A REVIEW PAPER ON

RADICAL ANOMALIES REMOVAL FOR VOTING SYSTEMS USING DIGITAL AUTHENTICATION

MilindVedi

Department of Information Technology

Babu Banarasi Das National Institute of Technology and Management

Lucknow, India

1. ABSTRACT

The purpose of the project is to remove the problems that occur in the voting systems that are present right now and create a voting system that would be rather fool proof and 100% transparent with secure and 100% trustworthy validation processes.

The voting systems that are present in the present scenario are not completely trustable by the people. Many cases have been seen in which the people report about scams in voting and people have issues and complaints about mismatching of their votes.

This is because there are no appropriate methods to check whether the casted vote has reached to the right candidate. A version ofthe software in project also aims at providing voting services at schools, colleges and other levels also.

Various problems in current voting systems like time consumption in casting of votes, multiple voting problem, time taken in result declaration and counting of votes, no validation of vote by voter, reduced number of voters, validation of voters done incorrectly, altering of election results by accessing the machines by frauds, no procedure to provide the transparency for verification of casted votes led to the development of this project.

Keywords- Electronic Voting System, EVM, Secure Voting, Digital Authentication in EVMs, Validation in Voting, Aadhaar Voting, Transparent Voting, Radical Anomalies Removal for Voting Systems using Digital Authentication.

INTRODUCTION

This is a research paper about developing a 100% transparent Voting System with efficient Validationprocesses gaining faith of voters as well asproviding efficient security in voting.

1. RESEARCH PROBLEMS (ISSUES WITH CURRENT VOTING SYSTEM)

Several studies using computer technology improved in elections. These lessons tell about the risk of use of the electronic voting system as a result of software challenges, internal threats, network vulnerability, and audit challenges. Various kinds of errors are introduced in Electronic Voting Systems.

• **Time Consumption between casting and recording of votes -**   The time taken between the casting of the vote and recording it over the server make the votes vulnerable to be disordered or sometimes even prone to be hacked.

• **Multiple Voting Problem -**   Voting systems are vulnerable to the casting of votes by a single person multiple time. Nowadays only a physical identification for checking whether a person has casted the vote is used. In various of the cases this issue is raised by the voters.

• **Time Taken in Result Declaration and Internal Counting of Votes -**   the counting of votes is much longer as the votes are 1st stored and then they are added up which also increases the time taken in result declaration and also puts the votes to a risk of being altered.

• **No Validation of Vote by Voter** -   Once a voter casts a vote, he has no method to validate whether his vote is casted to the same candidate he intended to. This is another reason for people to claim that their vote is not casted successfully. This brings down their trust in voting and also decreases the number of voters.

• **Reduced Number of Voters-**   Often cases for wrong voting are reported by the voters because they could not validate their votes. This results in decreased number of voters.

• **Validation of voters done incorrectly.**

• **Altering of election results by accessing the machines by frauds.**

• **The voters find the event boring and time consuming and most importantly doubtful about correct casting of votes leading to lesser number of voters.**

•**No procedure to provide transparency for verification of casted votes.**

2.   SECURITIES PROVIDED IN OUR VOTING SYSTEM

• **Eligibility:** Only the genuine person should be able to vote.

• **Authenticity:** Only the certified person should be able to vote.

• **Uniqueness:** No voter should be able to vote two times or more.

•**Accuracy**: Recording of votes should be done properly.

•**Integrity**: Number of casted votes should not be transformed.

•**Fairness**: Incomplete presentation of results should be avoided.

• **Reliability**: Systems must work strongly with greater assurance by minimizing the faults.

• **Confidentiality**: No leakage of data should be done (avoided).

