

Application of Biometrics in Mobile Voting

Donovan Gentles¹, Suresh Sankaranarayanan^{2,3}

¹Mona Institute of Applied Sciences, University of WestIndies, Jamaica
dongen02@gmail.com

²Computing & Information Systems, Institut Teknologi Brunei, Brunei

³Department of Computing, University of WestIndies, Jamaica
pessuresh@hotmail.com

Abstract — Voting process in today's era is behind its time in respect of the usage of modern ICT. The voting process is being seen mostly as a manual and paper based one. This process can be overwhelming, time-consuming and prone to security breaches and electoral fraud. Over the years technology related systems were being developed to resolve some of the issues like electoral fraud, impersonation, double voting etc. One such system is Electronic based voting that has been actively used for voting in countries like India. However, these systems seem to be prone to electoral frauds and voters have to make tremendous effort to cast their ballots. There are still a few very important areas which have to be identified and addressed viz., the Security which involves a person be able to vote in a secure manner, the time spent for voting by voters, the efficiency in counting of votes and the cost involved in employing people towards monitoring the voting process. So taking these areas/issues into consideration we have now come with the biometrics authenticated mobile voting system, to start with for a country like Jamaica. The technology being proposed now is novel and the first of its kind proposed at present. It is proposed that using fingerprint supported biometric control information and encryption along with Secure Socket Layer i.e. SSL using VeriSign, would make the software involved in the voting process well secured. In addition tying the credentials to a mobile device will make the system even more robust. We have considered the mobile equipment for the present system development, a smart phone using Android 3.0 (Honeycomb). The details of the proposed development are presented in this paper.

Index Terms — Electronic voting, Mobile Voting, SSL, Android 3.0

I. INTRODUCTION

The voting process in today's context is behind its time in respect of the usage of modern ICT as seen by experience. The voting process begins with persons manually going to an election office showing proof of address and then a national identification card (Id) will be issued for getting the authentication during the actual process of voting at the polling booth/station. With this, a voters' list will be generated for each constituency. Each voter will then have to go to a polling station where they

believe that their names are made available and if so after authentication with their Id, they will cast their vote by placing a mark against the political party symbol of their choice. In some cases, on the voter's right thumb/index finger, an indelible ink mark is made to show that this person has already voted and so the voter cannot vote again. After the voting schedule is complete, booth officials will then take the ballot boxes to a centralized place, then declare the voting results by manually counting the votes polled, and tally the counts. In some cases, there may be some need for a recount of ballot papers polled also due to discrepancies. These processes are often lengthy, tedious, inaccurate, and risky and in some cases the final count may get skewed and end up in court cases also. This manual process leaves scope for errors to creep in, political dishonesty and political fraud, which is seen through the voicing of their feelings by people in the media in many countries using these systems.

In countries that are better developed like in India, electronic voting (e-voting) is made possible and this technique encapsulates both electronic means of casting of votes and also counting of votes [1]. This process cleared up lots of problems and barriers faced by the paper based voting process explained above. But problems of long lingering lines of voters on the day of voting to cast their votes still persist and consequently not enough persons come for voting thereby neglecting their civil rights. Another reason for the lack of participation is that of security and the fear that they may be bullied into voting for someone that they don't wish to vote and cases have been reported in the media regarding political riots during the polling day. Another important reason is impersonation, voting by somebody before the actual person arrives in the polling booth for voting. These are just a few reasons why persons may be reluctant to exercise their rights to vote on the polling date.

With all these problems in mind, we here propose a novel Mobile voting technique [2][3] for Jamaica at the first instance, with the hope that this Biometric based technology will erase the above issues. Our reported research focuses on the application of mobile technology with the use of biometrics encryption for authentication. The paper is organized in sections as follows. Section 2 provides details on some of the Electoral Methodologies currently in vogue. Section 3 gives details on Fingerprint matching and Security authentication schemes. Section 4

gives details on the Biometric based Mobile voting technology being proposed. Section 5 gives the implementation and validation details using Android 3.0.2 and Section 6 is conclusion and suggestion for future work.

II. ELECTORAL METHODOLOGIES IN VOGUE

A. Paper Based Process

The process, which is involved in the paper-based electoral system in Jamaica, is a rigorous one [4]. First, all persons who are eligible to vote (normally eighteen years of age or older) should be a citizen of the country. These persons will have to go and get enumerated six months in advance after which the election workers will visit their residential addresses to ensure first that those persons actually live there and ascertain that they have given the correct information about themselves. After validation, a voter's Id will be issued. The complete procedure involves lot of paper work. Appropriate training will have to be provided for the staff members in charge of polling duty. During the day of polling, the concerned staff members are required to be present half hour prior to the opening of the polling booth/station to check that all arrangements have been done correctly. On the day of polling, the Officer in charge has to ensure that a final checklist includes but not limited to:

- *Ensure that polling stations are in contact*
- *Ensure that security forces are notified – liaise with head of their division.*
- *Ensure that all Presiding Officers and Poll Clerks are clearly identified for established polling stations.*

After voting, the counting of ballots will be looked after by another group of officers [4]. With all these steps, groups and procedures that are involved, the process can prove to be tedious, error prone and costly. Some introduction of technology currently in the Jamaican system, however, makes the process semi-manual, but this is far from what could be really accomplished by a fully ICT driven process. The semi-manual process only allows the government to store voters' information on a database, which can be retrieved on a computer on the election date to facilitate faster searches.

B. Electronic Voting

Electronic voting (also known as e-voting) encompasses both electronic means of casting votes and counting of votes. It can include punched cards, optical scan voting systems and specialized voting kiosk, transmission of ballots via telephones, private computer networks or the internet [1]. There are different types of electronic voting systems with the advent of technology to avoid electoral frauds like paper based electronic voting, Direct Recording Electronic Voting, public network Direct Recording Electronic Voting

C. Paper-based electronic voting system

This system is sometimes called a "document ballot voting system" [1]. Paper-based voting systems originated as a system wherein votes are cast and counted by hand, using paper ballots. With the advent of electronic tabulation systems, paper cards or sheets could be marked by hand, but counted electronically.

D. Direct Recording Electronic Voting System (DRE)

A direct-recording electronic (DRE) [1] voting machine records votes by means of a ballot display provided with mechanical or electro-optical components that can be activated by the voter - typically buttons or a touch screen; that processes data with computer software; and that records voting data and ballot images in memory components. After the election, it produces a tabulation of the voting data stored in a removable memory component and as printed copy. The system may also provide a means for transmitting individual ballots or vote totals to a central location for consolidating and reporting results from precincts at the central location.

E. Public network DRE voting system

A public network DRE voting system [1] is an election system that uses electronic ballots and transmits vote data, from the polling place to another location over a public network. Vote data may be transmitted as individual ballots as they are cast, or periodically as batches of ballots throughout the Election Day, or as one batch at the close of voting. This includes Internet voting as well as telephone voting. Public network DRE voting system can utilize either precinct count or central count method. The central count method tabulates ballots from multiple precincts at a central location.

Internet voting can use remote locations (voting from any Internet capable computer) or can use traditional polling locations with voting booths consisting of Internet connected voting systems. Corporations and organizations routinely use Internet voting to elect officers and Board members and for other proxy elections. Internet voting systems have been used privately in many modern nations and publicly in the United States, the UK, Switzerland and Estonia.

