ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 12, December 2015

A Survey on Mobile Phone Voting System with High Secure

Suresh Lakavath, R.Naik

Senior Project Fellow, CSIR-URDIP, Pune, India

ACME Cleantech Solutions Pvt Ltd, Gurgaon, Haryana, India

ABSTRACT: Voting is a widely spread and democratic way of making decisions. For centuries, worldwide has been using the popular paper-based voting system, which does not provide the desirable blend of accessibility and efficiency. Missing ballot papers, invalid votes and miscount are some of the challenges associated with the paper-based voting system. Electronic voting has been attracting a lot of attention and research for the past few years all over the world, for it has some remarkable advantages over traditional paper-based voting. This research proposes the use of mobile phones to facilitate communication and rapid access to information and their diffusion has reached a larger proportion of the population in a short period of time. When such a device is available why not use it for a time saving, cost effective, secured method of casting a vote. On the other hand, GSM (Global System for mobile communications) is the most widely used mobile networking standard. There are more than one billion GSM users worldwide that represent a large user potential, not just for mobile telephony, but also for other mobile applications that exploit the mature GSM infrastructure. GSM mobile technology is presented. By integrating an electronic voting scheme with the Mobile infrastructure, we are able to exploit existing Secure Mobile authentication mechanisms and provide enhanced voter authentication and mobility while maintaining voter privacy. This provides a voting system based on smart mobile communication devices. It comprises at least one smart mobile communication device, at least one server device, a client module, and a server module. The client module is installed on the smart mobile communication device and it is used for temporarily saving the voters information, submitting identity verification request, showing voting inquiries, and submitting votes. The server module is installed on the server device and it is used for storing the voter's information, verifying the voter's registration and identity, issuing and verifying the voting certificate, creating and publishing the voting affair, and calculating and publishing the voting contents statistics. The client module and the server module perform digital communications through a mobile communication network. The invention also provides a voting method based on smart mobile communication device. According to this invention, voting can be safe, convenient and fast.

KEYWORDS: M-Voting, Mobile Phones, democracy, Security, Voting, Database.

I. Introduction

The main key role-players in mobile phone voting system are the Independent Electoral Commission (IEC), mobile voter, observers, political parties, mobile phone, the system (MPVS), Mobile Network Operators (MNOs) and the Department of Home Affairs (DoHA). In above Figure the use of a mobile phone by the voter to cast the vote. The mobile voter connects to the mobile network using the 2G, 3G or the 4G technology that allows the mobile voter to connect to the application server to download the application. Once the application is downloaded and installed, the mobile voter registers to vote using the application. During the registration, the application connects to the DoHA database to verify the Identity Document (ID) number of the mobile voter. After a successful registration, the mobile voter can cast his/her vote.

II. Related work

Mobile Voter:

The mobile phone allows the voter to download the application for free from the MPVS application server. Once the application is installed, the voter can register to vote and then cast their vote using their mobile phones free of charge.

DOI: 10.15680/IJIRCCE.2015. 0311122

The application developed is suitable for most mobile phone devices as it is very simple and with as limited pictures or graphics as possible. The application is developed for inexpensive mobile devices; these devices are used by people in mostly rural and also in urban parts of the country. Our proposed application allows voters to share one mobile phone, from one person to the other by registering their own individual account on the system. Voting using this application is not per phone but per person registered, so it is not linked to the mobile phone or mobile phone number.

Web Server:

A **web server** is an information technology that processes requests via HTTP, the basic network protocol used to distribute information on the World Wide Web. The term can refer either to the entire computer system, an appliance, or specifically to the software that accepts and supervises the HTTP requests.

