Development of a Credible and Integrated Electronic Voting Machine Based on Contactless IC Cards, Biometric Fingerprint Credentials and POS Printer

CONFERENCE PAPER · MAY 2016

4 AUTHORS, INCLUDING:

Md. Tahmid Rashid
BRAC University
8 PUBLICATIONS **0** CITATIONS
SEE PROFILE

Md. Shadman Sakib Chowdhury
BRAC University
1 PUBLICATION **0** CITATIONS
SEE PROFILE

Development of a Credible and Integrated Electronic Voting Machine Based on Contactless IC Cards, Biometric Fingerprint Credentials and POS Printer

Syed Mahmud Hasan, Md. Tahmid Rashid, Md. Shadman Sakib Chowdhury and Dr. Md. Khalilur Rhaman
School of Engineering and Computer Science
BRAC University
Dhaka, Bangladesh
{syed.mahmud777, tahmidrashid, hchowdhury64} @gmail.com, khalilur@bracu.ac.bd

***Abstract*—In recent times there has been a decline in the confidence of common people over electronic voting machines (EVMs). More anticipated than what the reality actually is, today's automated vote casting methods have faced immense controversy related to being vulnerable to hacking and questions have been raised about their transparency and security. This paper proposes the design and development of a novel tamper resistant electronic voting system that aims to mitigate the recurring issues and flaws of existing voting machines of today. To elucidate the system in brief, multiple layered verification process would be carried out on a potential voter by the means of fingerprint recognition and a Near Field Communication (NFC) smart card entry in order to authenticate his or her identity. Subsequently, the person would cast the vote by pressing a button corresponding to a particular candidate which would be recorded in the system providing the vote caster a visual confirmation. The final vote would then be printed out spontaneously onto a ballot box using a POS (Point of Sales) printer for an added level of validation. This system not only prevents multiple vote casts, but also eliminates the discrepancies that commonly arise with a person claiming not to have voted, whereas his or her name is present in the list of vote casters. The project is an incremental extension of a previous research.**

Keywords—electronic voting machine; EVM; fingerprint recognition; NFC; POS printer

I. Introduction

Over the course of time, technology has found its way into the domain of democracy, the influence of which is so as intense that today, the mere thought of casting vote on papers have been replaced by pressing buttons on ballot machines or touchscreen kiosks. In certain applications today, even voting online, sitting at home has come to acceptance [1]. It is needless to mention that in the same pace as traditional voting processes have undergone evolution and have transitioned to the electronic versions today, concerns for doubts about the legitimacy and unfair means have also spiraled up. In the era of "all-digital" systems, hacking has become the icon of fear that plagues governments, financial institutions, multinational corporations and businesses in general. Building upon that, attacks on electronic voting systems are no exceptions [2]. Consequently, citizens find it difficult to rely on these systems when it comes to choosing the candidate of their choice.

II. Background Study

Digging superficially into the timeline of voting systems, traditional paper based voting method first came into existence in the Australian state of Victoria, in the year 1856 [3]. Since then, very few incremental changes were brought to the system. Around 1960s, electronic voting systems first made their appearance and punched card systems were introduced to facilitate voting [4]. These systems are widely termed as "paper-based electronic voting system" because here paper cards or sheets were marked by hand, but the vote counting process was carried out electronically [5]. Such systems ranged from punched card based vote casting to digital pen voting systems. A critical flaw of these systems was that they were not fully computerized and they required marks to be made by hand which brought along possibilities of miscounting, tampering and discrepancies.

The modern generation of voting machines are Direct Recording Electronic (DRE) systems, which are basically computers running customized software and providing a user interface to cast votes [6]. DRE systems are considered as upgrades over punch card based systems and as such, in conjunction with touch screen interfaces, DRE systems reduce voter inconveniences. However, when it comes to transparency and fairness, voters here have no choice but to trust on the machine manufacturers and the experts who maintain the systems. As a partial solution to the problem, in 2009 Alan Dechert introduced the "Dechert Design", an open source paper ballot printing system with printed bar codes on ballot papers [8]. Derivatives of this system include an Electronic Ballot Marker (EBM) that lets voters make their choice by pressing buttons on a touch screen or a set of tactile switches on a panel which in turn prints their decision on a paper using a POS printer and subsequently, drops it into a ballot box [3, 5]. Although certain DRE implementations include a paper tape that records votes as they are cast, this is not a commonplace in all DRE systems [9]. Thus DRE voting systems generally do not provide a human countable record.

