Android Based Smart Voting Machine (SVM)

Tawseef Mahmood, Shamah Mahbub Zoha, Ashis Kumar Das and Amitabha Chakrabarty
Department of Computer Science and Engineering
BRAC University, Dhaka, Bangladesh
tawseefmahmood@gmail.com; shamah1992@gmail.com; akd.bracu@gmail.com; amitabha@bracu.ac.bd

***Abstract*—The process of efficient voting is a vital component in the proper functioning of our increasingly-modernized society. The traditional way of conducting a voting process is not only time-consuming, but also prone to security issues and election rigging, as well as being outdated and wasteful. For this purpose, Electronic Voting Machine or EVM was introduced which addressed some of the issues while having limitations of its own, such as its scope of application and its inherent limitation of being a mere electronic device, prone to malfunction and other mechanical issues[1]. Hence, there is a need for a system that would build upon that concept as well as being more compact, elegant and cost-effective, while at the same time capable of catering to a broader range of populace, whilst maintaining fairness and impartiality all the time. The Android-Based Smart Voting System that we propose will simplify the voting process by considerably reducing the steps for voting and increasing overall throughput, keeping interaction between voters and the system easy and understandable, as well as eliminating unnecessary and costly hardware that have no overall impact on the final outcome, thus providing for a smarter and more feasible solution.**

***Index Terms*— Fingerprint, Biometric template, Arduino, Android Smart phone, Database, Security, Scanner, Thermal Printer.**

I. Introduction

The process of electing a leader who'll be responsible for carrying out the will of the normal populace is one of the most crucial and fundamental elements that comprises a democratic society[2]. Voting is an exercise of power and sovereignty; a powerful tool to show not only approval, but also displeasure if needed and firmly establishes the control of fate in the hands of its people. As societies progress, new complexities arise which make conventional methods of voting more and more difficult. Relying on physical ballots alone is no longer an option [3]. As a result, there has been a gradual shift towards electronic methods in conjunction with traditional, physical methods to preserve the legitimacy and integrity of the voting process, similar to the approach adopted by India [4]. Additionally, there has always remained dispute concerning the voting process and the outcomes derived from it throughout recorded history. There is a distinct lack of trust permeating throughout. Some issues have been addressed over time, but there has never been a completely sound approach that would win back the lost trust among the voters. Therefore, it has become more important than ever to devise a system that would make the process of voting stripped to the bare essentials while still remaining robust and fail safe.

A. Motivation

The last major election that was hosted in Bangladesh occurred in 2014, with 47,262,168 votes being cast from a total of 92,007,113 registered voters, an astronomical amount which represented a significant obstacle in ensuring efficiency and complete impartiality, as the population growth continues to increase exponentially [5].

With such an upsurge in population increase, the next elections in the country will become progressively challenging, as newer and newer voters are introduced and keeping track of each and every vote becomes time consuming and inefficient. As such, credibility and integrity of the whole political landscape may be affected, as questions about the practicality of traditional methods and vote manipulation methods pop up. As a result, the Smart Voting Machine or SVM has been conceived that will take on this enormous challenge and deliver the desired results, all which while ensuring maximum security and maintaining the upmost credibility.

II. System Architechture

The tasks that the Android-based Smart Voting System shall undertake can be broadly classified into three functions; firstly, taking the fingerprint of the user as input to authenticate users and their type; secondly, the actual voting process after the user is verified, and finally, producing a physical output, a printout of the vote cast by each voter, to serve as evidence of their respective votes, which is to be placed in a physical ballot box to maintain its credibility.

A. System Overview

Our system comprises of two layers; software and hardware. In the software layer, we have an interface which provides access to two types of users; administrators and general voters. The administrators can be divided into two subclasses as well - administrators and super administrator. The two levels of administrators have different levels of access of the administration panel, as shown in Figure 1. The system application takes the fingerprint of the user, verify whether the user is an administrator or a voter by matching the prints against the database entries stored in the Android device, and then open the appropriate panel. If the values of the fingerprints do not match, access is denied to the system. The administrative panel provided to the administrators will have the provision to either access the admin panel, or when the voting process is in effect, will display an option to vote as well, if the administrator is assigned to the voting center in context. In the admin panel, administrators will have special features such as registering new voters or removing existing voters, activate or deactivate the voting process, and the like. The process of activating or deactivating the voting process cannot be done by a single administrator. At least three members of the administrative panel have to authenticate in order to start or stop the voting process. The voters in turn will have access to the ballot upon fingerprint submission where they can cast their vote. This vote is stored electronically in the database and the voter can obtain a physical copy with the help of a thermal printer. This physical copy is then dropped in a physical ballot box by the voter, which will add a final level of credibility to our system.

