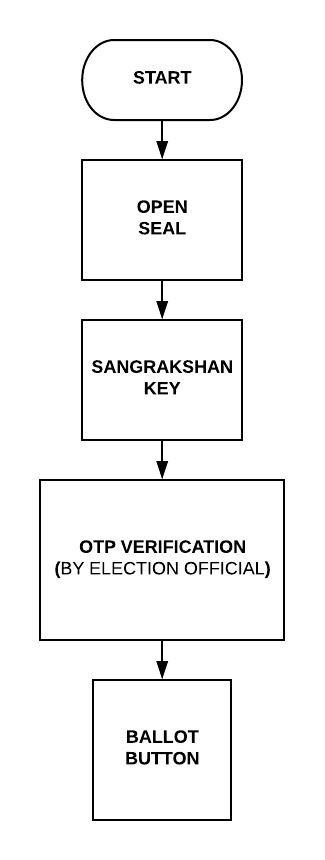


Figure 1. Initiating the Voting Machine

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

* Fingerprint Scanning
* Iris Scanning
* Facial Recognition

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

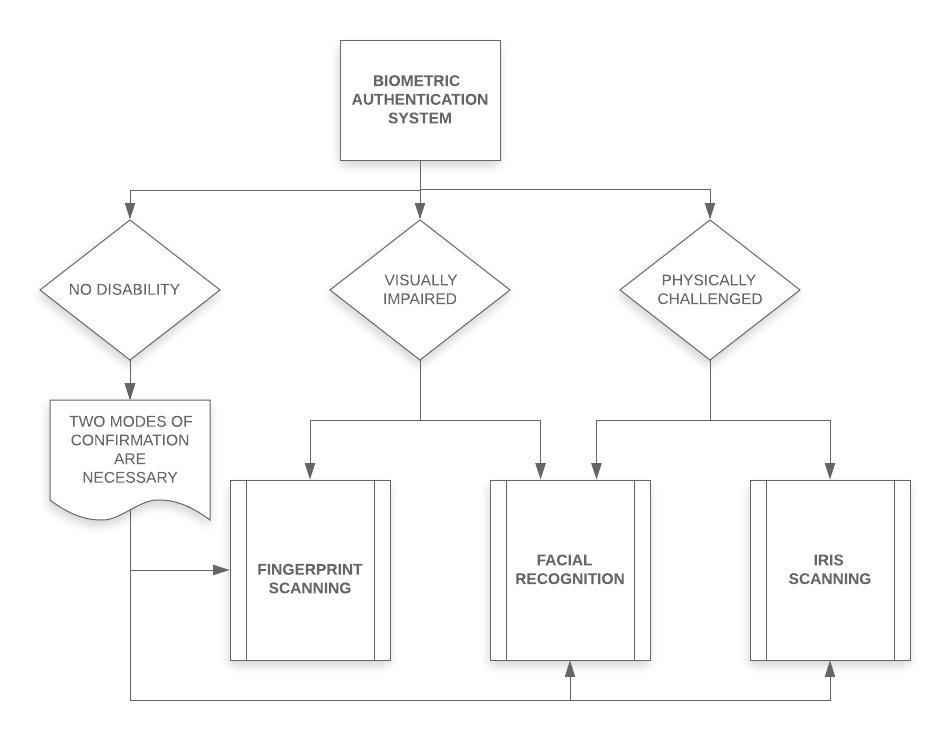


Figure 2. Multi-Mode Authentication System

This system can be broadly divided into 3 phases namely:

* Authentication and Verification Phase
* Voting Phase
* Counting and Tallying Phase

1. Authentication and Verification Phase

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

* Database Check
* AADHAAR Card Number Check
* Age limit and Eligibility Check
  1. *Database Check*

In this phase, 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 local database, it is searched for in the cached copies in the state database. If not found in state database, it is searched for in the cached copies of 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 for a time interval. It can be unlocked only by the election official present at the polling booth as the machine is secured, using the USB type key which is present only with the election official. After that, an OTP verification process the machine gets the machine unlocked.