F. Smart Card in Voting

With the use of the smart cards and kiosk there was a significant leap in voting technology, as persons were able to vote within their own comfort zone or that was the intension. The need for the various human security bodies was eliminated. However, everyone who is eligible to vote would have to have a pre-program smart card. The voting Kiosk is where all the action is located. To start, the voter must place the voter token into the slot. The voting kiosk will seize this token until the voter has successfully voted. After the token has been seized, the kiosk will verify that this token is valid authentic, this is done by looking at the RV signed token, timestamp and the polling site id [5]. This system however, has flaws on security aspect and voters could vote multiple times. In

addition, persons may have to stand in long queue to cast their votes.

Taking the above aspects into consideration, we here propose a Biometric authenticated Mobile voting system [2][3] for Jamaica in the first instance, which would use authentication using Fingerprint and voting using the mobile device id i.e. IMEI number, as main security mechanisms. Now before going into the details of this proposed system, we would briefly review security schemes that would be used for mobile voting.

III. FINGERPRINT MATCHING AND SECURITY SCHEMES

Fingerprints are graphical flow-like ridges present on human fingers [6][7]. Fingerprint identification is based on two premises: (i) fingerprint details are permanent – based on the anatomy and morphogenesis of friction ridge skin, and (ii) fingerprints of an individual are unique. In order to perform matching, it is critical that an understanding of the structure and features of the fingerprint is obtained.

The lines that flow in various patterns across a fingerprint are called ridges and the spaces between ridges are called valleys. The more microscopic of approaches is called minutia matching. The two types are, ridge ending and bifurcation. An ending is a feature where a ridge terminates and a bifurcation is a feature where a ridge splits from a single path to two paths say a Y-junction. Since fingerprints are permanent as discussed above, if they were intercepted during communication or retrieved from an endpoint because of poor security, a perpetrator could effectively fake their identity, pretending based on false biometrics. Therefore, good security schemes are extremely important to protect this biometric data. There are numerous cryptographic schemes and algorithms available however, this research is specifically interested in a certificate based authentication and trust, HTTPS, and AES symmetric key encryption, which are discussed below.

X.509 certificate is a signed record that associates users' identification with the cryptographic keys and the framework postulates that everyone will obtain certificates from an official certifying authority (CA) usually a Trusted Third Party (TTP). One such company is Verisign, which provides Secure Socket Layer (SSL) Certificates and more in a single solution. They have been providing the service since 1995. Over the years, users of websites have grown to trust the websites that bares the logo of a SSL Certificate Company. The public-key certificate consists of a data part and a signature part. The data part consists of the name of an entity, the public keys corresponding to that entity, and additional relevant information including the validity period for the public key and so on. The signature part consists of the signature of a TTP over the data part [8]. Hypertext transport protocol secure (HTTPS) is a technology where Secure Socket Layer (SSL) or Transport Layer Security (TLS) is applied as a sub-layer over HTTP. HTTPS automatically encrypts and decrypts data during communication

transfer. SSL is designed to make use of TCP to provide a reliable end-to-end secure service [9].

The National Institute of Standards and Technology (NIST) worked with the cryptographic community and developed Advanced Encryption Standard (AES). The overall goal was to develop a Federal Information Processing Standard (FIPS) that specifies an encryption algorithm capable of protecting sensitive (unclassified) government information [10]. The Irondale proposal for AES was accepted by NIST and defined a cipher in which the block length and the key length can be independently specified to 128, 192 or 256 bits. The AES specification uses the same three key size alternatives but limit the block length to 128 bits.

IV. BIOMETRIC BASED MOBILE VOTING

As stated by Mobile Marketers, voting by mobile could become a reality by 2012, according to one of the leading mobile messaging companies [11]. Very few researches have been carried out on mobile voting. One such system proposed [12] is where the voting machine works on an embedded system with a touch pad and a memory unit kept at the main office. In another development, a voter is identified using a wireless certificate without additionally registering [13] when a user votes using his mobile terminal such as a cellular phone or a PDA.

It may be mentioned here that there has been no published research material on Mobile Application based Voting using biometrics and cryptography that enforce security and confidentiality of voter, which cannot be altered. So with this as background a Biometric authenticated Mobile voting system [2][3] is being proposed here that will be solely based on mobile technology from the client side, powered by the use of Android (3.0) and VeriSign for trusted SSL Certificate, and integrated secure access level databases from the server side. The secure use of biometrics encrypted information and access control to secure database will produce the resolution needed. This proposed system will utilize a GSM mobile system, which consists of a GSM SIM card. The Android operating system will be used in conjunction with the mobile device. The mobile device will be sensitive to capture biometrics information, for example high tech camera and scanning capabilities to capture ridges of the fingerprints. Each voter will be assigned to a mobile device hence government would have tied their biometrics information to the device at the time of verification. To store and manage data in an accurate and secure way, the government database will use Microsoft Sql Server as the database. The database architecture will be separated into two levels. There will be two levels of Servers also.

- **Constituency level database (Level 1):** This database will be able to view data pertaining to voters and politicians within the respective constituencies. Each constituency will have the same database architecture structure. The Constituency level database will allow ballot casting and counting. This will make the counting of ballots easier. Authentication and

verification towards mobile device identity of the voter will be done at the constituency level. Only voters found in a particular constituency database will be allowed to vote in that constituency. Constituency level database can validate the address of the voter and communicate to Main electoral database, which updates it against the voter id. The same applies for Mobile device identity too.

- **General or main level Database (Level 2):** This database in the Architecture is called the General (or main) Database. This database is like a watchdog. It monitors the validity of the information it captures like the Fingerprint and Voter id. It also stores voters and politicians' information for all constituencies. It communicates with all the constituency level databases to ensure that person doesn't vote in more than one constituency. And it tallies all the votes by constituency.

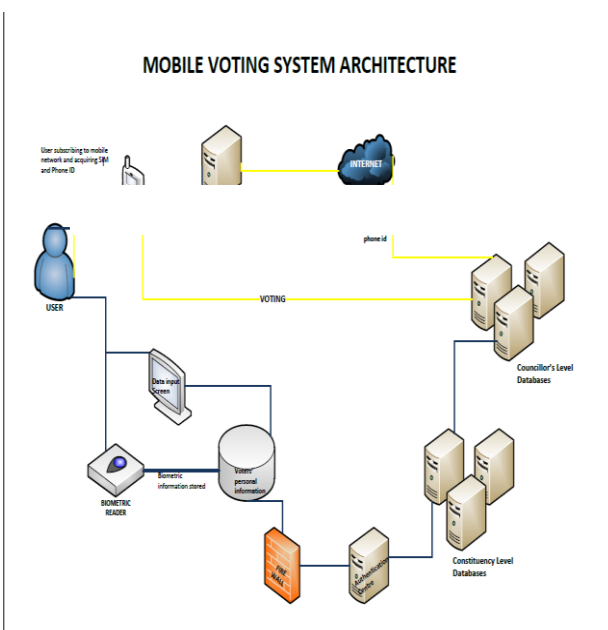


Figure.1 Architecture of the proposed Mobile Voting System

The Architecture of the proposed system is shown in Fig.1. The user will have to acquire the service of a smart phone. For the purpose of this research, the smart phone must be compatible with the Android 3.0 Operating System. The mobile company will register the SIM and phone identity to the individual. Users will register their information at the central government database level. This said level represents the Authentication Centre. Users will be authenticated at the Authentication Centre. Voters will go to their constituency office and get their fingerprints scanned along with the verification of residential addresses and other personal information. This information will be authenticated at the Authentication Centre. The internet along with the use of second generation (2G), third generation (3G) and fourth generation (4G) mobile technology will be used for networking in order to effectively make this system successful. With that said it is of utmost importance that

the system should be highly secured. The biometric data, cryptography and the use of a secure socket layer technology will enforce the level of security needed. The following steps outline the process of mobile voting system which is been depicted as flowchart in Fig.2. The details on implementation are discussed in the following sections.