The newest and most advanced breeds of electronic voting systems are the ones that allow citizens to cast votes over the Internet. One of the earliest iteration of internet based voting was Secure Electronic Registration and Voting Experiment (SERVE), which was an attempt taken by the United States' Federal Voting Assistance Program (FVAP) to allow a certain group of overseas citizens to vote in elections held in the United States through an internet gateway [10-11]. According to statistics, SERVE garnered participation of more than 100,000 voters from 51 countries [11]. The project got canceled, however, in February 2004 upon the release of a critical report by an expert group quoting several security flaws that could easily invite hackers to tamper with voting results [12-13]. Other concerns were raised about the transparency of the backend processes involved. The biggest issue of internet based voting is that voters have no notion of what is going on behind once they cast their votes with their computer [12, 14].

Till date, there are no set rules, principles or standards for developing a secure, tamper resistant electronic voting machine. As suggested by research and deriving on empirical voting, a voting system should be able to curtail fraudulent behaviors [15-16]. Problems like the issue of multiple votes cast by a single voter and tampering of voting data are common problems. More complex problems include hacking and information theft as mentioned earlier. It is imperative for an electronic voting system that each vote is recorded accurately and that once recorded, the data and the resultant tabulation are free from tampering. Additionally, the system must ensure data confidentiality and voter anonymity for the security of the voter. As such, results of a vote must not be readable externally and no association between the vote and voter made [17]. There should be no trapdoors that permit "maintenance" access as this could provide a means to subvert the election machine [12]. Another criterion for a secure electronic voting system is "openness". The electorate must trust that the election process is fair and that the process is transparent, the system software and hardware must be open for inspection.

The system proposed within the scope of this paper aims to eliminate the problems associated with today's voting systems. A two-stage verification process has been developed that would first identify the voter by the means of Near Field Communication (NFC) smart card and then assert the voter's identity by using fingerprint recognition. Historically, it has been observed that single verification processes like smart card authentication open up multiple lines of attacks and are susceptible to failure [18]. Thus, this two-layer authentication endeavor has been taken up. When these two passes have been complete successfully, the voter may proceed to the voting panel consisting of a set of buttons corresponding to electoral candidates. Upon holding a button, the system would record the vote digitally in the onboard storage and also, through an encrypted local area network then synchronize the record with the other voting machines. If it is discovered that the vote has been cast already elsewhere or at the same voting terminal, there would be a visual warning and the particular voter's details would be recorded for further investigation by law enforcers. After a successful vote, a visual confirmation would be provided and a thermal "point-of-sale" (POS) printer would print the vote and dispense it into a ballot box for further assurance of the voter and also to eliminate any discrepancy arising during counting. Fig. 1 illustrates the conceptual model of our system and the flowchart in Fig. 2 shows the logical control flow process.