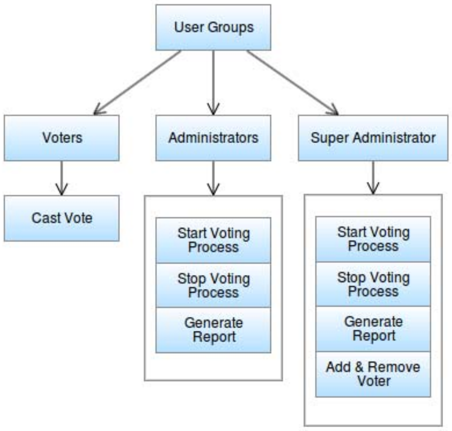


Figure 1. User Groups of the System

In the hardware layer, careful thought has been undergone to ensure the minimal hardware to be used in the system, so that hardware redundancies are minimized, as well as reducing the complexity of operating the system, to facilitate usage by normal users, as opposed to highly specialized ones. All the connections used in the system are serial (TTL), so that security hacks that can occur with wireless connection is eradicated. Moreover, our system utilizes a fingerprint scanner which can convert user's biometric fingerprint impression to proprietary binary template; which cannot be used with any other scanners, allowing us to ensure better level of performance and much more reliability of the system, over other fingerprint verification processes, such as minutiae extraction [6].

However, the limitation of the scanner we used was that it can only store 200 fingerprint templates in its physical memory. This is impractical when it comes to an application which is as vast as an election process, in which a huge number of people take part to cast their votes. This was tackled through using our Android application, where the templates are stored in a database, in the internal memory of the device, and are uploaded into the scanner when required, breaking the barrier of the limited number of templates that can be stored.

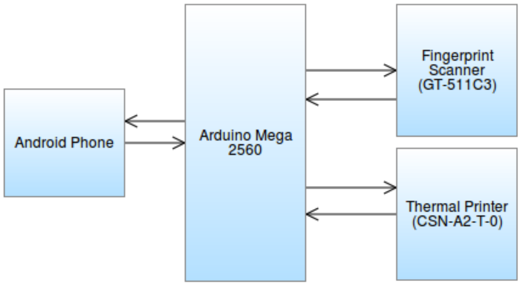


Figure 2. Architecture of the System

The Android phone, on which the application software is running, is connected to a central Arduino microcontroller unit, which maintains the communication between the phone and the hardware components. The fingerprint scanner, as well as the thermal printer, is connected to the Arduino board and the board is responsible for driving the hardware components. The Arduino board has customized device drivers, which controls the scanner and the printer, as per the command transmitted from the Android device. When the voter comes in to cast his or her vote, he or she has to enter their fingerprint for biometric verification. This is achieved by the fingerprint scanner, which scans the fingerprint image, converts it to a binary biometric template and then stores it in the buffer of Arduino. The Android phone then transfers the existing templates that are stored in its database to the Arduino device, to set them in the fingerprint scanner, where the verification process will be performed. The templates that are transferred are then matched against the recorded template to verify the user. Furthermore, when a voter is added to the database, the fingerprint scanner helps to enroll the voter's biometric information by taking the fingerprint impression and then convert it to a binary biometric template. This template is then transferred to the Android device through Arduino micro controller and is stored in the database.

The system also includes a thermal printer, which is very compact in size and utilizes TTL serial protocol, making it easier for us to interface it with our existing system. This printer is used to obtain a physical ballot paper after the user has casted his or her vote, such to ensure the credibility of our system, with a physical evidence. Our system prints the monochrome image of the entity symbol at the end of the voting process, along with a timestamp and a randomized number, and this physical copy will be placed in a physical ballot box, which can be used later as evidence toward casted vote.

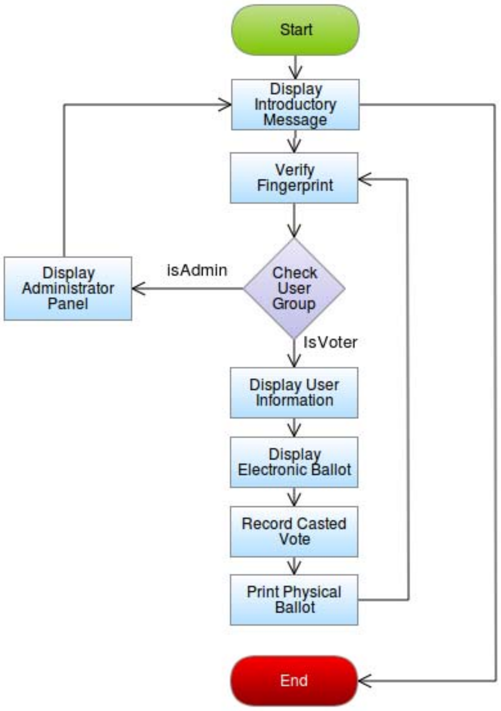


Figure 3. Flowchart of the Application

B. *Hardware Specification*

1) Fingerprint Scanner

The fingerprint scanner used for the system is TTL-(GT-511C3)[7]. This model has been chosen for reliability and for cost considerations. This scanner will be attached to the Arduino board using a JST SH Jumper 4 Wire Assembly[8].