Application Server:

The application server houses the mobile phone voting application and also handles all application operations between the voters and the MPVS database. During the voting process, the voter interacts with MPVS database through the MPVS application interface. Mobile phone devices have small screens with restricted display and navigation capabilities; restricted data-entry capability due to the size of the key-pad; with the disadvantage of low bandwidth and network latency. Consequently, the application developed is simple, user friendly but still detailed with no ambiguities so that voters can cast their votes with little or no assistance regardless of their educational background. The simplicity allows the voters to register and cast their vote at a very minimum time as possible. The proposed ballot design takes form of the traditional paper-based ballot which incorporates the party logo, party name and the name of the party representative. To further enhance usability and friendliness, we propose a multilingual application, this assist voter of different backgrounds. Voters can decide to stop the voting process at any time before they confirm the vote, but the vote will not be counted.

Database Server:

The MPVS database performs back-end tasks such as data analysis, storage, data manipulation and archiving. The database is built using MySQL and stores all registered voters, all contesting political parties and their representatives and the voter's roll according to the DoHA database. The databases stores complete information about each eligible voter and also status information related to them. Each voter record has two status flags, the first flag automatically becomes "True" once the voter has registered and the second flag represents whether the voter has casted the vote or not. Initially all status flags are "False". The vote choice is not linked with the voter to provide privacy to the voters.

System Architecture Overview & Diagram:

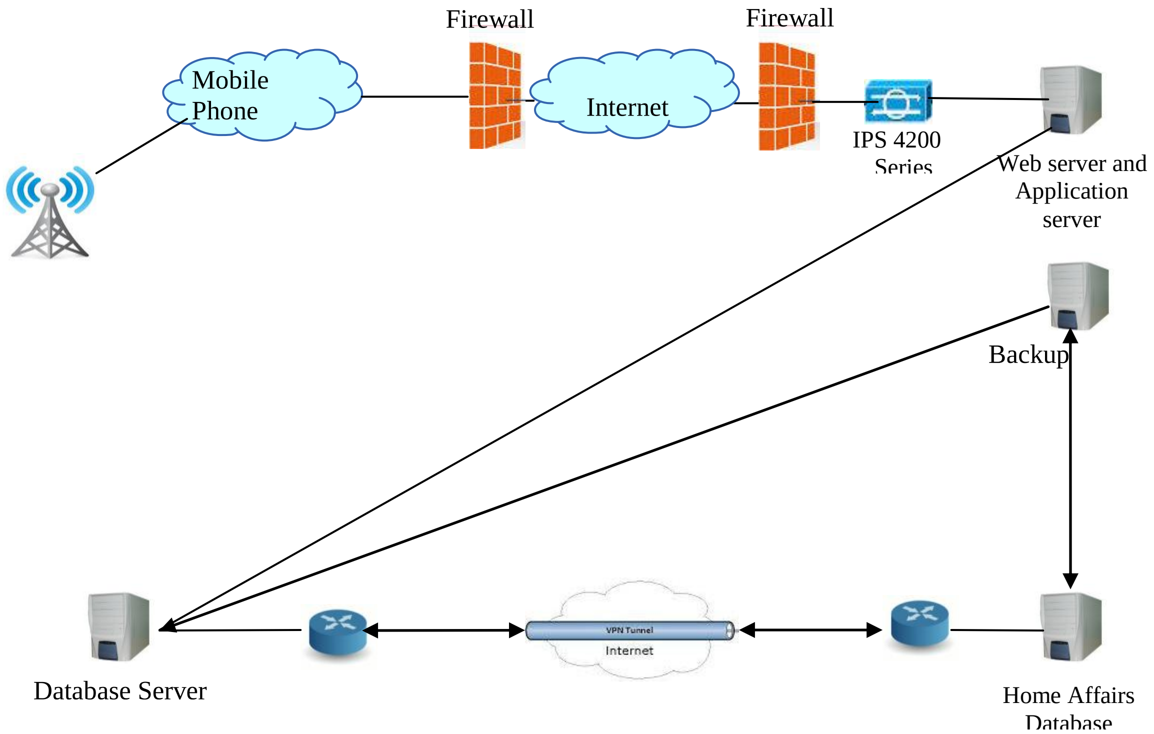


Figure 1: Mobile Phone Voting System (MPVS)

Department of Home Affairs database:

The Department of Home Affairs (DoHA) database houses the national population list, with individual ID numbers and their personal details. The DoHA database connects with the MPVS database to provide authentication for voters. The voter is only allowed to vote if the ID number is valid and they are 18 years of age or older.