• **Secure Validation of votes by voters(Double layer of Validation)**

3.   OBJECTIVES OF THE PROPOSED SYSTEM

➢ To Create a voting system that provides 100% transparent voting.
➢ To provide validation of votes to the voters and gain their trust in voting.
➢ Providing double layer of validation to the voters.
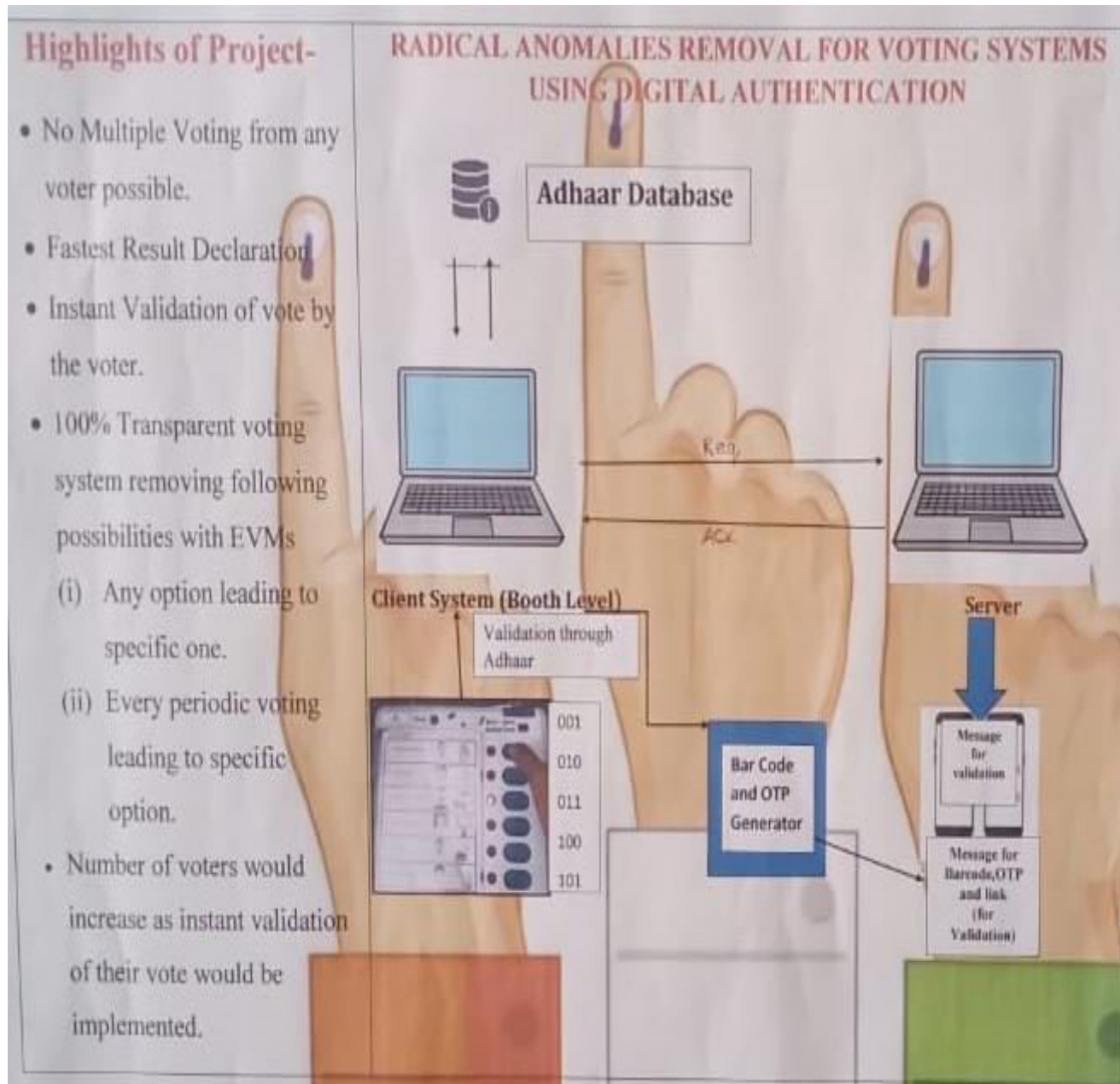➢ Making use of barcodes that will be unique for all voters to validate their votes.
➢ Making use of biometrics while voting for providing guarantee of genuine voters and not allowing votes to becasted more than once by a particular voter by accessing details from Aadhaar.

4.   Proposed System

To overcome the problems stated above a new voting system is proposed in this project. This voting system provides 100% transparent voting with surety of genuine voters, security and no casting of more votes than 1 individual and most importantly a double layer of validation. It uses biometric traits of the voter for verifying the authenticity of the voters.

If the biometric scan data is matched to the database, he or she will be allowed to vote, otherwise it will be discarded and we will be declared a false voter. Everyone has unique Biometric properties such as fingerprints, iris, gloves, voice, face etc.

