International Journal of Scientific Research and Engineering Development-– Volume 4 Issue 1, Jan-Feb 2021

Available at www.ijsred.com

RESEARCH ARTICLE OPEN ACCESS

Voter Authentication, Vote Counting & Voter Verifiability in an Electronic Voting Machine

Md. Abdul Based*, Tafsir Ahmed Khan**, K.M.Peash***

*(EEE Department, Dhaka International University, Dhaka, Bangladesh)

** (EEE Department, Dhaka International University, Dhaka, Bangladesh)

***(EEE Department, Dhaka International University, Dhaka, Bangladesh)

----------**********----------

Abstract:

Electronic Voting is the most modern system for vote casting and counting in the world which uses electronic means to take care of casting and counting votes. However, there are lots of debate exists on the practicality of an electronic voting machine. This paper presents an electronic voting machine which can authenticate valid voters and take care of vote casting and counting. Though this particular machine has lots of resemblance with some previously developed machines, it has some unique features that justify the rebuilding. This work requires voters' identification card to allow them to enter the voting center. Then the voting machine inside the booth will authenticate the voter and check the status of the voter for preventing multiple votes. If everything goes right then the voter will be allowed to cast a vote. The voting machine will then generate a random reference number and the voter can keep this random number for verification purpose later. The vote cast by a voter will be written in a hidden Micro SD card and the random number will be written in another hidden Micro SD card which will later be sent to election commission for publishing along with the result. This random number will be used to verify whether the vote cast by a voter is counted or not. Our voting machine can reduce the cost of voting system & time to count votes manually and can provide improved accessibility. This is due to easy and cost effective integration of existing and upcoming technologies.

Keywords **—Electronic Voting, Electronic Voting Machine, Authentication, Verifiability, and Election Commission.**

----------**********----------

I. INTRODUCTION

Bangladesh is a democratic country and the Bangladeshi people have a lot of interest in elections for selecting their chosen candidates. Ensuring a fair election has become a great challenge for the Election Commission (EC) of Bangladesh. The EC has been trying to implement Electronic Voting (E-Voting) in Bangladesh for the last few years. The EC has developed and/or imported different Electronic Voting Machine (EVM) in different elections though information security flaws were big concern in all elections.

It has been a big challenge for the EC to convince the opposition parties and the general people about the advantages of EVM. The EC of Bangladesh introduced EVM in Chittagong City Corporation Election (2010), Comilla City Corporation Election (2011), Narayanganj City Corporation Election (2011), some centers of Rangpur, Barisal, Sylhet, Rajshahi and Khulna City Corporation (2016) and only in six places in the national election (2018) [1]. It has created awareness to the general people gradually and EVM starts getting popularity. Recently, EVM is used in the city corporation election of Dhaka and Chattogram in 2020. An illustration of 2020's EVM is shown in Fig. 1 [1].

Although it was a pretty good device, it lacked the feature of voter verifiability.

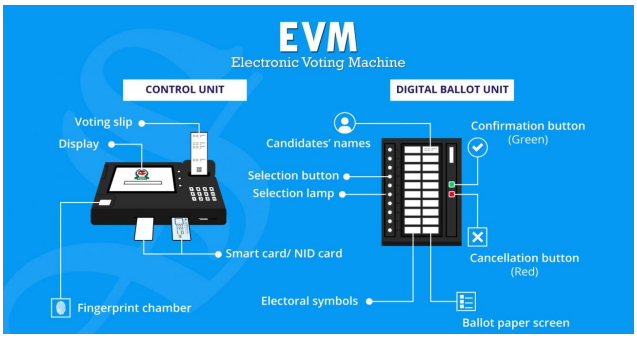

Fig. 1.EVM system used for 2020 Dhaka City Corporation Election.

In this paper, we present an electronic voting machine that will help to eradicate defrauding of the manual voting systems and prior versions of e-voting. This e-voting machine allows people to cast vote from a vote centerafter being validated using the fingerprint sensor. Primarily, we target to use it in the elections of Bangladesh though it is easily extensible to use in other countries.

We discuss the properties of EVM in Section II. Our proposed EVM is explained in Section III. We present the advantages of our EVM in Section IV. Conclusions are presented in Section V.

II. PROPERTIES OF EVM

An EVM is expected to solve the problems that exist in the traditional paper based elections. However, it is nearly impossible to overcome all problems by using a particular EVM. Before designing an EVM, the expected properties should clearly be stated first. Most of the researchers expect the following properties [2] from EVM:

Accuracy: By accuracy we mean it is not possible for a voter to alter or change a vote that is cast already. An invalid vote should not consider in the counting process. In addition, a valid vote should not be eliminated from the final tally.