2) Arduino

Arduino Mega 2560[9] is chosen among other microcontrollers, due in part to its comparatively large RAM. The board will act as the interconnecting, processing part of the system, passing data through it, sent to and received from other peripherals, communicated by its bundle software package.

3) Android Device

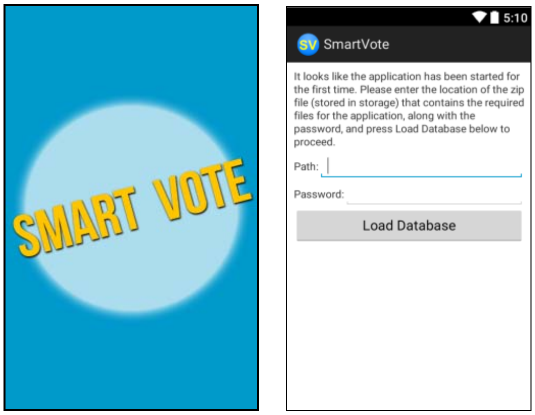
Any smart device powered by Android Operating System can be used for the system, which is version 4.0 or above, with minimum 512 MB of RAM. The database is stored in the device and is connected to Arduino for communication with the other peripherals.

4) Thermal Printer

A highly specialized, low-cost, small-sized unit that will print a monochrome bitmap image of the symbol of the voting party in question, completing the final task of producing a tangible print for credibility purposes [10].

III. SYSTEM FLOW

Once the application is run on the Android device, the user is greeted with a Splash screen, beneath which the connection with Arduino is established and the database files are checked. If some files are missing, the Load Database screen is displayed.



It looks like the application has been started for the first time. Please enter the location of the zip file (stored in storage) that contains the required files for the application, along with the password, and press Load Database below to proceed.

Path:

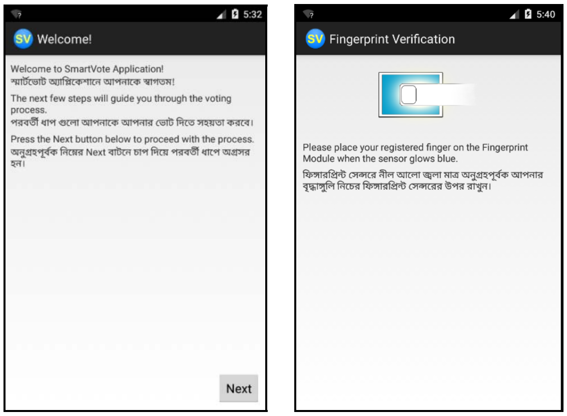
Password:

Figure 4. Splash and Load Database Screen

In the load database screen, the user - super administrator, in this case - is required to provide the path of a password-protected zip file, along with a password. Once the user presses the "Load" button, he has to verify his fingerprint through the scanner and proceed to the next step.

If the super administrator is verified, he is directed to the administrator panel.

However, if the files are already available in the application's data directory, then the user is greeted with the welcome screen, where they are given a brief instruction about the application. Upon pressing "Next", they are forwarded to the Fingerprint Verification screen, where the live impression of their finger is obtained using the scanner.



Welcome to SmartVote Application!
স্মার্টভোট অ্যাপ্লিকেশানে আপনাকে স্বাগতম!

The next few steps will guide you through the voting process.
পরবর্তী ধাপ গুলো আপনাকে আপনার ভোট দিতে সহয়তা করবে।

Press the Next button below to proceed with the process.
অনুগ্রহপূর্বক নিম্নের Next বাটনে চাপ দিয়ে পরবর্তী ধাপে অগ্রসর হন।

Please place your registered finger on the Fingerprint Module when the sensor glows blue.