5. Proposed System Design

6. OBJECTIVES OF THE PROPOSED SYSTEM

- ➢ To Create a voting system that provides 100% transparent voting.
- ➢ To provide validation of votes to the voters and gain their trust in voting.
- ➢ Providing double layer of validation to the voters.
- ➢ Making use of barcodes that will be unique for all voters to validate their votes.
- ➢ Making use of biometrics while voting for providing guarantee of genuine voters and not allowing votes to be casted more than once by a particular voter by accessing details from Aadhaar.

7. RESEARCH METHODOLOGY

7.1 Heading with Creating a Secure Environment

Firstly, a secure environment for voting is created otherwise the voting is not initiated.

7.2 Verifying the voter

When the voter casts the vote, it is checked whether the person is a genuine voter or not. For example: checking whether the person is an Indian or not, this is done by checking his biometric credentials with the one recorded within the Aadhaar database. This also helps in verifying whether the person has casted the vote previously or not.

7.3 Barcode Generation

The barcode is generated using the credentials of the server system or the client and server system both depending upon voting scenario. It consists of details about boot level computer, voter, voter number and EVM machine from which the vote is casted.

7.4 Generating Barcode and sending it to the voter

Immediately after the vote is recorded within the E.V.M a unique barcode is generated for that candidate and a hard copy of the barcode is provided to the voter. Also, a softcopy is sent to the voter's mobile number. This is done for validation purpose.

7.5 Sending of vote to the server

Immediately after the vote is recorded, the vote is sent to the server system. A barcode is generated at the server system during the recording of the vote and its count is also done parallelly and the barcode is created using the same information as done at the EVM level. So, if the two barcodes are same it shows that the vote has been casted successfully at the correct point as intended by the voter. Also, as a second layer for validation a file with some unique password is also sent to the voter which holds information about casted vote. This file is also created by the server during the recording of the vote so it also validates the vote.

7.6 Sending verification message from server

Verification messages are sent to the voters from the server system. A barcode is sent with the verification message which is created using the same credentials as those utilized at the E.V.M. level. Verification message is sent after the vote is recorded at the server which implements that the votes are casted to the correct candidate. The verification message also contains a password protected and encrypted file which contains information about that particular vote/voter.

8. WORKING

The working of the proposed electronic voting system can be serially described in following steps.

8.1 Step 1

Firstly, vote is casted by the voter at the EVM using finger (fingerprint). The EVM sends information about this vote to the client system. A barcode is generated by the client system. The hard copy of this barcode is provided to the voter immediately. Also, a soft copy is sent to the voter's mobile number using data from Aadhar link with the corresponding finger biometric in Aadhar. The details of the voter are also confirmed using these Aadhaar details. So, a voter cannot cast a vote more than 1 times.

8.2 Step 2

After successful verification of voter's details using Aadhar the casted vote's information is sent to the server system. The vote is then recorded at the server system. Parallelly to recording of the vote another barcode is generated at the server using the same details that were used at the EVM level. This barcode is sent to the voter. Also, parallelly a file is created with the details of the vote. This file is also sent to the voter from the server. The counting of the vote is also done parallelly to avoid any alteration in votes casted.

8.3 Step 3 (Validation)

After, the vote is casted a message is sent from the EVM to the voter. Another message is sent from the server during the recording of the vote. Both the messages contain barcodes. These barcodes are created using the same credentials but at different times. The first one is created by the booth level system (EVM level barcode) when the vote is casted by the voter and the second one is created by the server computer when the vote is recorded. If the two barcodes are same then it means that that the vote is casted to the correct candidate as done by the voter and this provides validation of the vote.

8.4 Step 4 (Second Validation)

A file is also sent to the voter by the server. This file holds information about the casted vote and is created and sent during the recording of the vote at the server level. This provides a second layer of validation to the voter.

8.5 Step 5 (Result Declaration)

The counting of the votes was done parallelly to the casting of the votes so results are declared immediately after the voting is completed.

In case of multiple number of client systems at far away locations the information from these systems is first brought to the election commission server and here the counting of the votes is done and then result is declared.