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 network barrier and will prevent the attack while raising an alert for the same. Even if an attacker can circumvent the network – barrier, he will have to try and breach the host – based firewall too around each individual server, to cause any form of damage. To protect data both in transit and at rest, the network perimeter will be continuously managed and controlled. Voter will not only be given controlled access to the machine, but also his activity log will be audited by the completely autonomous voting machine itself in every few seconds, to keep a check for any unusual activity. The complete process of database check is described using figure 3.

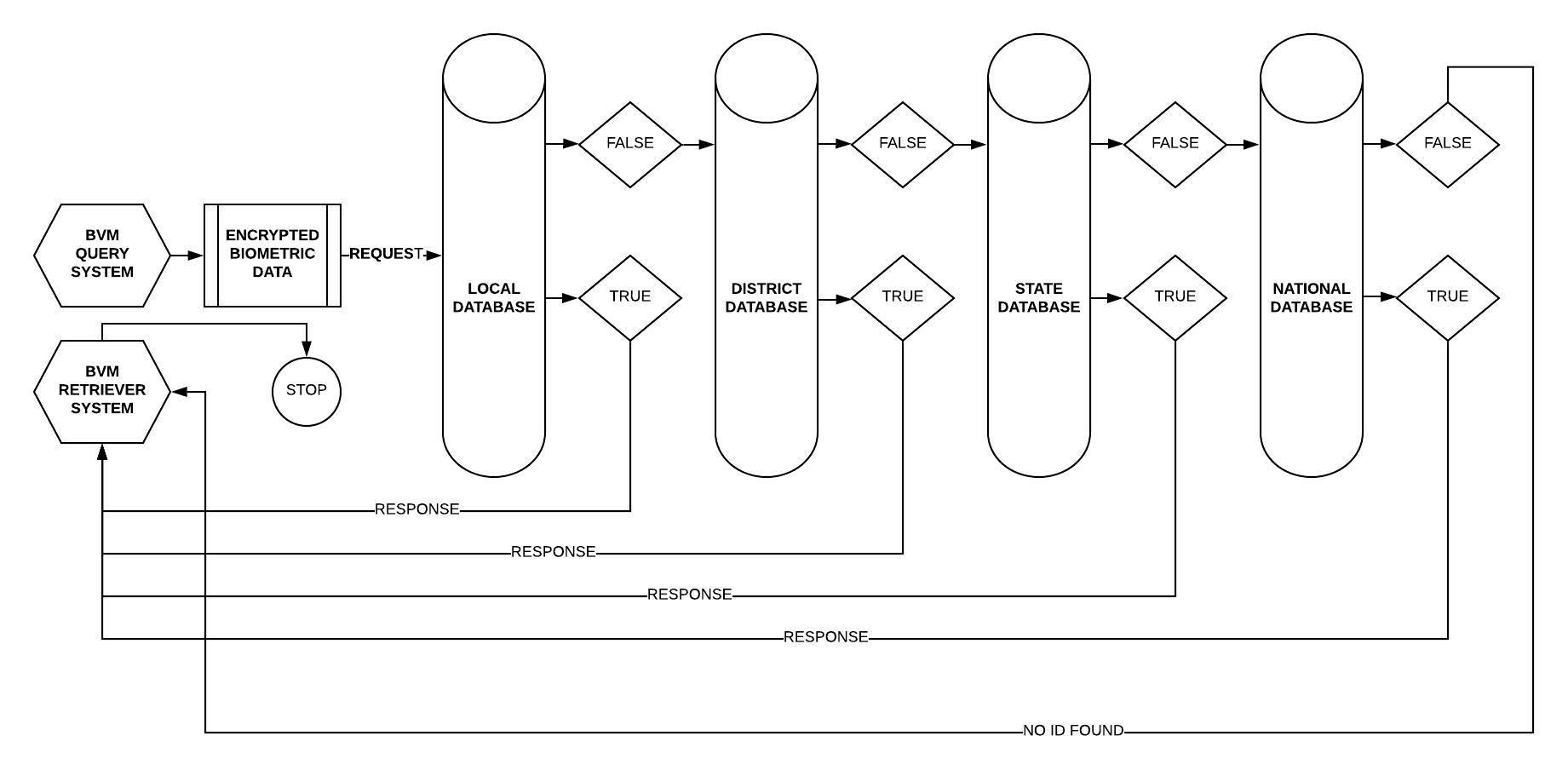


Figure 3. Query - Response System to authenticate voter

* 1. *AADHAAR Card Number Check*

After the database check it’s an important to check the originality of voter through Aadhaar card database. So, under this process if the biometric data is found in any of the database, that database starts getting updated. When the Aadhaar Card number of the voter is found to be existing in the database, an age limit check is also imposed for verification to check the eligibility of the user to caste vote in the elections.

* 1. *Age limit and Eligibility Check*

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

Thus, for any voting system the above three checking process are best to overcome the issues of misuse or wrong voting as it directly effects on the voting results.

1. Voter-List Check

As we know that the elections are characterize into many different forms like state, district/region or any sub-area wise. So in any kind of elections, if the user is found in the voter list of local or state database, the respective databases starts getting updated allowing the voter to caste his/her vote from anywhere in the country at his/her own convenience, else a notification is displayed asking the voter to fill the Form-6 to register themselves in the voter list, buzzer beeps and an exit screen is displayed. All this logging data is protected by AES encryption. The query-response system for checking voter-list check is designed as figure 4.