- 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.

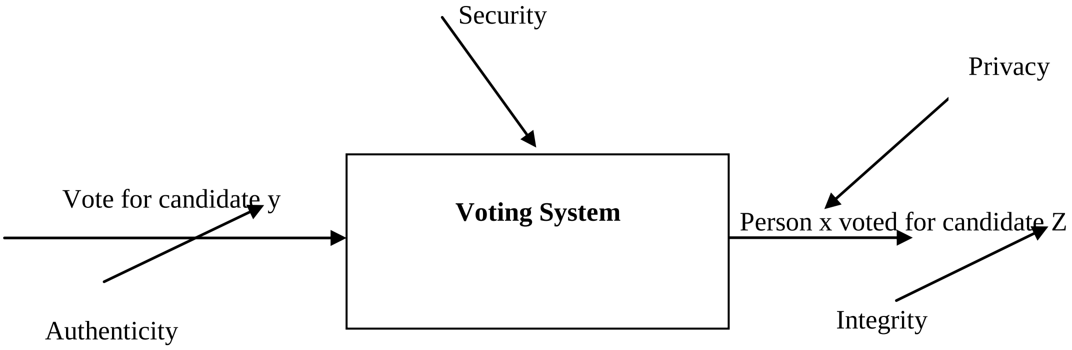
- After the user has submitted the correct finger- print from the correct phone and also provide the correct voter's ID then the server will authenticate the voter. After which the voter is now permitted to vote.
- When the voter casts his/her vote then voter status will be changed and also the party 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.

Security:

Now we will describe a set of voting security criteria. However, depending on different democratic requirements in different countries, and the different scales of electronic voting systems, security goals can vary. General security requirements include democracy, privacy, accuracy, fairness, verifiability and recoverability.

Democracy: All and only the authorized voters can vote, and each eligible voter can vote no more than once. Voters can also choose not to vote. To achieve democracy, voters need to be properly registered and authenticated, and then there should be a convenient way for them to cast their votes, for example, availability of different language choices, special aid for disabled voters, and proper ways for absentee voting and early voting.
Privacy: All votes remain secret while voting takes place and each individual vote cannot be linked by any individual to the voter who casts it. The privacy issue is paramount.
Accuracy: The voting result accurately reflects voters' choices. In this case, no vote can be altered, duplicated or eliminated without being detected.

Fairness: No partial result is available before the final result comes out.



Some of the key criteria's to be met to successfully develop a secure and trustworthy mobile phone voting system include the following features:

1. Anonymity - the vote must not be linked to the voter
2. Authenticity - only eligible voters can cast their votes
3. Integrity - once a voter cast a vote, no alternation to this vote is permitted.
4. Accuracy - all valid votes must be counted
5. Democracy/ uniqueness - only one vote per voter
6. Verifiability - voters can independently verify that their votes have been counted
7. Multi-user - a number of voters can vote simultaneously
8. Accessibility - the system can be accessed by voters from any location
9. Availability - the system must have high-availability during an election campaign.
10. Simplicity - the system must be easy to use
11. Multi-lingual - translates to all eleven official languages

12. Reliability - election system should work robustly, without loss of any votes, even in the face of numerous failures, including failures of voting machines and total loss of mobile communication.

Before the registration can start, the voters are expected to have registered their mobile phone with the MNOs, downloaded the mobile application from the application server, and install the application on their mobile phone.