9.   SOME SNAPSHOTS OF THE WORKING SYSTEM

EVM Side (Virtual EVM)

Figure 9.1- Start page in the Virtual EVM

Figure(s)9.2 – Loading of candidates and other pre voting important (admin's) details needed for voting.
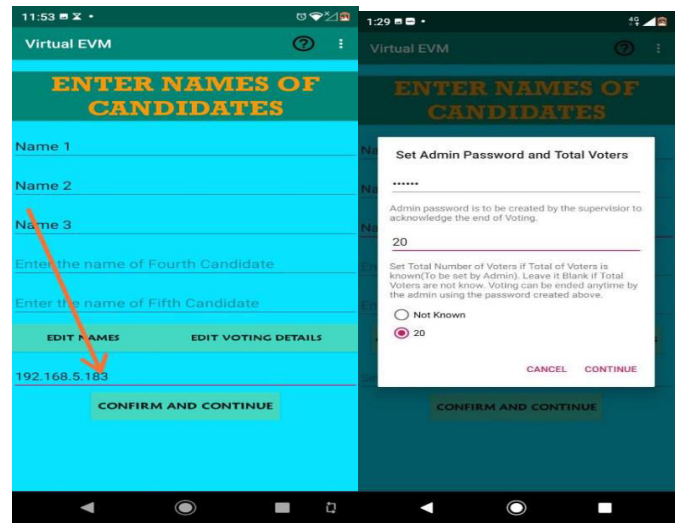
Figure(s)9.3 – Casting of Votes from the EVM.
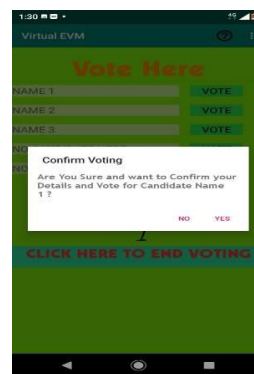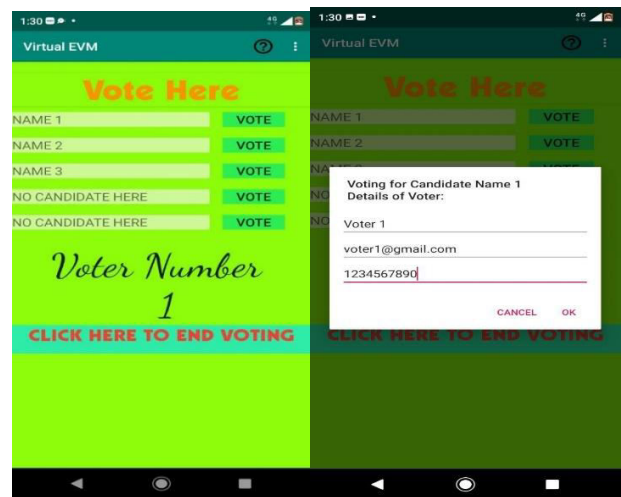
Figure 9.4 – Generation and Sending of QR CODE (EVM Level)
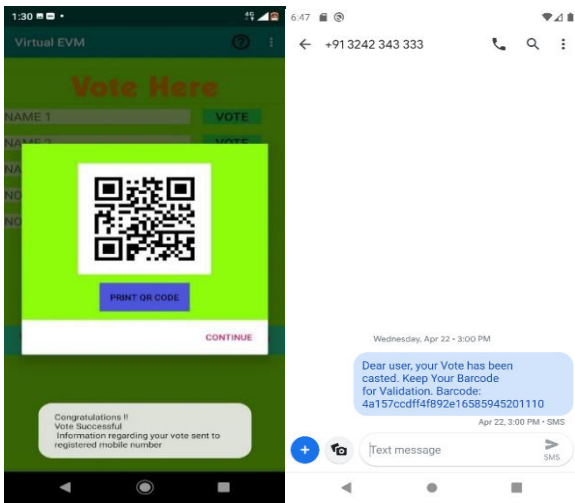
Figure(s) 9.5 – Help and About Section
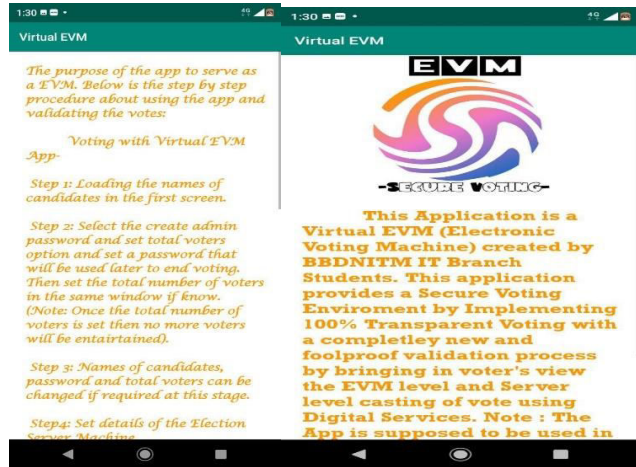
Figure(s)   9.6   –   End   of   Voting   Message