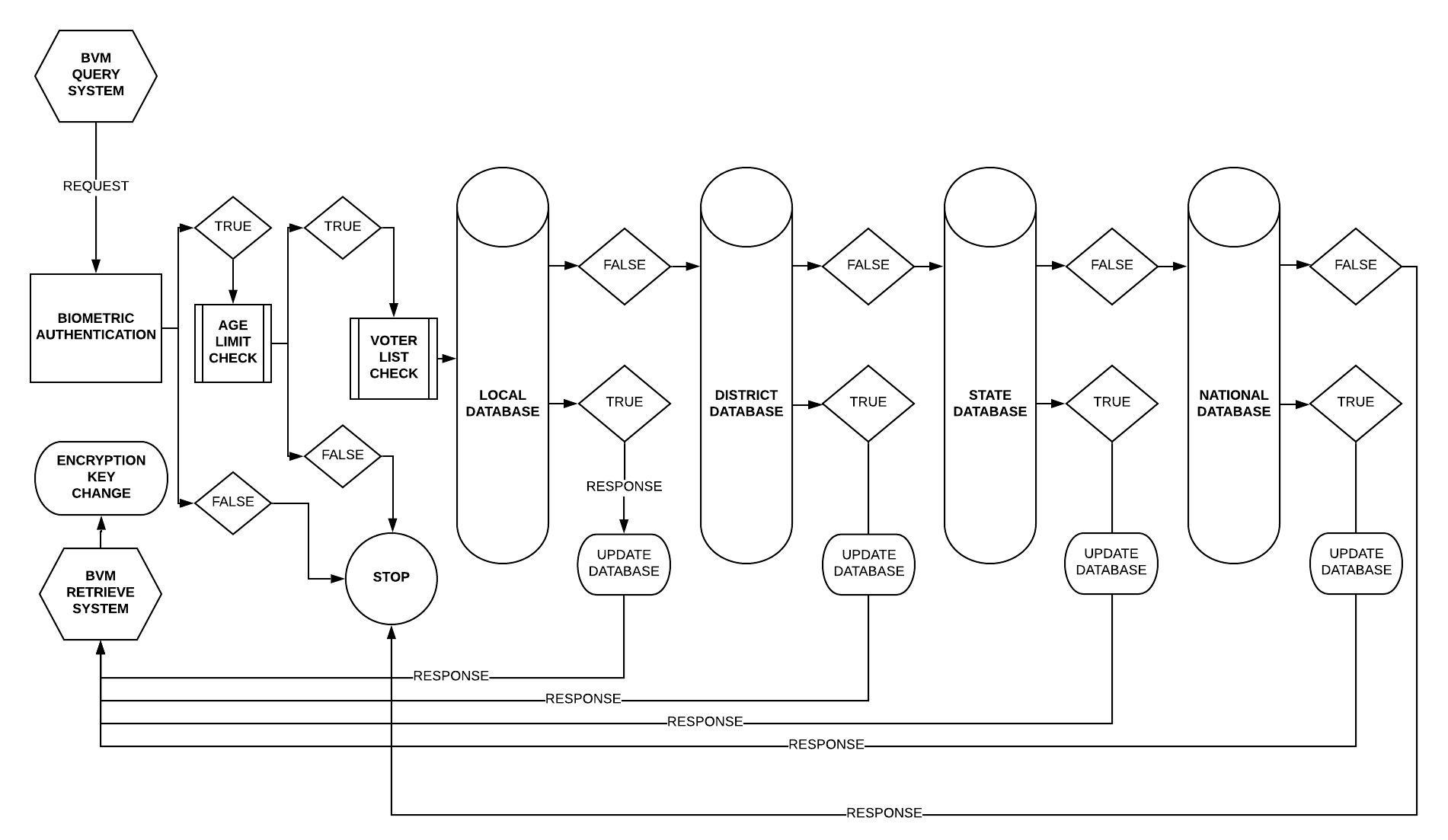


Figure 4. Query-Response System for Voter-List check to determine Constituency of the voter

* 1. *Voting Phase*

After authentication and verification, user starts getting recognised as a voter. The voting phase is designed as figure 5.