- Voters and prospective voters will open the application without the security and login requirements.
- If the user intends to register then they will be connected to the server using TCP connection. However the only thing they will be allowed to do at this point is registration.
- If the users have already registered and authenticated by their finger-prints then they can login using their respective finger-prints and voter's id.
- If the user wants to register then a screen to capture personal information will appear. The form will ask the user to enter name, date of birth, tax registration number (TRN) for the case of Jamaica and address. To capture the address Google maps is used in the code available in order to facilitate faster and more accurate searches.
- A user also has the option to change his/her information such as phone information (in the case of a lost or stolen phone), and also address information. To get access to this functionality, users will have to supply finger-prints and voter's ID.
 - The fingerprint information is encrypted and sent to the government server along with the voter's ID. (The government server also has an encryption algorithm which is identical to encrypt finger-prints to make a match)
 - If the person chooses to register then information is stored on the government databases and the server but they are not allowed to vote or make changes to any information given until all information are verified and then authenticated by submission of finger-print in person.
 - After the user has submitted the correct finger-print from the correct phone and also provide the correct voter's ID then the server will authenticate the voter. After which the voter is now permitted to vote.
 - When the voter casts his/her vote then voter status will be changed and also the party count will increase as per the voter's choice. The voter's identity however will not be tied to the party which he/she voted for
 - This information is then stored on the government server and databases.

V. IMPLEMENTATION USING ANDROID 3.0

The implementation of the above proposed Biometric based Mobile voting system [2][3] was carried out using

Android 3.0 [19]. Details on the technologies used will be discussed in brief before going into the implementation details.

Android [14] is a mobile operating system for mobile devices such as mobile telephones and tablet computers developed by Google Inc and the Open Handset Alliance. Android has seen a number of updates since its original release. These updates to the base operating system typically fix bugs and add new features. The version history of the Android operating system began with the release of version 1.0 in September 2008. Android 3.0 is a new version of the Android platform that is specifically optimized for devices with larger screen sizes, particularly tablets. It introduces a brand new, truly virtual and “holographic” UI design, as well as an elegant, content-focused interaction model. With the Android Honeycomb it offers all the tools developers need to create incredible visible interaction experiences on the devices, which includes but not limited to:

- New UI framework for creating great tablet apps
- High-performance 2D and 3D graphics
- Enhancements for enterprise
- Compatibility with existing apps

The choice of operating system was selected based upon all these features, functionalities and capabilities of the Android Honeycomb. The programming language of choice is Java. The server and database was implemented using Microsoft SQL Server 2008. Microsoft SQL Server 2008 was chosen because of its ease of use for development and administration, its robust architecture and high-end security feature and the online support from the provider. GrFinger Fingerprint SDK Recognition Library for Fingerprint Readers was the software used to capture and process the fingerprints. This software was used because it has various versions, which are compatible with various environments, platforms and programming languages. It has a version for the Java programming language. This SDK is easy to use and does not consume lots Random Access Memory (RAM)

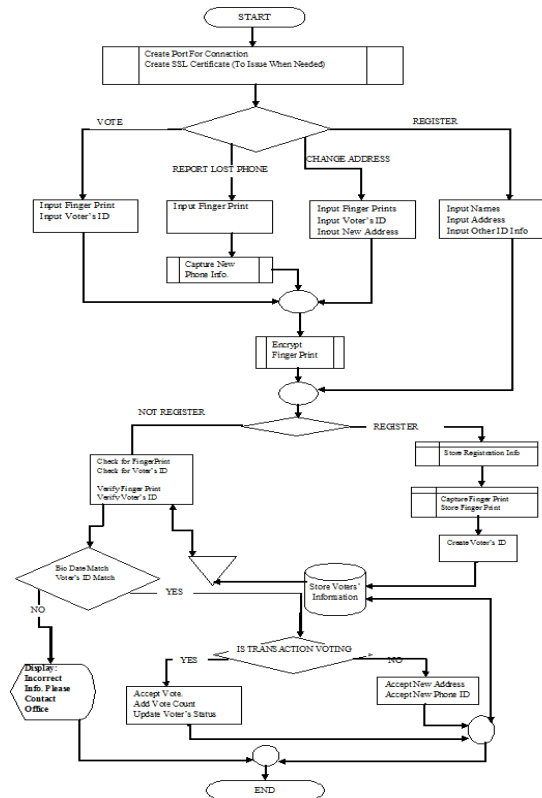


Figure.2 Flowchart of Mobile Voting

Fig.3 shows the applications screen on the Android Phone. It is displaying all the applications including the voting application, which was created by us, and this is shown with a circle over that. When the user clicks on this icon, it will open this application. The Android applications interface setting allows for ease of use and easy access and manipulation of the icons. Also deploying the application is very easy on the developer. Fig.4 shows the initial screen when the voting application starts up. It presents the user with four options such as below:

- Register – This option is used when the user is first registering through the application. It will take them to a registration screen.
- Vote – This option is used for users to vote if they have already registered and authenticated. This option will take them to the voting module where they will be required to supply their fingerprints and voter's ID.
- New Address – This option is used in the event persons need to change or modify their address information. They will be taken to a screen which allows them to update their address through the mobile application
- Lost Phone – This option should be chosen only in the event that the users may have lost their old phone. They will be taken to a screen, which will allow them to supply their fingerprints and voter's ID.

In addition, the VeriSign Identity Protection logo is at the bottom of the application to verify that the application is valid and secure. Registration captures all the information about the voter that is needed. Fig.5 shows what will be the display when the user selects the option

to register. It captures all the information about the voter that is needed. This includes names, addresses, date of birth and tax registration numbers (TRN). For the address, to make it easier to search and to utilize the 21st Century technology when it comes on to locating address, an address search map has been used. The button, which is highlighted -“Find Address”, in Fig.5 when clicked will initiate the address map. When the user selects the “Search Address” button, they will be taken to a map of the earth. This map is the Google map for android applications. They are able to navigate, zoom in and zoom out as it is on a regular Google maps search. The user zooms in on the map of Jamaica. User has the ability to move to all locations on the earth that Google Maps have covered and also to zoom in and zoom out.

Fig.6 shows the user selecting the address. This address in our simulation example is Shadbark Road, Kingston. When user selects the “OK” button, they are taken back to registration screen. All the information has been filled and the information is now ready to store. User now has to select the “OK” button to connect to the government database where the information will be stored as shown in Fig.7. If the user decides however, to decline from registering, then they can select the “Cancel” button and then they would be taken back to the initial display screen. After the user clicks the “OK” button confirming his registration information, they will be taken to the screen shown in Fig.8. This is the confirmation and ticket notification screen. The information on this screen is taken from the database. After the user registers and the request and information reaches the government database, a ticket is created for that person. The ticket at this moment is open; this means that the registration process is still not completed. The user will be required to know his/her ticket number. On visiting the electoral office, they will be asked for their ticket number. They will be asked to give their fingerprint and upon extraction of the fingerprint, then the ticket will be closed. At this point, the registration process gets completed.