Server Side

Figure(s) 9.7 – Working
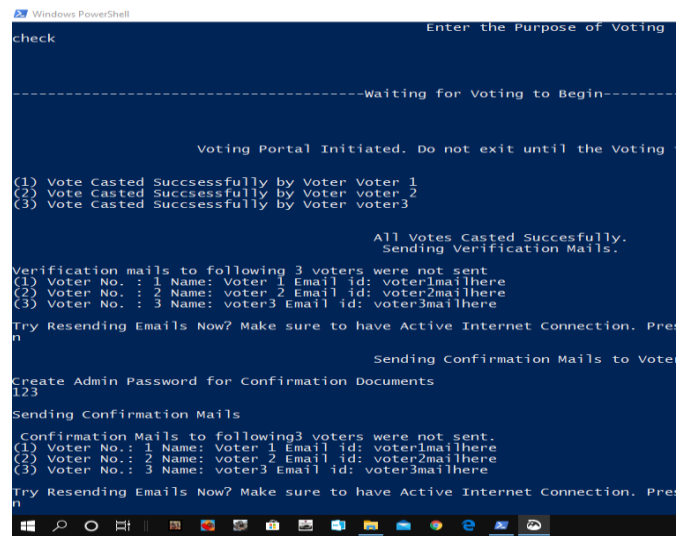
Figure(s) 14.7 – Saving of Data over the Server Securely in Encrypted Format
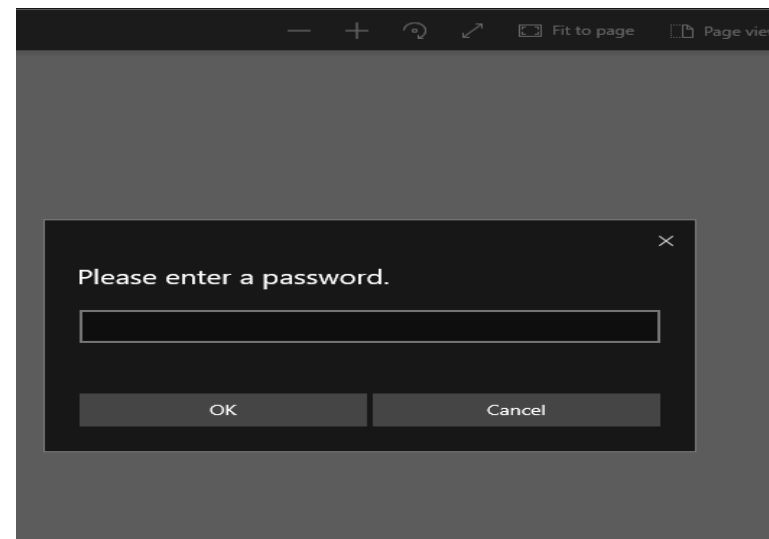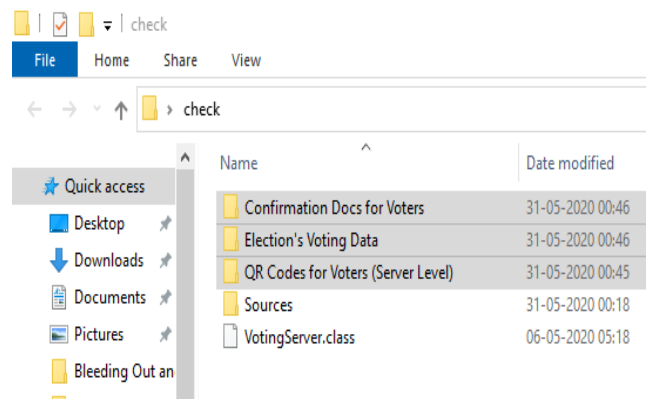
Election's Voting Details