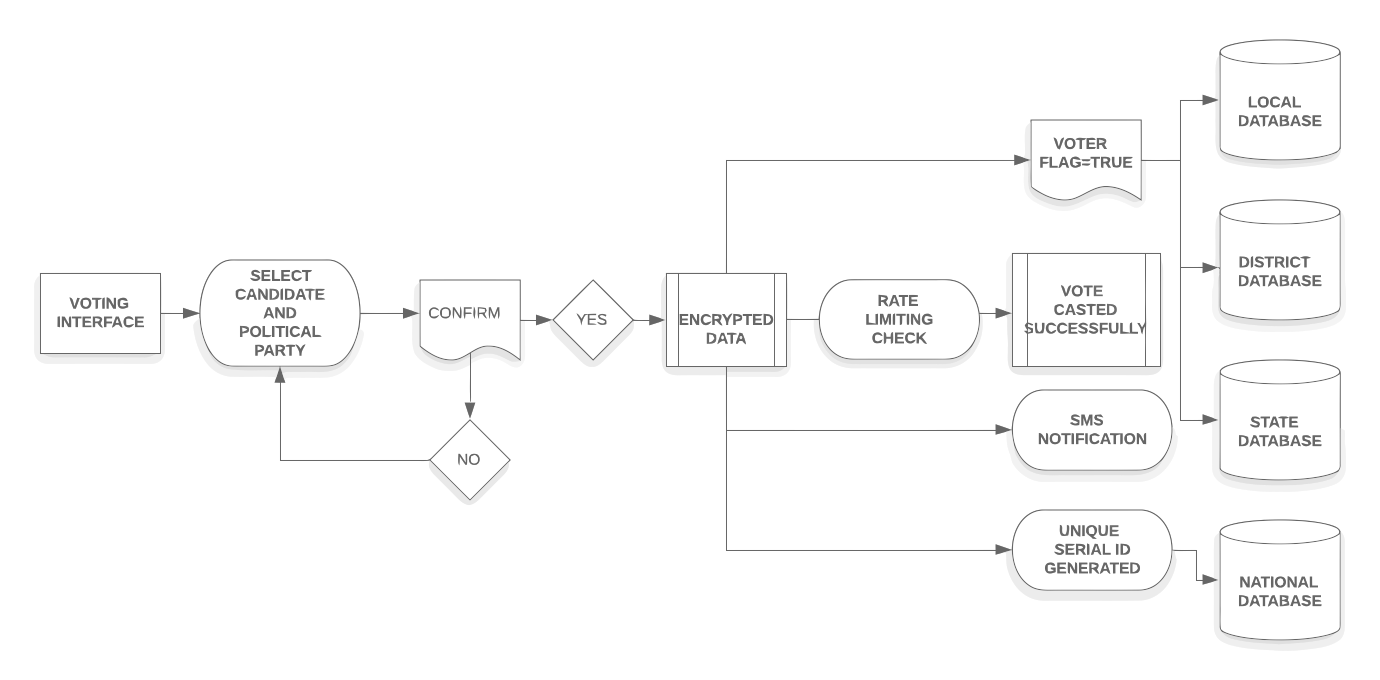


Figure 5. Voting Phase

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 caste his/her vote. After selecting the candidate and the respective party, voter clicks on the vote button. A pop-up message is displayed asking the voter to confirm his/her preferred choice. If voter does not confirm the message, he/she can make a change in his/her choice but if the voter confirms the message, vote gets casted and the database gets updated. Once the vote has been casted, the value of voter flag gets set to true or 1 and a serial ID is generated simultaneously. This is done to prevent the voter to cast a vote more than once. The serial ID generated gets stored in the state and the national database. This voting interface is open for a specific duration of time. And 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.

1. 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 loss with full security. Therefore, the major advantage of our paper is that we introduce the new technique for counting and tallying voting record in safer form. 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 of votes is done across all the databases. Then the tallying process begins. If any bogus votes found, they are eliminated automatically using the difference in serial IDs generated and updates in local database.

At local and state database, only voting data is present. But 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, 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 and take required steps and make much needed reforms to increase voter turn-out in the future. In the proposed system, Rate-Limiting function is also included where not more than 3 votes can be casted in a minute to neutralize physical challenges such as booth-capturing.

1. Conclusion

As a result, to this paper we had concluded with the new voting system that provides five major specific advantages over existing voting machine as:

1. Transparency
2. Accessibility
3. Security
4. Speed
5. Accuracy

It restores the integrity of electoral process makes the voting system of the nation more reliable by comprising of unique features to overcome different challenges faced by the classical system. It has a rate – limiting feature which sets the limit of 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 multi-modal biometric authentication system, voting data - encryption, a