Democracy: Democracy means a voting system should allow only the eligible voters to cast a vote and a valid voter should vote only for once.

Privacy: Privacy property ensures that no voter can prove that how did the voter cast the vote. In addition, neither the authorities nor anyone should link any vote to the voter who has cast it.

Verifiability: By the verifiability, anyone can independently verify that all votes have been counted correctly (public or universal verifiability). It also ensures that any voter can verify that his/her vote has been counted correctly.

Availability: The availability property provides access of a voter to vote from the beginning to the end of the poll and ensures that the voting system works fine for the whole period of voting.

Resume Ability: The system allows any voter who had interrupted his/her voting process to resume it or restart it while the poll stands [3].

III. OUR PROPOSED EVM

Our proposed E-Voting system has been divided into several parts. The different parts are explained as follows:

1. **Voter Access:** First a voter needs to show his/her smartcard on smartcard reader to get access in the voting room. We have done it by Radio Frequency Identification (RFID) card and reader as a sample version.

2. **Biometric Voter Authentication:**After entering the voting room, a voter needs to put his/her finger on the fingerprint module. If the fingerprint is found on the stored database then a voter will be able to give his/her vote to the desirable candidate.

3. **Vote Casting & Counting:** After fingerprint authentication, a voter can cast a vote. After completion of the entire voting process, counter unit counts the stored votes for different candidates and it is also responsible for publishing the result.

4. **Voter Verifiability:** In our work, voters will be able to verify the vote by verifying a random reference number.A random number will be generated for every voter while the voter casts a vote and it will be stored in a SD card. Another SD card will contain the vote that has cast already. The EC will publish a chart/table showing the candidate wise vote from one SD card and the list of reference numbers from another SD card on the website. By checking the reference number, voters will be able to verify that the cast vote has been counted.

5. **Display:** This part shows the votes that have cast, the random reference numbers, and results at the end of the vote casting period.

The authors are concern about other important issues of e-voting system. However, in this paper the main focus is on voter authentication, vote counting and voter verifiability. In the recently (February 2020) used EVM in Bangladesh, voter verifiability cannot be achieved. If we can add the mechanism presented in this paper, then the EVM used by the EC will satisfy voter verifiability property.

The block diagram of our proposed voting system is presented in Fig. 2 and in Fig. 3.

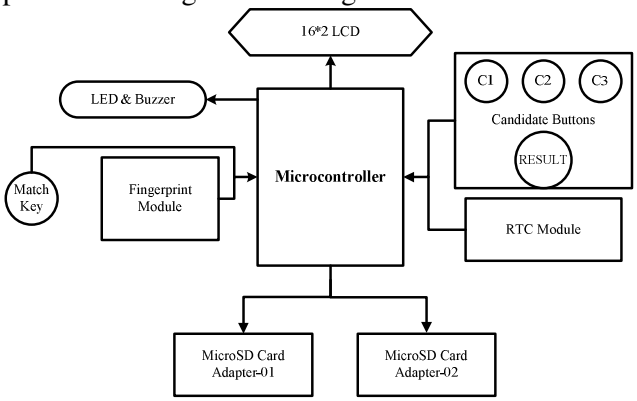

Fig. 2. Block diagram of EVM for vote casting, counting & voter verifiability.

By pressing the match key button, a voter can place his/her finger on the fingerprint module. After fingerprint authentication, a voter can cast his/her vote to the desirable candidate. A voter can cast a vote for once.

Here, we assume three buttons for three candidates as for example. The 'Result' button in Fig. 2 is used for showing the final result and it only works with the fingerprint of a specific authority (trusted) in the voting center. This trusted authority will be responsible to collect the votes and the random numbers in presence of the observers and vote officials. LCD display will show all the information about voter authentication, votes that are cast, random reference number, and results. One SD Card will store the random reference number and another SD card will store the vote for particular candidate. The random number has been produced by microcontroller programming. We have used Arduino as experiment purpose only. However, we can use any microcontroller programming. The EC will publish a chart/table showing the candidate wise vote and the random reference numbers on the website.

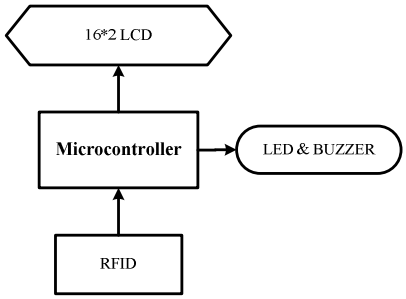

Fig. 3. Block diagram for voter access.