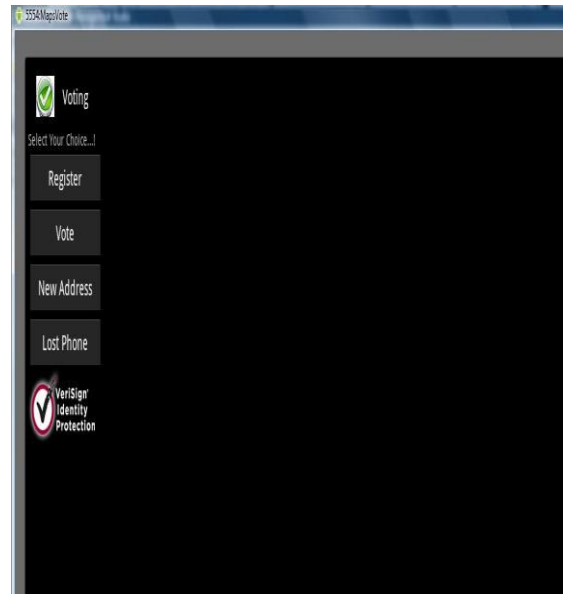


Figure.4 Initial Start-up Screen (Application)

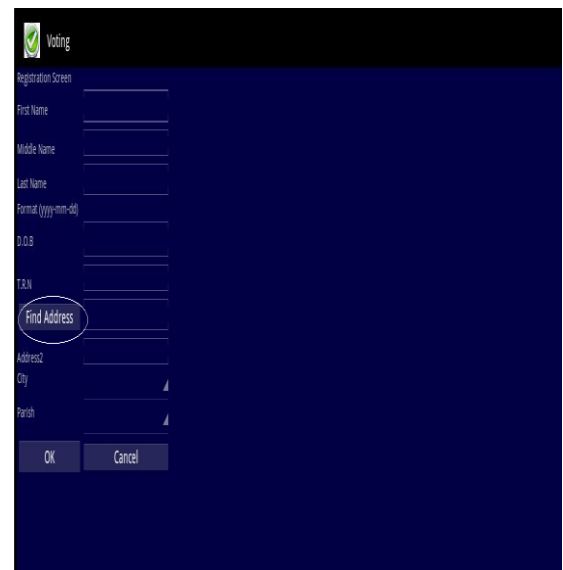


Figure.5 Registration Screen and Address Search



Figure.3 Mobile Voting Icon – Android Application

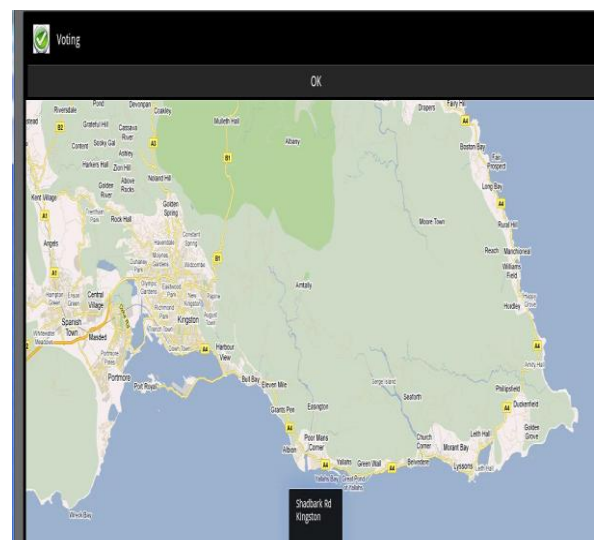


Figure. 6 Selecting Address

Potential voters will produce their TRN and the user of the system will then enter their TRN and click the search button. If the user has registered then all the registration information will be displayed on the form. There is a section on the form to display the fingerprint of the voter. In this case, the voter has not yet been authenticated; hence, there is no record of voter's fingerprint. The "Image" button on the menu bar is used to search for the fingerprint after it has been captured by a fingerprint scanner. The enroll button has been gray out at this time as it is only enabled when a fingerprint is supplied. If voters does not get their fingerprint scanned then they will not be authenticated, therefore they will not be able to vote using the "Biometric Mobile Voting" application. Fig.9 shows the "Electoral Office Voters' Authentication" screen when the user's fingerprint has been supplied. A physical picture of the fingerprint showing the ridges has been displayed. The enroll button is now enabled to allow the user to update the database with the new voter's fingerprint. After the voter's fingerprint is enrolled then the voter is fully eligible to vote. The voter however, has to vote using the phone that was used to do the registration. Voter's fingerprints are linked with the user's TRN in the appropriate database. At this point all fingerprints stored in the main database have been encrypted. Reason for this is to conceal persons' biometrics identity. Even if intruders should get access to the database then they will have to get access to the key and the decryption algorithm in order to get the biometric identity. However, after the fingerprint has been enrolled, the address status in the database gets changed for verification. This is important as when a user wishes to change or modify his/her address, then the status will be set back to "Not Verified" condition, until they come into the electoral office again towards verifying the information. This is part of the security strength mechanism. The operations control of the system is done both in the backend and the front-end (application side) of the system. This is to prevent false voting and forgery, and preventing users from voting more than once which is shown in Fig. 10. Fig.11 shows the condition that the voter decides to vote. In this case, the user will be required first to produce his fingerprint and voter's ID. After supplying, the fingerprint and voter's ID then voter will click the login button. On clicking the login button, the fingerprint is instantly encrypted. The encrypted fingerprint and the voter's ID are sent to the government's database where it is authenticated and validated. If the information, which the voter supplied, is validated correctly with the matching mobile phone identity then they will get the go ahead to proceed to vote. Fig.12 shows the voter after supplying his information and verified is then taken to this screen and the selection of political party will appear in the form of radio buttons. User will select the party of choice then click the "OK" button. Upon clicking the "OK" button, the choice of selection will be sent to the government along with the voter's ID for processing. The voter's ID is sent to the database along with the updated count of the party, which was the choice of voting as shown in Fig.13. In this way,

the voting status of the voter is captured but the identity of the voter is concealed as it relates to the party, which he voted for. This mechanism enforces security so no history of the party has been linked to a particular voter.