firewall system for preventing any malicious attacks on voter database, thus making it more secure, transparent and accurate. A unique serial ID is generated for every successful vote that is casted, and stored in national database, which makes the process of counting, tallying, auditing, and in special circumstances such as recounting of votes, faster and easier. Thus, the proposed system discussed in this paper will be beneficial to new world for providing better and safe electronic voting machine to users by using multi-modal biometric authentication system, data encryption and firewall.

References

1. T. Kohno, A. Stubblefield, A. D. Rubin, 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, D.S. Wallach, “Hack-a-vote:Security issues with electronic voting systems”, IEEE Security & 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, V. Yagati, and R. Gonggrijp, “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, 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, 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 & Technology (ICAST), pp. 1 – 7, 2014.
6. J. Pomares, I. Levin, R. M. Alvarez, G. L. Mirau, 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.

## A. Das, M. P. Dutta, 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.

1. Z.A. Usmani, K. Patanwala, M. Panigrahi, 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.
2. R. Rezwan, H. Ahmed, M. R. N. Biplob, S. M. Shuvo, Md. A. Rahman, “Biometrically secured electronic voting machine”, 2017 IEEE Region 10 Humanitarian Technology Conference, pp. 510-512, 2017.
3. R Bhuvanapriya., R. S. Banu, P. Sivapriya, V. K. G. Kalaiselvi, "Smart voting", in Proceedings of 2017 2nd International Conference on Computing and Communications Technologies (ICCCT), pp. 143 – 147, 2017.
4. T. Illakiya, S. Karthikeyan, U. M. Velayutham, and N. R. Devan, “E-voting system using biometric testament and cloud storage,” in Science Technology Engineering & Management (ICONSTEM), 2017 Third International Conference on IEEE, pp. 336–341, 2017.
5. Ch. J. Lakshmi, 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.

## L. R. CarrIII, A. Newtson , J. Joshi, “Towards Modernising the Future of American Voting”, 2018 IEEE 4th International Conference on Collaboration and Internet Computing (CIC), pp. 130 – 135, 2018.

1. S. Patil, A. Bansal, U. Raina, V. Pujari, 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.