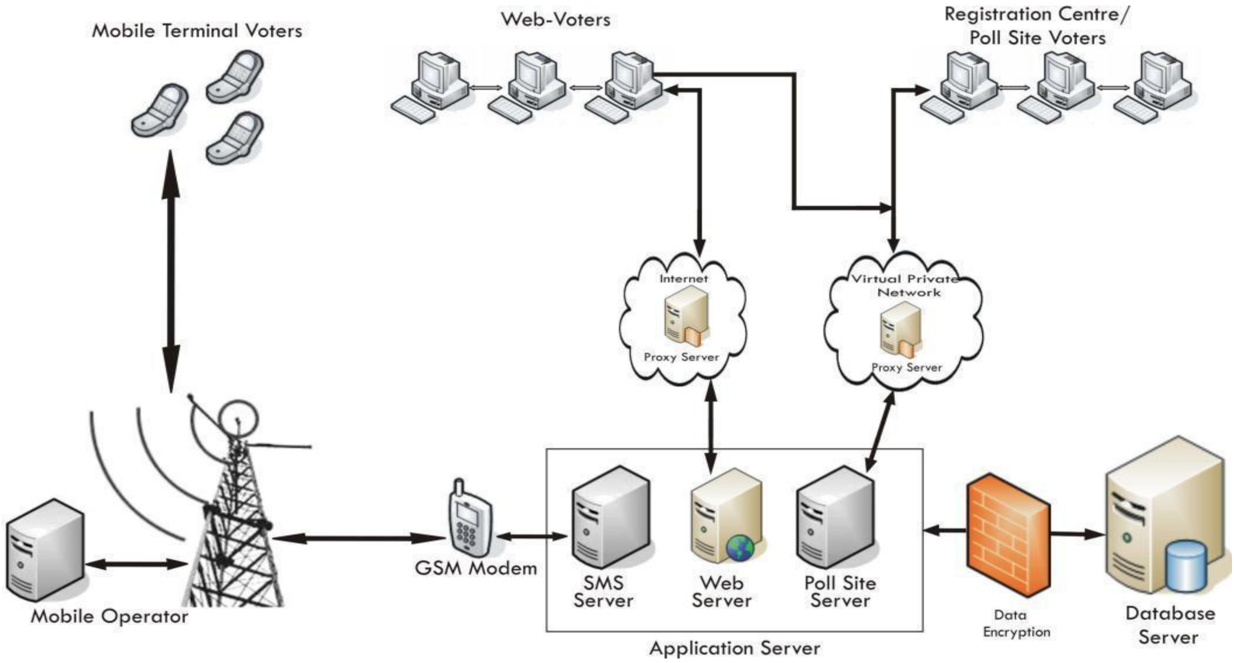


Fig 2: Mobile Phone Voting System (MPVS)

The system architecture defines the key components of the proposed system together with the interactions between these components. The overall functional structure of the framework is summarized as follows: an eligible electorate (18 years and above) registers with the electoral body at a gazette registration centre. The person identifies self by providing all the required bio data, phone number and the fingerprints of the person will be scanned and stored in the database. The registered electorate will be given a unique voter identification number and a unique voting code which he/she is expected to keep confidential. A remote internet voter (client) runs the Uniform Resource Locator (URL) for the e-voting system through a web browser. The web application prompts the voter to download the voting application package that should be installed on the voter s computer. The voting application runs remotely on the client s computer. Voting is done via the voting application installed on the client s computer by selecting the political party of choice and a fingerprint scan. A remote mobile terminal voter votes via SMS. Poll site voters cast their electronic ballots at designated Poll sites. The voter selects the political party he/she wants to vote for on the voting interface and scans a fingerprint to cast the vote.[1][7].