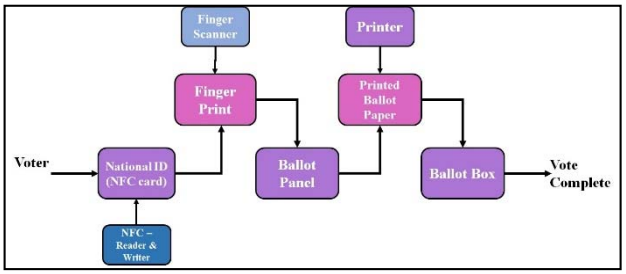

Fig. 1. Conceptual model of the system

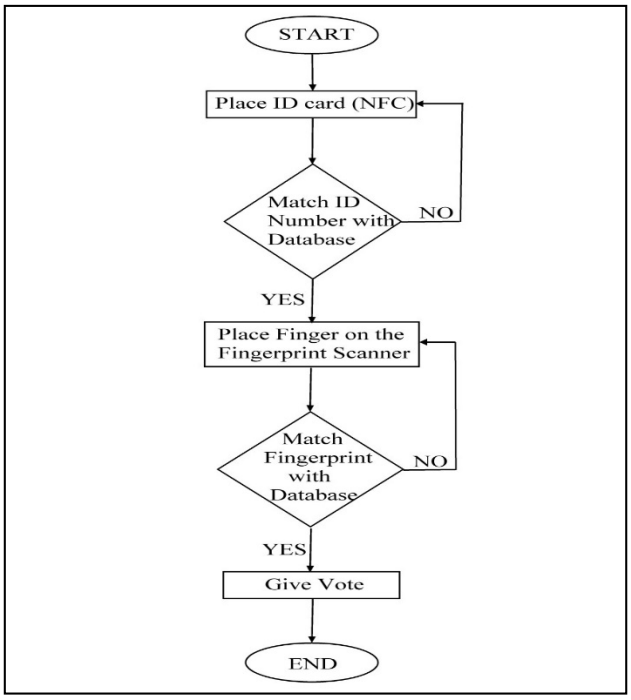

Fig. 2. Logical control flow process of the system

Due to the integration of just a local area network, through an intranet, the system does not constitute any internet coherence, thus causing the vote casted to be relatively secure from any tampering. The scope of this paper incorporates research conducted earlier and is essentially an extension of a previously developed electronic voting system that did not have the POS printer feature or the dynamically updating database [19].

III. System Design and Implementation

The complete system can be considered a package comprising of a Raspberry Pi 2 System-On-Chip (SoC) computer, an Arduino Uno R3 microcontroller board, an NFC controller module shield for Arduino, an optical fingerprint sensor, a 2.8" LCD touchscreen for Raspberry Pi, a thermal POS printer, a local area network and the voting panel. Working in tandem, these components provide the solution of a tamper resistant electronic voting system. The sections that follow describe, in turns, the functionalities of the devices and

ultimately describe how the system works together. The connection diagram in Fig. 3 illustrates how the devices are connected and the sequence diagram in Fig. 4 demonstrates the sequence in which the system is intended to perform.

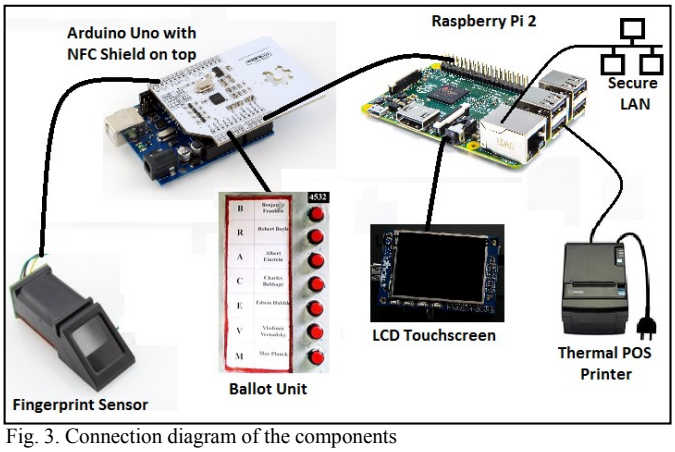

Fig. 3. Connection diagram of the components

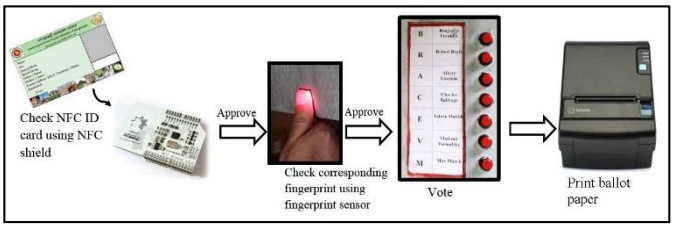

Fig. 4. Physical data flow sequence of the system

A. *Raspberry Pi 2*

The Raspberry Pi 2 SoC computer is the core constituent of the entire system and serves as the central manager of all the supporting devices. The Raspbian operating system running in the board operates SQLite, which is a lightweight database manager. A user interface has been designed using Python that provides visual instructions and confirmation through the LCD touchscreen. The Raspberry Pi board allows the integration of voter's database network, Arduino board, display panel and POS printer within the system. It connects to the Arduino through serial interface (UART), to the POS printer and Wi-Fi adapter through USB and to the LCD touchscreen through GPIO pins.