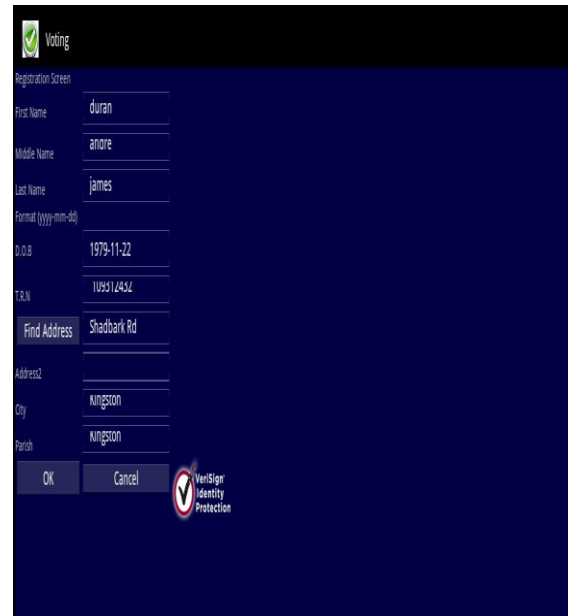


Figure.7 Registration Completed

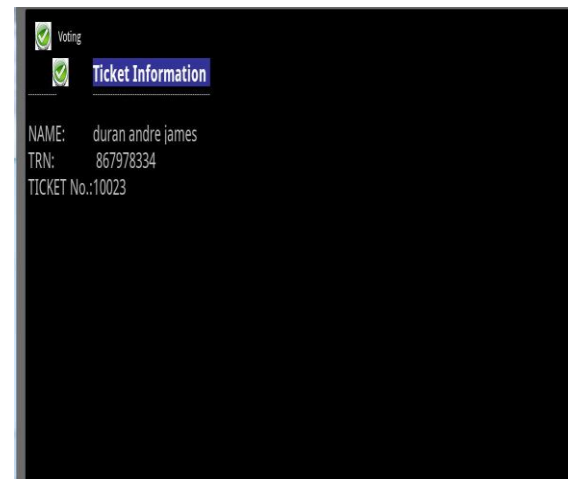


Figure.8 Registration Confirmation

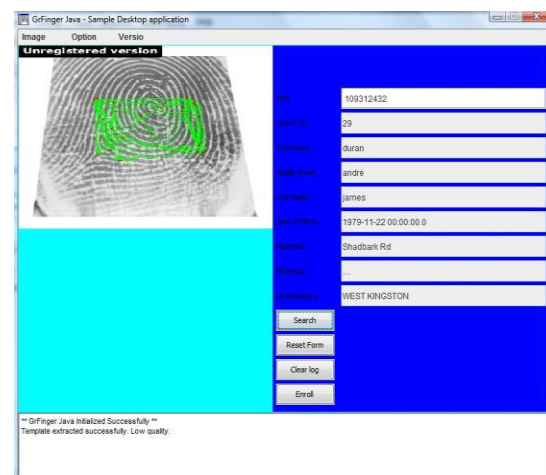


Figure.9 Fingerprint Capturing- Electoral office

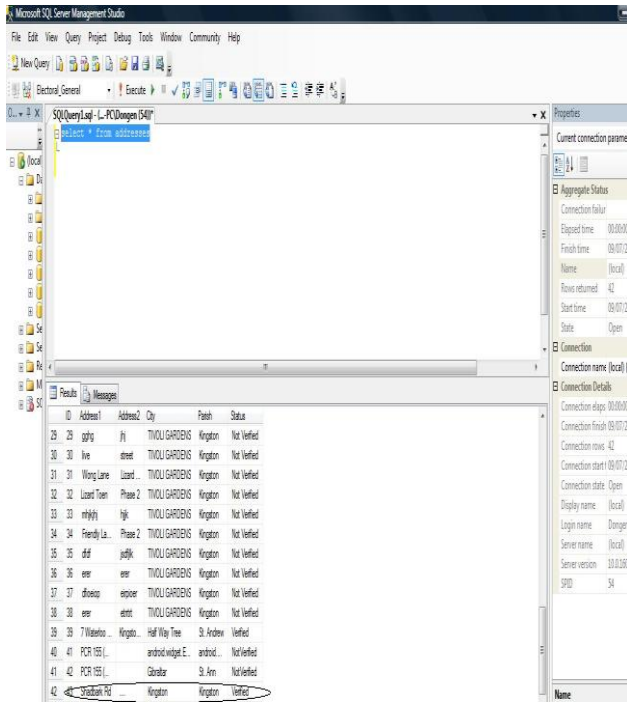


Figure.10 Voter Address- Verified

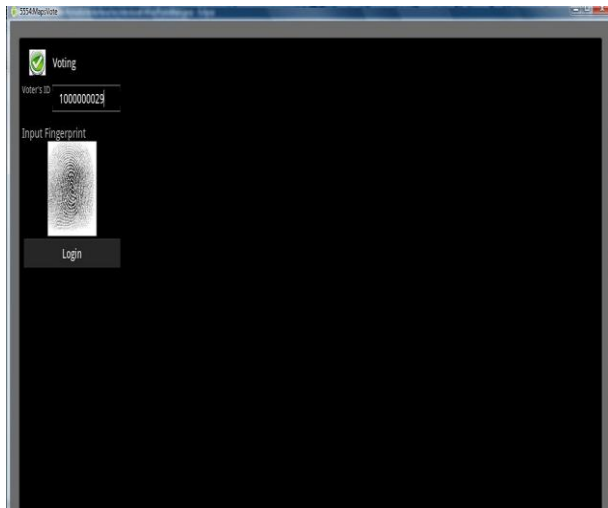


Figure.11 Biometric Mobile Voting

A. Address Change

If a person decides to change their address information then they will be brought to the screen shown in Fig.14. The “New Address” option when selected will bring the user to this screen. The potential voter will be required to give their fingerprint and voter’s ID. The fingerprint is encrypted the same time in the application before been sent over the network to the backend to be processed. The “Address Locator” button will take you to the Google Maps screen so user can choose the new address. This address will however be put on hold until it is been verified. This verification can be done at government electoral office outlets and at the local constituency offices. A web application is available to make the information given is authentic. But before that, the user address information in the database is set back to “Not Verified”. Fig.15 shows a confirmation message after

address information has been submitted. The server received the information and notify the voter that their information is been received Fig.16 shows the website which can only be accessed by the electoral office network.

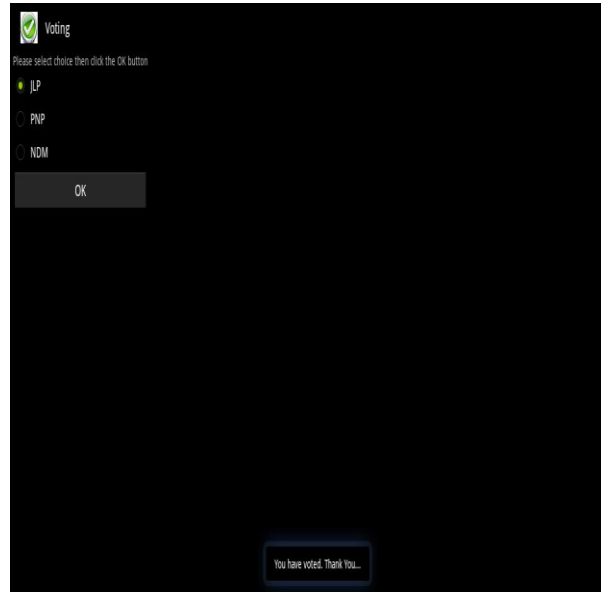


Figure.12 Confirmation of Voting

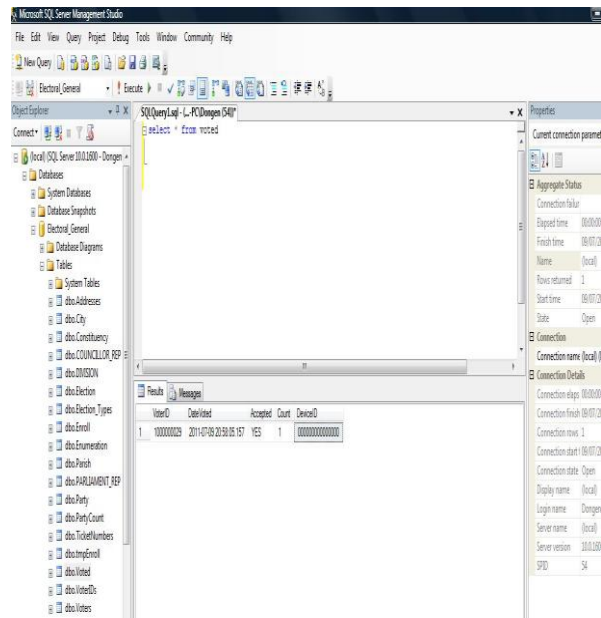


Figure.13 Voting count

This web application is used to validate voter’s new address information. The voter will supply their voter’s ID and the officer will input the “Voter’s ID” in the text box and then click “Find Voter” button. On clicking the “Find Voter” button the application will do a search for the voter’s address. If search is successful then the form will be filled out. At this point the officer can now click the verify button. This will instantaneously update the database as shown in Figure.17 where new Address Princess Alice Drive is been validated and confirmation sent that the address is now validated. A notification message, at the bottom of the web page, shows that the

address information is now validated. This process is done in the form of web application for easy access and ease of work load on the electoral office staff. It also makes it much easier on the voters to go into their nearest (local) constituency office to get the address information validated.