The developed e-voting system was designed to allow many voters to voting simultaneously while ensuring highly availability during the electioneering process. Authentication into the voting system is either by biometrics or voter identification number (voter ID) and voting code generated for each voter after registration. Poll site voting and internet voting requires a fingerprint scan for ballot casting while SMS voting requires combination of mobile number (SIM) of the electorate, the generated voter ID and voting code, which are unique for voter. A voter ID and voting code sent to a particular SIM after registration cannot be used on another SIM for voting. The security considerations of the system were based on a RSA encryption algorithm which was implemented to secure end to end messaging, the Transport Layer Security (SSL/TLS) which is a VPNs cryptographic tunneling protocol and firewalls in form of proxy servers. Furthermore, the web server only hosts the web page of the e-voting system. Actual ballots casted by web voters are sent to the Poll site server which is on a VPN. Ballot casted are record in the data tables at the backend of the database as binary templates. [1]

The system ensures only one-person, one-vote (democracy) property of voting systems. The voters fingerprint, voters SIM, voting ID and voting codes of a voter intending to cast his/her ballot are matched at every voting attempt to prevent multiple voting. During registration, fingerprints of new electorate about to be registered are matched against exiting fingerprints in the database to prevent multiple registrations.

The system design mainly focuses on following areas:-

1. Module 1: Server
2. Module 2: Client
3. Module 3: Fingerprint Recognition

A. *Module 1: Server*

This module contain following component which are to be used in the Server.

Create Account:

The voter has filled the registration form first. In that all information regarding voter is correctly fill by voter. After filling all necessary information the account get created at server site.

Delete Account:

They have privilege of deleting the created account.

Edit Account:

If any necessary are there, then server site can performing some edition over there.

DB worker:

DB worker can maintain the database of whole users.

Add Candidate:

After creation of voter account the server site validates that voter.

Authenticate Voter:

Server can authenticate the user s identity.

Count Server:

There is count server at server site which tally a final result as well as it count the duplication of records and maintain a log for that.

Dispatch Result:

Final step is dispatching a result.

B. *Module 2: Client*

Create Account:

Voters have to fill all the necessary information on the particular site. After the fill the form with necessary documents the voter account get created at server site. Then voter can perform all operation which privilege they have.

Vote:

At the Election Day, voters just have to login into his/her account which is previously created. After login successfully, voter can cast his/her voter to their choice person..

Login:

The voter can login into his/her account at any time. In this login, voter can check to whom he/she vote, and whether his/her vote is tally in final result or not.

C. Module 3: Fingerprint Recognition

The Basics about fingerprint:

A fingerprint is comprised of ridges and valleys. The ridges are the dark area of the fingerprint and the valleys are the white area that exists between the ridges. Many classifications are given to patterns that can arise in the ridges and some examples are given in the figure to the right. These points are also known as the minutiae of the fingerprint. The most commonly used minutiae in current fingerprint recognition technologies are ridge endings and bifurcations because they can be easily detected by only looking at points that surround them.[7]

The input fingerprint image is the gray scale image of a person, which has intensity values ranging from 0 to 255. In a fingerprint image, the ridges appear as dark lines while the valleys are the light areas between the ridges. Minutiae points are the locations where a ridge becomes discontinuous. A ridge can either come to an end, which is called as termination or it can split into two ridges, which is called as bifurcation. The two minutiae types of terminations and bifurcations are of more interest for further processes compared to other features of a fingerprint image.

Binerization:

Binarization to convert gray scale image into binary image by fixing the threshold value. The pixel values above and below the threshold are set to 1 and 0 respectively.

Block Filter:

The binarized image is thinned using Block Filter to reduce the thickness of all ridge lines to a single pixel width to extract minutiae points effectively. Thinning does not change the location and orientation of minutiae points compared to original fingerprint which ensures accurate estimation of minutiae points. Thinning preserves outermost pixels by placing white pixels at the boundary of the image, as a result first five and last five rows, first five and last five columns are assigned value of one. Dilation and erosion are used to thin the ridges.

Minutiae Extraction:

The minutiae location and the minutiae angles are derived after minutiae extraction. The terminations which lie at the outer boundaries are not considered as minutiae points, and Crossing Number is used to locate the minutiae points in fingerprint image. Crossing Number is defined as half of the sum of differences between intensity values of two adjacent pixels.