B. *Arduino Uno R3 board*

The Arduino board takes care of the NFC controller shield, fingerprint sensor and the voting panel unit. Connection to the fingerprint sensor is made with TTL serial interface and to the voting panel with I/O pins through an encoder IC. The NFC card recognition data and the fingerprint identity data is transferred to the Raspberry Pi for match with the database.

C. *NFC Controller Module Shield*

To evaluate and operate the NFC ID cards, the PN532 NFC controller shield is used with the Arduino board. As the NFC cards come with a unique identification number which was used as the identification number for each voter, information carried within the card is kept discrete by encapsulating, and the data can only be manipulated during the initial set up procedure. The cards are blank at the primary stage and have to be initialized to be entered into the system. Once the card is brought into the range of the shield, through the use of the serial monitor, the information within it becomes available. To enroll a voter into the list, the corresponding identification number of each card and individual is stored into the database. Registered voters may proceed to the next step only when they have placed their ID cards within the range of the NFC shield. Once the card has been acknowledged by the device, it proceeds to check that the identification number is present in the provided database.

D. *Optical Fingerprint Sensor*

The multipurpose fingerprint sensor incorporating Principal component analysis (PCA) has the options to enroll and check different fingerprints. The enroll sketch is run to store the fingerprints into the device. Through the serial monitor each finger entered into the system for each voter is given an identification number. This number is stored into the database to the corresponding voter's identification number. During the process for checking the fingerprints, the serial monitor displays a value for the confidence level when a match has been found, which corresponds to how well the device is able to identify and match the fingerprint that has been placed. When a fingerprint match has been found within the device, the enrolled number for the fingerprint is checked with the database in the Raspberry Pi. The number obtained from the sensor and the corresponding fingerprint number of the NFC card entered earlier is matched by one to one checking. The comparison then yields a value for success that allows the voter to proceed to vote.

E. *LCD Touchscreen*

Instructions and results are displayed through a 2.8" 320x240 LCD touchscreen display. Throughout the entire voting process, the user is guided through messages on the display. Each step of the identity verification is followed up with visual confirmations on the screen. The voter's picture and name are displayed when the information of the voter's ID card and fingerprint matches. When a person attempts to cast a second vote or attempts to access another voting terminal elsewhere, he or she is presented with a warning message through the display.

F. *Thermal POS Printer*

The auto-cut POS printer connected to the Raspberry Pi prints out the confirmation of the vote to a ballot box for the added verification. The voter gets to see the process for assurance. To interface the printer into the Raspberry Pi system first we utilized Common UNIX Printing System (CUPS). This allows the printers driver to be installed onto the Raspberry Pi environment and the printer may be accessed through prompts in terminal software.

G. *Secure local area network*

The Raspberry Pi SoC computer connects to the secure local area network of the electronic voting system through Ethernet. It helps to synchronize the encrypted SQLite database containing voters' information and also the entry of the votes across other voting terminals through a secure IP network. A

network switch at each center manages the connections to every voting panel. The network switches are then connected to a central server that manages the entire voting system.

H. Voting Panel

Vote is cast through the use of buttons corresponding to each candidate's information. The prototype system produced for testing purpose consists of seven candidate choices. The buttons are connected to a decoder IC which is interfaced to the Arduino board though digital I/O pins. Each entry is stored in the database for the candidates in the election. Once a button is pressed and held down for 3 seconds, the candidate count is incremented, a beep is sounded, the POS printer prints the vote to a ballot box and then the voting process is stopped. If a voter attempts to press the button multiple times, or tries to select any other button, the buzzer will ring and as mentioned earlier, there will be a visual warning. Subsequently, when a candidate's count has been incremented, the voter's NFC identification card is encrypted to prevent any further acceptance into the system. Fig. 5 shows the voting panel sitting atop the housing that holds the Raspberry Pi, Arduino and other hardware. In the picture, to the right of the voting panel, we can see the POS printer.