The hardware part of our EVM contains among others the following components:

- Fingerprint Sensor [FPM10A]
- Microcontroller (ATmega 328P)
- Microcontroller (ATmega 2560)
- RFID (Radio Frequency Identification) Card & Reader
- RTC (Real Time Clock) Module [DS3231]
- MicroSD card Adapter (Quantity-2)
- 16*2 LCD
- LEDs & Buzzers
- Push Buttons

A. Voter Access

Display unit is an important part of the EVM. Here, 16*2 LCD (Liquid Crystal Display) is used as a display.

First a voter needs to show his/her smartcard on smartcard reader to get access in the voting room. It can be done by RFID card and a reader as a sample version.

First the following instruction (Fig. 4) will be shown on the LCD.

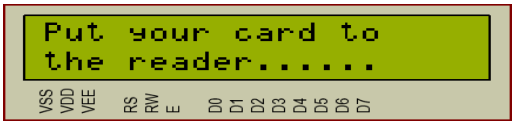

Fig. 4. Display shows the instruction to put the card to the reader.

If the voter's ID is valid, the basic information of the voter will be shown on the LCD including ID number, voter's name and date of birth (as shown in Fig. 5 & Fig. 6).

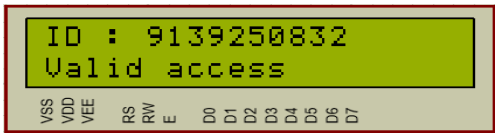

Fig. 5. Display shows the ID of a valid voter.

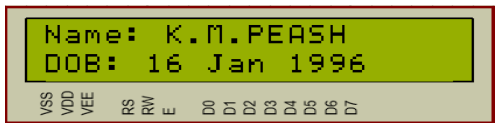

Fig. 6. Display shows the name of a voter with date of birth.

If the voter ID is not valid, the display will show the following information which is shown in Fig. 7 &in Fig. 8. If a voter from one center accidently goes to another center, he will not be considered as a valid voter.

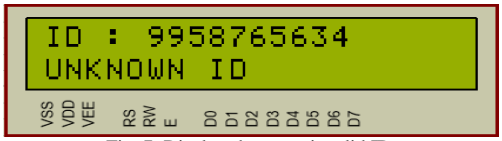

Fig. 7. Display shows an invalid ID.

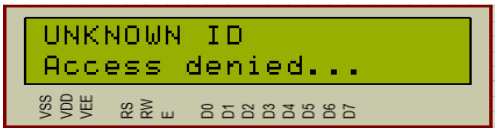

Fig. 8. Display shows access is denied for an invalid voter.

If a voter is considered to be an invalid voter in a particular vote center, he/she will not be able to cast any vote and the alarm will sound.

B. Biometric Authentication

After getting access to cast a vote, a voter needs to put his/her finger on the fingerprint module. If the fingerprint is matched then a voter will be able to cast his/her vote to the desirable candidate. Instruction will be shown on the LCD.

By pressing "Match Key" button (as shown in Fig. 9) voters have to place their finger on the fingerprint module.

Fig. 9.Instruction for pressing Match Key button.

If the fingerprint module is unable to identify the fingerprint of a voter, following instruction (as shown in Fig. 10) will be shown on display.

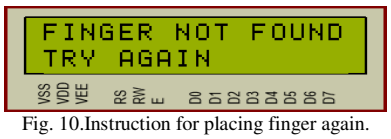

Fig. 10.Instruction for placing finger again.

If fingerprint is matched with the stored fingerprint, a voter will able to cast his/her vote (as shown in Fig. 11).

Fig. 11.Asking an authorized voter to cast a vote.

C. Vote Casting

There are three buttons for three candidates as for experiment. Voters can see on the monitor which candidate they have voted for.

If the voter casts a vote for candidate number 1, display will show the following (as shown in Fig. 12).

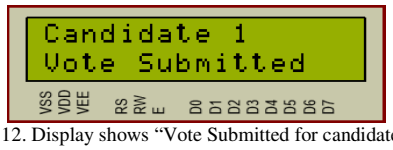

Fig. 12. Display shows "Vote Submitted for candidate 1".

After casting a vote, a voter will notice a random reference number which will be shown (Fig. 13) on display for few seconds. Voters can keep this reference numberfor future purpose.

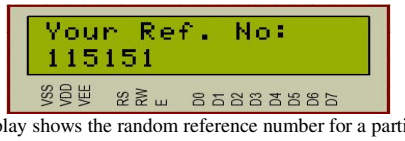

Fig. 13. Display shows the random reference number for a particular voter.