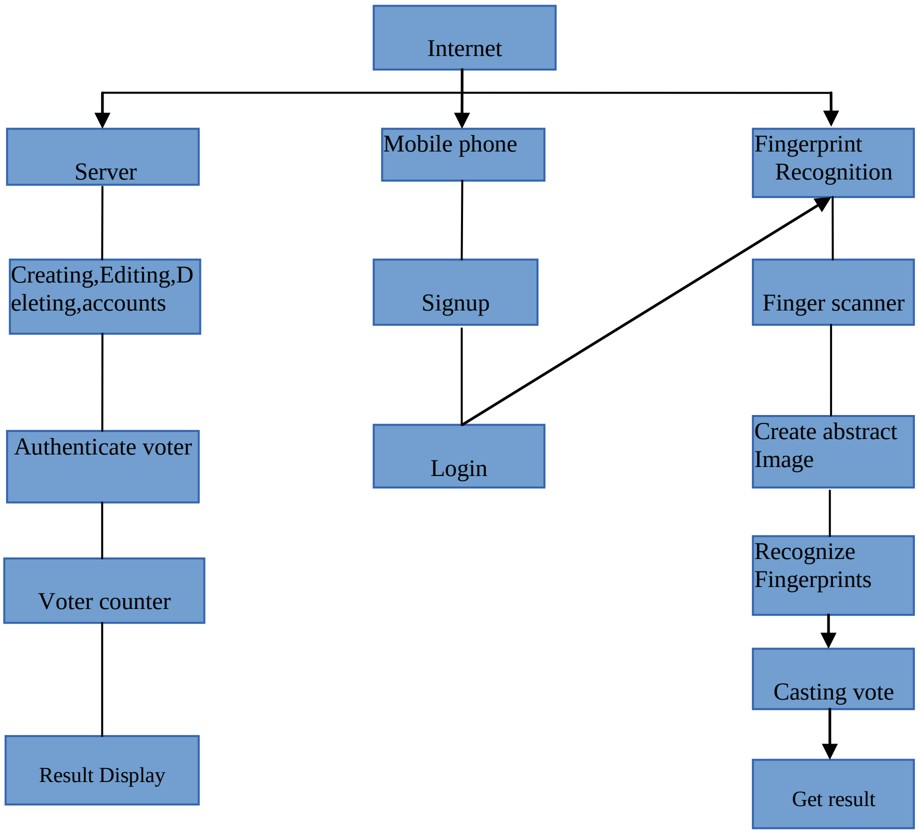


Fig 3: System Design

III. CONCLUSION

The E-voting system using Biometric enables a voter to cast his vote using internet without additionally registering himself for voting in advance and going to a polling place. Also, proxy vote or double voting is not possible. Any entities except for an e-voting device can't know the voting result. For over a century, fingerprints have been one of the most highly used methods for human recognition; automated biometric systems have only been available in recent years.

REFERENCES

1. Jain, a *et al.* 'On-Line Fingerprint Verification.' IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol. 19, (4), pp. 302-305, 1997.
2. Kim, K and Hong, D, 'Electronic Voting System using Mobile Terminal'. World Academy of Science, Engineering and Technology, Vol. 3(2), pp. 33-37, 2007.
3. Nwogu Emeka Reginald. 'Mobile, Secure E - Voting Architecture for the Nigerian Electoral System', Vol.17 (2), 27-36; 2015.
4. Donovan Gentles. 'Application of Biometrics in Mobile Voting', Vol.7, pp.57-68, 2012.
5. Okediran O. O., Omidiora E. O., Olabiyisi S. O., Ganiyu R. A., Alo O. O., 'A framework for a multifaceted electronic voting system', International Journal of Applied Science and Technology Vol. 1, (4), July 2011 .
6. Anita Maheshwari. 'Two way authentication protocol for mobile payment'. International Journal of Engineering Research and Applications, Vol. 2, Issue4, July-August 2012.