The process of entering an individual into the EVM system consists of running the program for enrollment. The individual is provided with an NFC ID card, whose credential is identified and stored alongside the person's name. Next the user's fingerprint signature is recorded using the fingerprint sensor into the database. Next the user's fingerprint signature is recorded using the fingerprint sensor into the database. A picture of the individual is also taken and stored in the database

IV. System Testing and Evaluation

To assess the functionality of the EVM, we made twenty different entries to the systems using twenty NFC cards as prototype national voter ID cards. These ID cards were assigned to each person and their corresponding information and fingerprint ID were entered into the system. For the test, the candidates for votes were listed as Candidate 1, Candidate 2, and so on where the first button corresponds to Candidate 1 and like so. To check the accuracy of the fingerprint device a total of twenty fingerprints were stored in the fingerprint sensor's memory. The confidence level received for the each of these fingerprints was collected in a total of twenty-five experimental trials. The graph in Fig. 6 shows the trend of the confidence level with the number of trials. When plotted for the best line, a linear curve with confidence level of higher than 100 was received as illustrated in Fig. 7. This demonstrates a good accuracy and the reliability of the fingerprint sensor.

Fig. 5. The voting panel (left) along with the POS printer (right)

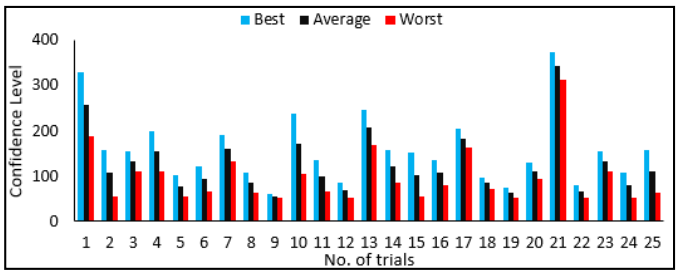

Fig. 6. Fingerprint recognition confidence level vs. number of trials

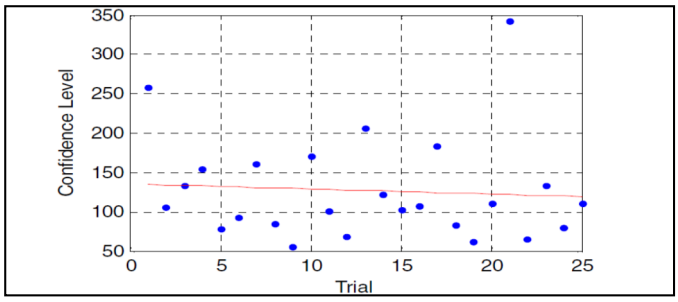

Fig. 7. Line of best fit of confidence level vs. number of trials

The test for the system's usability and user-friendliness was determined by carrying out a survey among a group of selected people. On a scale of 1 to 10, feedback was taken from 10 participants. Table I shows the scores obtained from the test. It is evident from the modal score of 6 on usability that most users found the system to be fairly usable. On the other hand, the highest frequency score for user friendliness was 8, indicating that the system is highly user-friendly.

TABLE I. Feedback on System's Usability and User-Friendliness

Participant	1	2	3	4	5	6	7	8	9	10
Usability	6	6	5	7	6	8	6	7	6	7
User-Friendliness	8	8	6	8	6	7	6	7	8	8

V. Conclusion

It is needless to mention that the concept of electronic voting systems is not a novel theory. The endeavor taken up under the limited scope of this research aims to demonstrate an implementation for fault free voting and dictate a much larger scale of the voting frontier. Thus the machine still has certain limitations that may need to be overcome to allow it to reach the level it is aimed for. The devices integrated in this prototype need to be upgraded to more robust and durable alternatives for large scale production. For example, with the fingerprint device we used, a total of 256 fingerprints may be stored, but for mission critical scenarios, an industry grade fingerprint scanner needs to be used that can be linked to a dynamic database. In a future version, the buttons on the voting panel can be completely replaced with a touch responsive Graphical User Interface. The obvious advantage of biometrics is that it cannot be altered or copied and the window of impersonation is nullified. To allow transparency with the user of the system, the printer provides a brief view of the ballot that is printed out after the vote is casted. The advantage of not handing out a ballot to the user means that

the voter is not able to manipulate or misplace the vote. Ballots stored in the ballot box also means that the electronic tally of votes received by each candidate can be cross checked with the count of paper ballots.