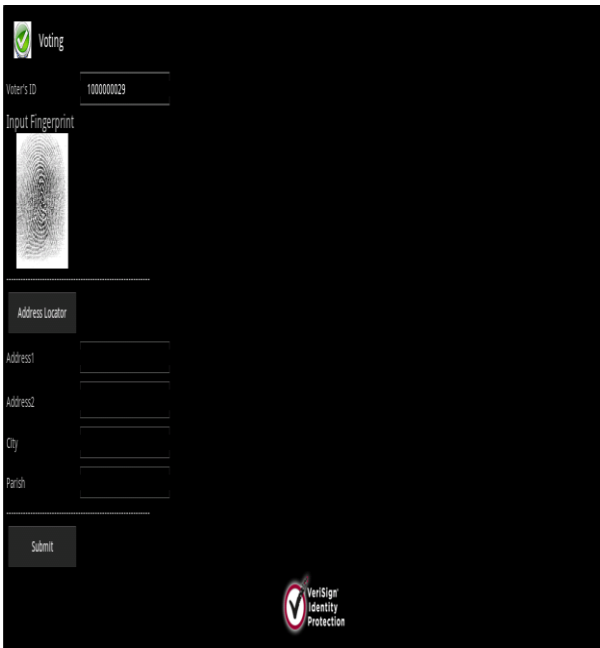


Figure.14 Address Change

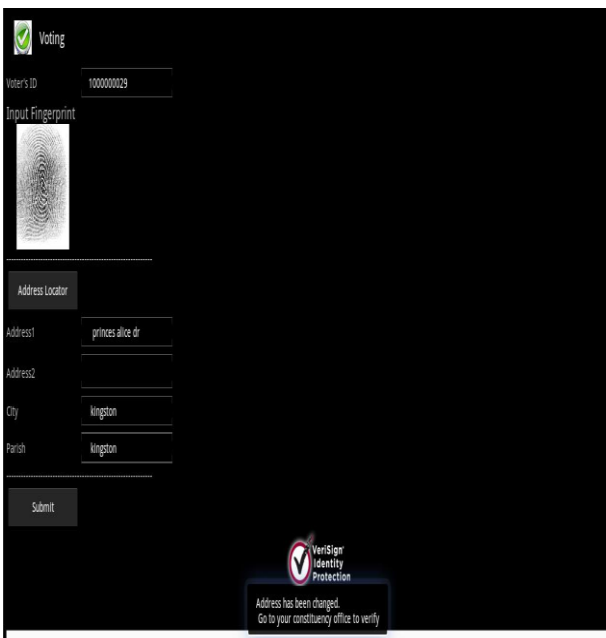


Figure.15 Confirmation of Address Changed

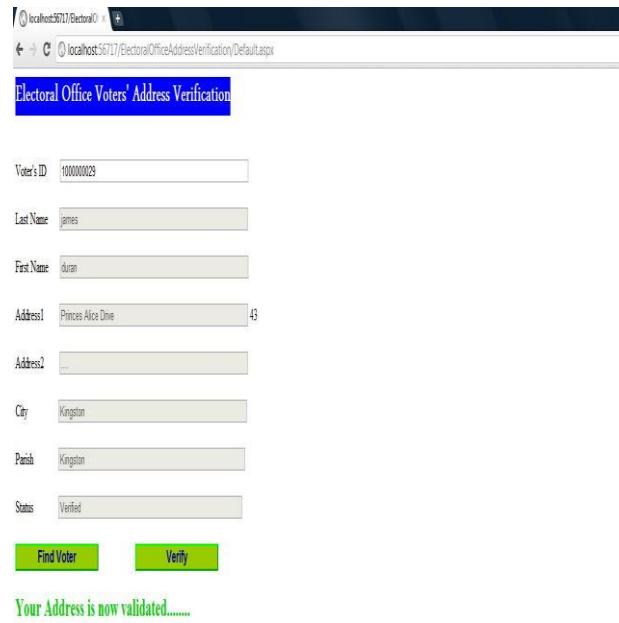


Figure.16 Validate Voter's New Address

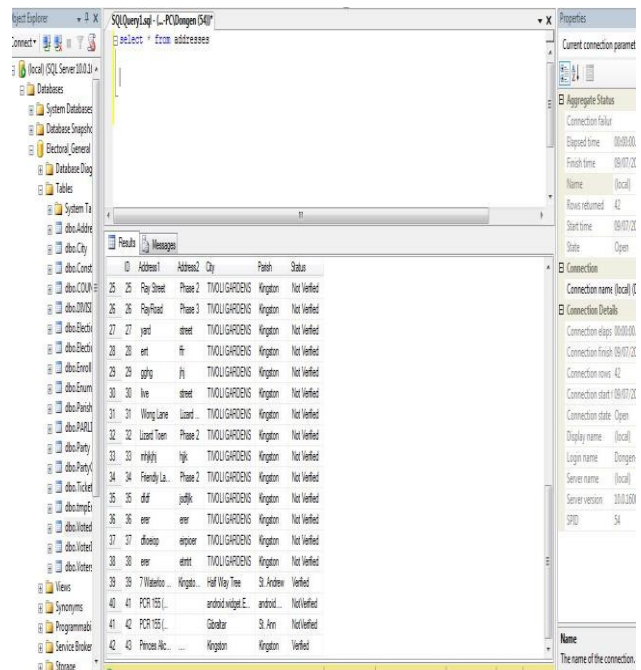


Figure.17 Voter's New Address- Verified.

B. Lost Phone

When a voter loses his/her phone, they will select the lost phone option from Fig.4 which will take them to the screen displayed in Fig.18. They will be required to supply their fingerprint and voter's ID. After supplying the information needed then they will select the submit button. They will not have to submit information about their old nor new phone, as the database have already tied their fingerprint and voter's ID to the mobile phone identity number. Also the application will be able to capture the new phone's information to store in the

database. Fig.16 shows that the server has received the lost phone notification from the user and responds with a notification message which is displayed on the screen. The voter's new phone is now updated in the database which replaces the old (lost) phone information.

C. Double Voting

Let us consider a scenario as shown in Fig.20 where a user is trying to breach the security operation of the system. Someone who has voted already is trying to cast another vote. The person has to log in his fingerprint again and also his voter's ID. On receiving this information the server instantly recognizes that the status of the person making the request is already voted. On receiving this request the server raises a red flag and send a notification/warning back to the voter telling that his request is been denied. A message is displayed on the screen to notify the user. A history of the attempts made on a particular device with a particular voter's ID is been kept. The timestamp, number of attempts and status is also captured. This information is been kept in order for a security mechanism and in order to help in any investigation anytime in the future. Fig. 21 shows database that the same user is trying to cast a second vote, however vote is not been accepted and the attempt count increases to 2. Remember a potential voter tries to vote from a phone that he is not tied to in the database. In other words he didn't register to vote from this phone that he will try to vote from and application will not allow the voter to do so.