ফিঙ্গারপ্রিন্ট সেন্সরে নীল আলো জ্বলা মাত্র অনুগ্রহপূর্বক আপনার বৃদ্ধাঙ্গুলি নিচের ফিঙ্গারপ্রিন্ট সেন্সরের উপর রাখুন।

Figure 5. Introduction and Fingerprint Verification Screen

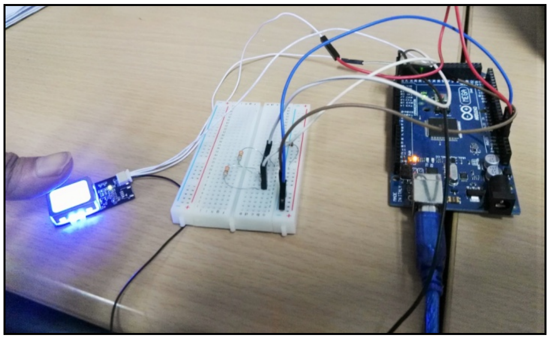
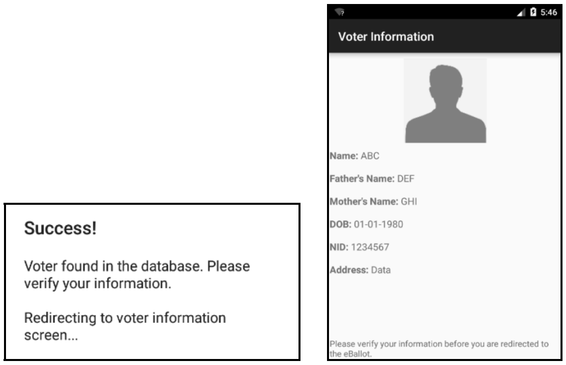


Figure 6. Live Fingerprint Scanning

If the user's fingerprint matches one of the entries in the database, then the user is shown a confirmation window, followed by a user details screen, that lasts for 10 seconds.



Success!

Voter found in the database. Please verify your information.

Redirecting to voter information screen...

5:46

Voter Information

Name: ABC

Father's Name: DEF

Mother's Name: GHI

DOB: 01-01-1980

NID: 1234567

Address: Data

Please verify your information before you are redirected to the eBallot.

Figure 7. Success Dialog and User Details Screen

The voter then finds the eBallot screen, where they can vote for their desired candidate. The list provides the voter with candidate name and entity symbol (not displayed in the current revision) and they may cast their vote by long pressing the item on the list. A confirmation dialog is displayed to validate the user's selection.

Upon casting vote, the user will be displayed a success screen, while the printer will print the image of the entity, along with a timestamp and a system-generated, unique random number. The application will then automatically move to the Introduction screen, allowing the next voter to cast their vote.

IV. SECURITY

The design of our proposed voting system is modeled in such a way that it satisfies various security concerns which are normally found in an ordinary voting process. By using a biometric verification approach to allow voters participating in voting dismisses the probabilty of casting illegal votes. Avoiding wireless communication between hardware subsystems directly makes it strongly defensive to illegal remote access. Moreover the inclusion of both the vote casting timestamp and the unique system-generated random number printed on the physical ballot paper directly leads our system to a trustworthy and well-balanced voting machine in terms of security and reliability.

V. CONCLUSION

This paper proposes a smart voting system which is reliable, cost-effective, secured and efficient enough to be used in various practical scenarios where an impartial voting solution is required. This system also offers an ideal solution to those voting scenarios where the number of voters is very high, it would be hard to manage a large numbers of voter information manually.

With addition to this, our proposed system also offers a biometric voter verification system, by which security and reliability is guaranteed to an acceptable level. In conjunction to the biometric authorization, the usage of thermal printer brings transparency and reliability to the overall voting process.

REFERENCES

[1] Anis, M. A., Rahman, H., Alam, J. S., Nabil S. I. and Hasan, S. M. 2014 Development of Electronic Voting Machine with the Inclusion of Near Field Communication ID Cards, Biometric Fingerprint Sensor and POS Printer: http://dspace.bracu.ac.bd/bitstream/handle/10361/3967/ThesisReportFinalv1.pdf?sequence=1

[2] The Importance of Voting in a Truly Democratic Society. 2010: http://vibeghana.com/2011/01/28/the-importance-of-voting-in-a-truly-democratic-society/

[3] Jones, D.W. 2001. Problems with Voting Systems and the Applicable Standards: http://homepage.cs.uiowa.edu/~jones/voting/congress.html

[4] Ford, M. 2014. Indian Democracy Runs on Briefcase-Sized Voting Machines: http://www.theatlantic.com/international/archive/2014/04/indian-democracy-runs-on-briefcase-sized-voting-machines/360554/

[5] International IDEA , Voter turnout data for Bangladesh: http://www.idea.int/vt/countryview.cfm?CountryCode=BD

[6] Mazumdar, S. and Dhulipala, V. "Biometric Security Using Finger Print Recognition", University of California, San Diego.

[7] ADH Tech GT-511C3 Fingerprint Scanner: http://www.adh-tech.com.tw/?22,gt-511c3-gt-511c5-%28uart%29

[8] JST SH Jumper 4 Wire Assembly: https://www.sparkfun.com/products/10359

[9] Arduino Mega 2560: https://www.arduino.cc/en/Main/ArduinoBoardMega2560

[10] Sparkfun Thermal Printer (CSN-A2-T-0): https://www.sparkfun.com/products/10438