Overall, the system shows an attempt towards better confidence of electronic voting machines. The integrated system eradicates common issues faced and ensures both voters and candidates a trusted means for elections. The proposed system was developed under 200$. Through incorporations of numerous devices, it can alleviate the satisfaction of all parties involved in an election.

REFERENCES

[1] G. S. Heiberg, P. Laud & J. Willemson, "The application of i-voting for Estonian parliamentary elections of 2011." *E-Voting and Identity: Springer Berlin Heidelberg*, Vol.7187, pp. 208–223, 2012.

[2] I. V. Blankenship, 'Trusting the Machine: Inherent Problems with Electronic Voting Systems', *Global Information Assurance Certification Paper*, 2004.

[3] Bellis, "The History of Voting Machines - History of the Voting System Standards Program", *About.com Inventors*, 2015. [Online]. Available: http://inventors.about.com/library/weekly/aa111300b.htm.

[4] S. Everett, "The Usability of Electronic Voting Machines and How Votes Can Be Changed without Detection," PhD dissertation, Rice University, 2007.

[5] C. Burton, C. Culnane, J. Heather, T. Peacock, P. Y. A. Ryan, S. Schneider, S. Srinivasan, V. Teague, R. Wen and Z. Xia "A supervised verifiable voting protocol for the Victorian Electoral Commission", *Proc. 5th International Conference on Electronic Voting*, 2012.

[6] Davis and S. Thomas, "Direct recording electronic voting machine and voting process", US5583329 A, 1996.

[7] F. S. Wood, "Electric voting-machine", U.S. Patent 616,174, Granted Dec. 20, 1898.

[8] J. Fried and A. Lee, "Study On Open Source Voting Systems", Draft Report, *San Francisco Local Agency Formation Commission*, 2015.

[9] Wikipedia, "Electronic voting", 2015. [Online]. Available: https://en.wikipedia.org/wiki/Electronic_voting.

[10] A. Boyle, 'Pentagon launches Internet voting effort for overseas Americans', *MSNBC*, 2003.

[11] D. Jefferson, A. Rubin, B. Simmons, and D. Wagner. "A Security Analysis of the Secure Electronic Registration and Voting Experiment (SERVE)". Technical report, 2004.

[12] GIAC Security Essentials Certification, "Trusting the machine: inherent problems with electronic voting systems", *Global Information Assurance Certification Paper*, 2004.

[13] CNN WB, 'Pentagon halts Internet voting system', 2015.

[14] L. Landes, 'Internet Voting -- The End of Democracy?', *Dissident Voice*, 2003.

[15] D. A. Gritzalis, "Secure electronic voting.", *Dordrecht: Kluwer Academic Publishers*, 2003.

[16] M. M. Sarker and M. N. Islam, "Management of sustainable, credible and integrated electronic voting (E-Voting) system for Bangladesh," *Management of Sustainable Development*. Vol. 5, pp. 15–21, 2013.

[17] P. G. Neumann "Security criteria for electronic voting", *Proceedings of the 16th National Computer Security Conference*, pp.478–481 1993.

[18] R. Newman, "Security and Access Control Using Biometric Technologies: Application, Technology, and Management" (1st ed.), *Course Technology Press*, Boston, MA, United States. 2009.

[19] S. Hasan, A. Anis, H. Rahman, J. Alam, S. Nabil and M. Rhaman, "Development of electronic voting machine with the inclusion of Near Field Communication ID cards and biometric fingerprint identifier", *2014 17th International Conference on Computer and Information Technology (ICCIT)*, 2014.