Voter's Number	Voter's Name	Voter's Contact Number	Voter's Email ID	Name of Voted Candidate	Voted Candidate's Serial Number as per EVM	Server Generated QR Code
1	Voter 1	1234567890	voter1mailhere	Name 1	1	
2	voter 2	987654321	voter2mailhere	Name 2	2	
3	voter3	1239876540	voter3mailhere	Name 2	2	
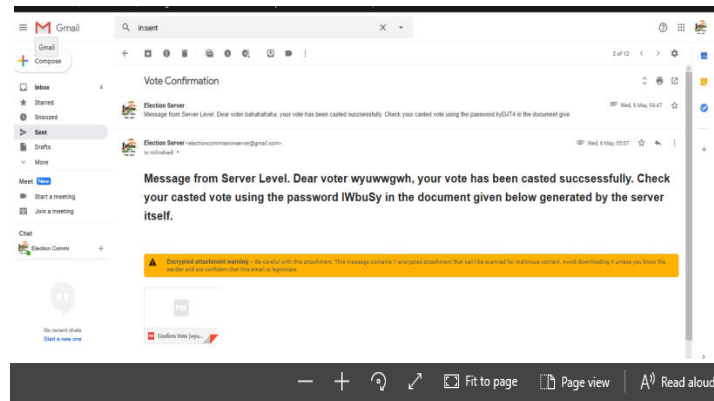
Details of Candidates
(1) Name 1
(2) Name 2
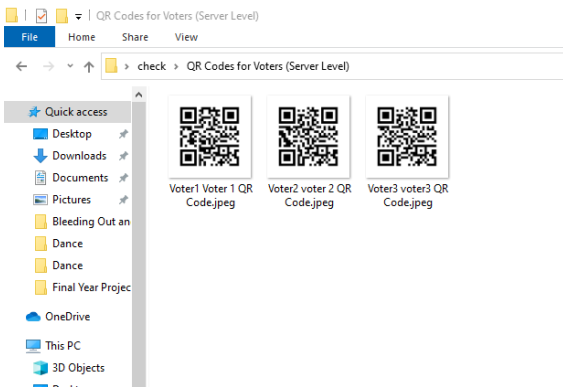
Figure(s)14.8- Sending of the Validation Messages from the Server
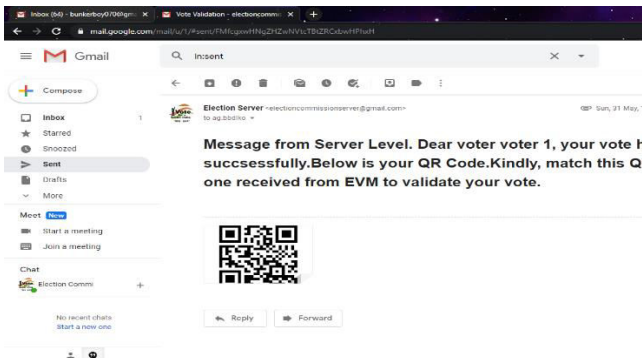
10. CONCLUSION

✓ We have removed the various problems in current voting systems.

✓ We have provided 100% transparent voting.

✓ Double layer of verification is provided to the voters for casted votes.

✓ Voting data is saved encrypted and in a proper manner.

✓ A secure voting system is created with double layer of validation.

✓ The Double layer of validation provided plays a very important role in validation of votes and is fool proof.

✓ The Double Layer of Validation and the 100% transparency provided in the Electronic Voting System plays a great role in attracting more voters by gaining their trust.

✓ No Multiple Voting from any voter possible.
✓ Fastest Result Declaration
✓ Instant Validation of vote by the voter.

✓ 100% Transparent voting system removing following possibilities with EVMs:
  a) Any option leading to specific one.
  b) Every periodic voting leading to specific option.

✓ Number of voters would increase as instant validation of their vote would be implemented.

11. ACKNOWLEDGEMENT

12. REFERENCE

[1] https://en.wikipedia.org/wiki/Electronic_voting_in_India

[2] https://eci.gov.in/evm/

 [3] https://economictimes.indiatimes.com/news/elections/lok-sabha/india/what-are-evms/articleshow/68807699.cms?from=mdr

[4] http://uidai.gov.in/aadhaar.html

[5] https://en.wikipedia.org/wiki/Electronic_voting_in_India#Benefits.

Name- Milind Vedi