On the other hand, if the fingerprint is not matched with the stored fingerprint then buzzer will alarm and voters will not be able to cast any vote. This is the main advantage of biometric authentication. Without fingerprint authentication a voter will not be able to cast a vote. In addition, a voter cannot vote twice.

If a voter tries to vote twice (as shown in Fig. 14), the buzzer will alarm and the following information will be shown on display.

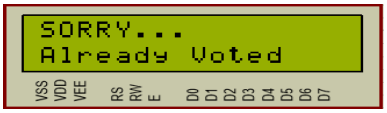

Fig. 14. Display shows "A voter has already submitted his/her vote".

D. Vote Counting & Result

After completion the entire voting process, counter unit counts the stored votes for different candidates and it is also responsible for publishing the election result. The result will be published after a specific time. There is no chance of publishing any partial result.

The number of votes a candidate receive will be displayed on the display separately as shown in Fig. 15. The candidate who gets the maximum vote will be shown as the winner (shown in Fig. 16).

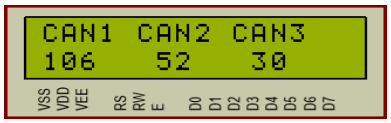

Fig. 15. Display shows the number of votes that the candidates have received.

The number 1 candidate will win because of maximum vote.

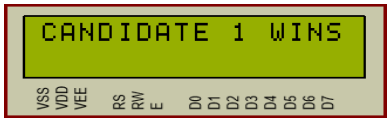

Fig. 16. Display shows "candidate 1 is the winner".

E. Voter Verifiability

As soon as a voter casts a vote, a random reference number will be generated by the microcontroller and this will be stored (as sorted) in a SD card as shown in the following.

Sample1: (SD Card 01)

Random reference numbers in descending order:
01. 984665
02. 964574
03. 878454

The voter will keep this random number which will be displayed by the EC. By verifying the random number, the voter will be confirmed that the vote has been counted correctly.

The vote will be stored in another SD card as shown in the following (Sample2). The EC will also publish this vote on the display. Total number of vote from one SD card will be equal to the total number of random numbers. This will ensure that no valid vote has been dropped or no invalid vote has been counted.

Sample2: (SD Card 02)

Candidate names according to vote sequence.
01. Voted for candidate 2
02. Voted for candidate 1
03. Voted for candidate 1

IV. ADVANTAGES

The following advantages will be achieved from our proposed EVM.

- Only the valid voters will cast vote
- One voter cannot cast vote of another voter
- A valid voter can cast a vote for once
- Not possible to cast a vote after the voting period
- Result is fair & accurate
- No delay for result announcement
- Result will be published after a specific time (No partial Result)
- Rejected vote will not be counted
- Result cannot be manipulated
- Same device can be used in many elections
- Voters can verify that their votes have been counted

V. CONCLUSIONS

The EVM presented in this paper will enable a voter to cast a vote through fingerprint in a voting booth and proxy vote or double voting is not possible. It allows fast access, easy to maintain all information of voting, efficient and flexible. It can also provide accurate counting without any troubles. In addition, it ensures voter verifiability to all voters of their voting with the reference number which will be published on the website of the EC.

This EVM is a reliable and secure voting method that will increase the voter participation in election and will achieve public satisfaction. It reduces unwanted human errors. Fingerprints of every person are unique and hence this system completely restricts the invalid voters.

There are some other possible scopes for future study as well. One of the challenging obstacles will be to store mass number of fingerprints and mass information in the database as the internal memory of the microcontroller has a very limited capacity. Providing receipt-freeness and coercion resistance will be another useful future work. After implementing this EVM for large scale election, performance analysis will be another task to accomplish.

ACKNOWLEDGMENT

The authors would like to acknowledge the contribution from the Research and Publication Cell of Dhaka International University to develop this EVM as part of the funded research project.

REFERENCES

[1] The Daily Star. Web: https://www.thedailystar.net/bangladesh-national-election_2018/news/how-vote-evm-1678195 (Last Access on 28.02.2020).

[2] Rubin A.D. "Security considerations for remote electronic voting", ACM, 5(12):39-44, Dec.2002.S. Zhang, C. Zhu, J. K. O. Sin, and P. K. T. Mok, "A novel ultrathin elevated channel low-temperature poly-Si TFT," *IEEE Electron Device Lett.*, vol. 20, pp. 569–571, Nov. 1999.

[3] Dill D.L., Mercuri R., Neumann P.G., and Wallach D.S., "Frequently Asked Questions about DRE Voting Systems", Feb.2003.