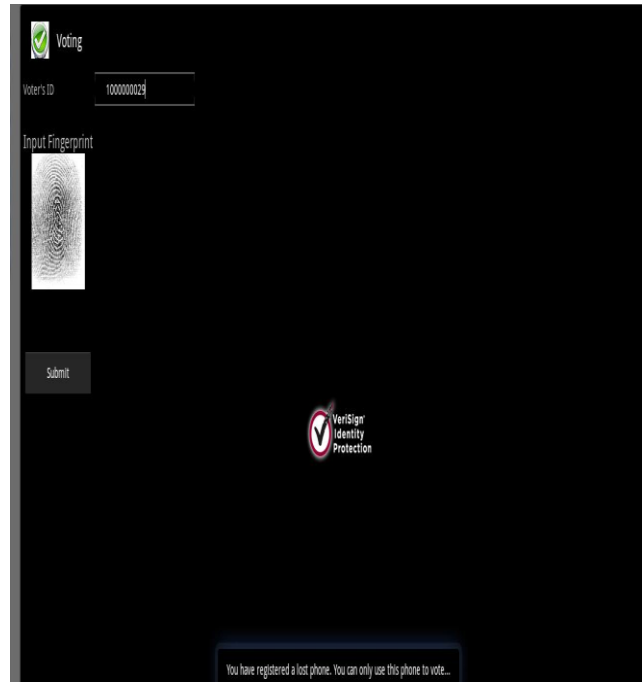


Figure.19 Confirmation of Phone Change

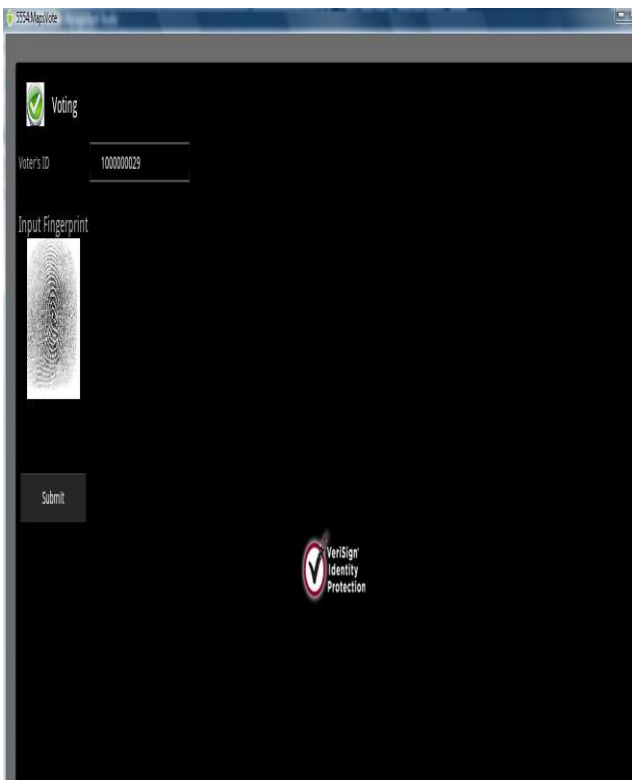


Figure.18 Lost phone

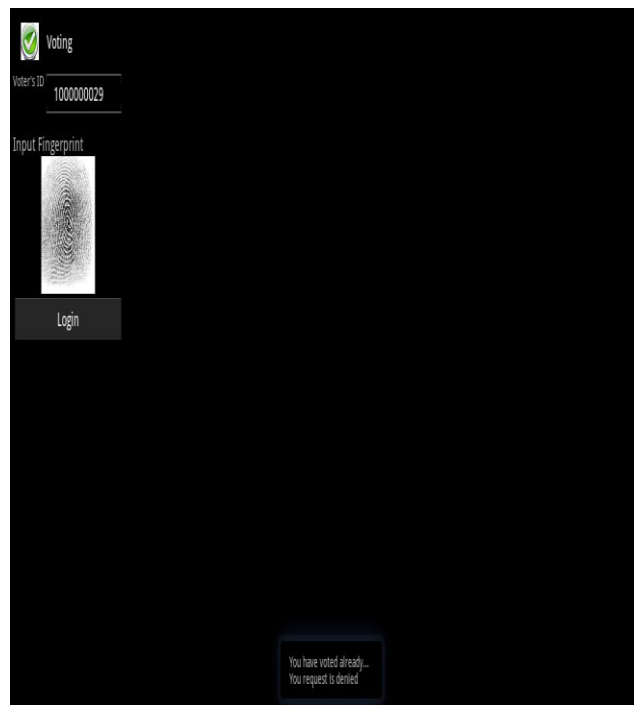


Figure. 20 Double Voting

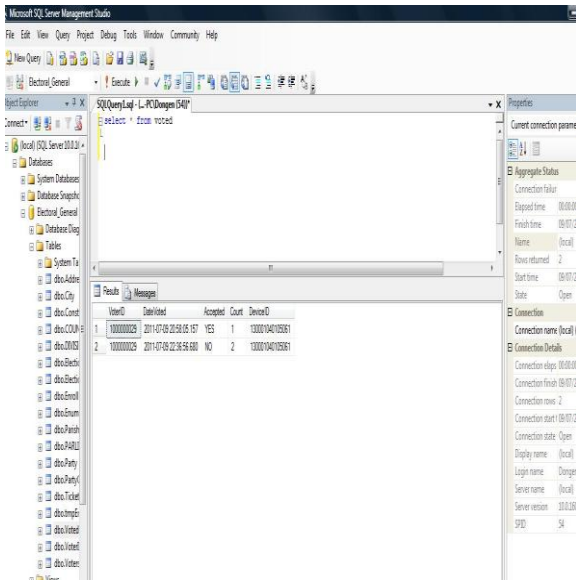


Figure. 21 Database of Voting Attempts

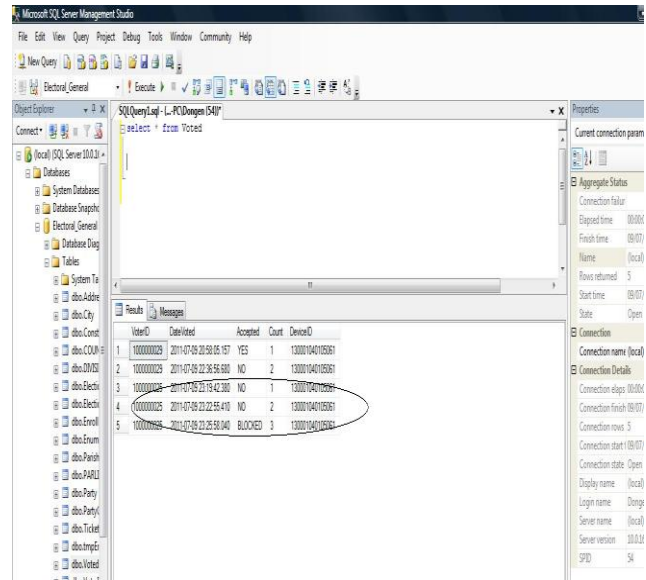


Figure.23 User barred from Voting- Database

D. Voting from a Wrong Device

In Fig.22 a legal voter with authenticated fingerprint and voter’s ID is trying to vote from a mobile device not registered to this voter. In a case like this, as part of the robust security mechanism there will be a bar to a request of this nature. This is to prevent valid voters to try to vote from multiple devices hence increasing the possibility of one person voting multiple times. A message is displayed to the user warning that he is voting from the wrong device and also the attempt count. Voter made a second attempt to vote from the same device. Again another warning message is displayed telling the potential voter that he is trying to vote from the wrong device and also the attempt count has increased to 2. If a user has already made 2 attempts to vote and both attempts failed then he only has one last attempt which he/she has to get correct otherwise the voter will be barred from voting. Voter tries to vote for the third time on the wrong device and now its strike three i.e. the user account. The voter’s ID and fingerprint is officially barred until checks are made in person that rectifies the situation.

VI CONCLUSION & FUTURE WORK

The manual voting process can be very tedious, prone to electoral fraud and costly. The time that is been consumed and the resources often times runs into expensive projects. With all this, security is compromised because of the inability of all the human factors to provide efficient security needed for robust operation of the system. The full potential of getting the citizen to express their democratic rights is not being realized because persons find it tiresome and time consuming, first to enumerate (register for voting) and then to stand in long lines to vote on election. In some areas persons are fearful of their lives and forced influence voting. The counting of ballots can also be rigged and very much time consuming and often times results are not tallied quickly enough. Tallied results seem uncertain and the credibility of the calculation is often times questioned. Semi-technological systems had solved some of these issues but create access to more problems such as persons breaking through the system to vote multiple times because of lack of strong security. The proposed system addressed these challenges which brings the application of Biometric i.e. Fingerprint towards voting from the mobile device where people can vote to any party of their choice from anywhere and also Registration can be done over the internet from mobile device itself except for registering the fingerprint where you have to visit the electoral office.

In future the software would have the capability to check if the fingerprint scanned is proper towards encryption particularly if the scanner being used is of cheap quality. Also the false positives/false negative of encrypted fingerprint be checked by the software towards real time voting process too in future to make sure only authorized person is given permission and not illegal person to vote though mobile identity be used as extra security measure too.. Also the database can be decentralized with more layers which will ease the load

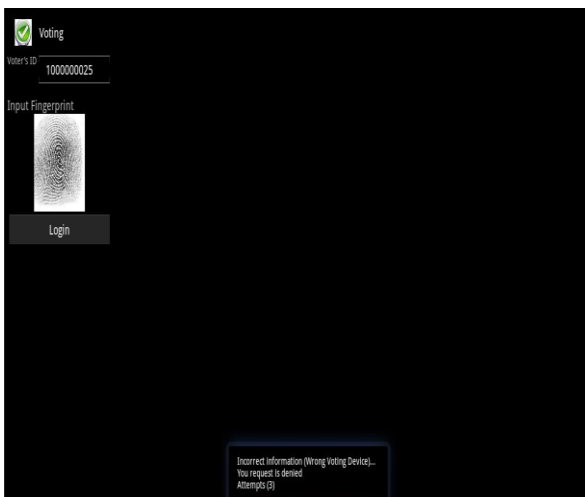


Figure.22 Voting From Wrong Device- Three Attempts

on database server and also security features at database level should be strengthened too towards accessibility of Government database. Finally Registration including fingerprint and Address verification also should be automated over internet instead of going to electoral office. Last but not the least creating an application in an environment that is platform independent and hence it can be run on various types of mobile equipment embedded with finger print scanner or and getting finger print scanner attached to mobile handset via USB. By doing this it will eliminate the effort of everyone trying to get specific mobile equipment that may be too expensive for them to afford. Lastly the people would get their fingerprint registered in database every five years taking into consideration the age, wrinkles appearing in finger print, blood circulation and so.

REFERENCES

- [1]. Electronic Voting (2009), Available from http://www.hwskioskprinter.com/terminology/electronic_voting.pdf
- [2]. Gentles, D and Suresh, S (2011). "Biometric Secured Mobile Voting", Proceedings of Second IEEE/IFIP Asian Himalayas International Conference on Internet, Kathmandu, Nepal.
- [3]. Gentles, D (2011). "Application of Biometrics for Mobile Voting", M.Sc Computer Science Dissertation, Department of Computing, University of West Indies, Jamaica
- [4]. Electoral office of Jamaica (2007), Available from www.jis.gov.jm/special_sections/election_2007/index.html
- [5]. Deville, D et al(2003), "Smart Card Operating system: Past, Present and Future" .Proceedings of *Fifth USENIX/NordU Conference*, Vasterås, Sweden
- [6]. Pfitzmann, B and Ahmad-reza S (1996). *Anonymous fingerprinting*. Berlin: Springer-Verlag, 1996.
- [7]. Jain, A et al (1997) "On-Line Fingerprint Verification." *IEEE Transactions on Pattern Analysis and Machine Intelligence VOL. 19, No. 4*, 1997: 302-305
- [8]. Menezes, A et al(1996). *Handbook of Applied Cryptography*. CRC Press, 1996
- [9]. William, S (2005). *Cryptography and Network Security Principles and Practices, Fourth Edition*. Prentice Hall, 2005
- [10]. Nechvatal et al. *Report on the Development of the Advanced Encryption Standard (AES)*. National Institute of Standards and Technology, 2000.
- [11]. Mobile Marketer (2009), "Mobile Voting Could become Reality by 2012: VeriSign", Available from <http://www.mobilemarketer.com/cms/news/messaging/2980.html>
- [12]. Wireless Mobile Voting (2000), Available from <http://www.andhranews.net/India/2008/January/25-Kerela-invents-30938.asp>
- [13]. Kim, K and Hong, D (2007), "Electronic Voting System using Mobile Terminal. World Academy of Science, Engineering and Technology, Vol .3(2), pp.33-37.
- [14]. Speckmann, B (2008). *The Android mobile platform*. Michigan: Eastern Michigan University, 2008.

Donovan Gentles is a Msc. Computer Science student in the Department of Computing at the University of the West Indies, Jamaica which he is pursuing since 2009. Prior to that, he obtained Bachelor's degree in Computing & Information Technology from University of Technology Jamaica in 2006.

He is currently working as Programmer/Analyst in Gleaner Company Ltd in Jamaica since 2009. Prior to that he worked as Programmer/Project Leader during 2008-2009 in Fujitsu and state of Connecticut Judicial branch, USA. Also during 2007-2008 he worked as Programmer/Analyst in MiPhone and Fiscal Services, Jamaica.

He is well versed in C/C++, Java, ASP.NET, JavaScript and Database management system using Oracle, DB2, MySQL and MSSQL.

In his Master's Programme he did Master's thesis on "Application of Biometrics in Mobile Voting which focused on using biometrics for mobile voting that has been published in IEEE Conference proceedings . His research interest includes Intelligent Agents, Mobile commerce, Biometrics.

Prof. Suresh Sankaranarayanan holds a PhD degree (2006) in Electrical Engineering with specialization in Networking from the University of South Australia. He is a Senior Member of IEEE computer Society and Computer Society of India too. He was working as a Lecturer (Asst. Prof. Status) in the Department of Computing and lead the Intelligent Networking Research Group, in the University of West Indies, Kingston, Jamaica, during 2008-11. He has also worked as a Professor, School of Computer Science and Engineering, Vellore Institute of Technology (VIT University), Chennai Campus, India, for a short period during 2011. He is now working as Associate Professor, Department of Computer & Information Systems, Institute of Technology, Brunei (ITB – A technological university). Currently he is also functioning as a Visiting Professor, Department of computing, Faculty of Pure & applied Science, University of West Indies, Mona Campus, Kingston-7, Jamaica, West Indies. He has got to his credit, about 50 fully refereed research papers published in the Proceedings of major IEEE international conferences, as Book Chapters and in International Journals. He is also a Reviewer and Technical Committee member for a number of IEEE Conferences and Journals. His current research interests are mainly towards Mobile and Ubiquitous Computing- Wireless Sensor Networks in Health & Engineering, Intelligent Agents, Cloud Computing, Mobile commerce.