Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 2, Issue. 5, May 2013, pg.123 – 128

RESEARCH ARTICLE

SCOPE AND LIMITATION OF ELECTRONIC VOTING SYSTEM

Atiya Parveen[1], Sobia Habib[2], Saoud Sarwar[3]

[1]M. Tech Scholar, Al-Falah School of Engg and Tech, Dhauj, Faridabad-121004, Haryana
[2]M. Tech Scholar, Al-Falah School of Engg and Tech, Dhauj, Faridabad-121004, Haryana
[3]HOD (Computer Science and Engg), Al-Falah School of Engg and Tech, Dhauj, Faridabad-121004, Haryana

[1] atiya.parveen@gmail.com; [2] habib.sobia85@gmail.com; [3] saoud.hod.cse@gmail.com

Abstract— Electronic Voting are now being performed using World Wide Web in many countries of the world due to this advancement a voter need not to visit the polling place. But has to just logging on the computer with an internet connection. Also, this voting requires an access code for the e-voting through the advance report of a voter. To reduce these disadvantages, we suggest a process in which a voter, who has the wireless certificate issued in advance, uses its own mobile phone for an e-voting without the unique registration for a vote. In this paper, a polling scheme by means of mobile technology is resented as most fundamental application of GSM based Personal Response System, which allows a voter to cast his vote in simple and convenient way without the limit of time and location by integrating an electronic voting method with the GSM infrastructure.

Key Terms: - Voting; Mobile Terminal; Confidentiality; Anonymity

I. INTRODUCTION

In democratic countries, voting is an vital tool to collect and re-act people‘s views. In the elections, the election of member of the assembly, the head of local/state government election, and others, a voter can cast vote after going to the designated polling place and checking his identity. Conventionally, voting booth is used for casting votes in both centralized and distributed places. Voting is done under the supervision of authorized parties. Counting of votes is done manually once the election is over. But with the rapid growth of electronic voting system, computer technology and cryptographic methods can be used that substitute the occurrence and most significantly error-prone human Component. To increase the productivity and accuracy of voting processes, electronic voting systems were developed to help accumulating and counting the votes. It comprises Lever Voting Machines, Punched Cards for Voting, Optical Mark-Sense Scanners and Direct Recording Electronic (DRE) voting systems.

In this paper, we recommend an electronic voting system that lets a voter to be identified using a wireless certificate without furthermore registering when a user votes using his mobile device such as a mobile phone or a PDA. We also propose a process that guarantees the confidentiality of voter and the secrecy of vote content. By our electronic voting system, a voter can cast his vote more easily and conveniently than the existing electronic voting using internet, within the planned time period anywhere even when a voter is not able to access internet on a voting day. Our suggestion can be used in all kinds of elections national as well as state/local elections. Our goal is not to design a cryptographically provable protocol [1] but to demonstrate electronic voting model and to define a voting procedure.

II. EXISTING ELECTRONIC VOTING SYSTEM

A. Paper Based Process

The process, which is involved in the paper-based electoral system, is a rigorous one [2]. 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 [2]. 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 [3]. 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" [3]. 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) [3] 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 [3] 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 [4]. 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 [5] [6] 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. E-VOTING SYSTEM USING MOBILE TERMINALS

Fig. 1 is an illustration of an electronic voting system for electronic voting over mobile communication network. E-voting system includes a mobile terminal, a mobile communication server, and an e-voting device. A mobile terminal is a device that includes wireless certificate used to verify a voter's identity. A mobile communication server within mobile communication network connects a mobile terminal to an e-voting device for e-voting service. It makes a role in transmitting data used in the e-voting process to both entities. It is not allowed to give any change of data except for deleting ID of a mobile terminal coupled with voting. An e-voting device can be a secure system managed by national organization such as a board of elections or an election

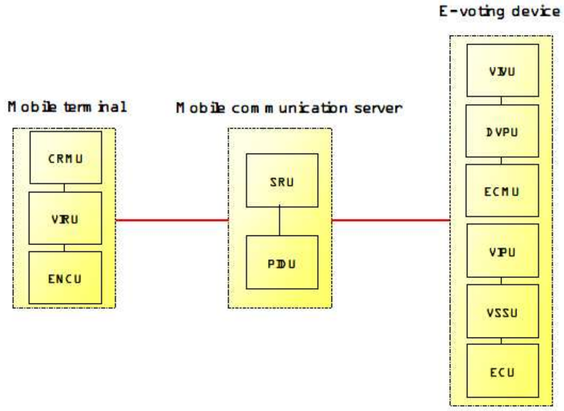

Fig 1 E-Voting using Mobile Terminal

A. E-Voting Device

E-voting device consists of 6 units for its internal functionality.

1. VIVU(Voter Identity Verifying Unit) -It verifies whether a voter is allowed to vote based on a wireless certificate received from a voter's mobile terminal over mobile communication network

2. DVPU (Double Voting Prevention Unit) - If a voter tries to access to e-voting device twice after he completes voting once, DVPU refuses a second attempt to verify his identity. This work happens if a voter accesses e-voting service again ever after already casting his vote at a polling place or finishing vote using his mobile phone.

3. EKMU (Encryption Key Management Unit) -This unit creates an encryption key to encrypt the vote content and transmits the key to a mobile terminal.

4. VIPU (Vote Information Providing Unit) - It provides vote information containing a list of possible voting selections or a list of candidates to a mobile terminal.

5. VSSU (Voting Selection Storing Unit) - It decrypts the encrypted vote content received from a mobile terminal. At this time, VSSU does not take identification information of voter since it was already removed in the mobile communication server. And, this unit stores the decrypted result to count votes after voting time is finished.

6. ECU (External Connection Unit) -This unit issues the wireless certificate to a mobile terminal. Or it may be connected to other device outside e-voting device to send a certificate to a mobile terminal.

B. Mobile Terminal

A mobile terminal includes CRMU, VIRU, and ENCU. A voter actually uses a cellular phone and PDA as a terminal.

1. CRMU (CeRtificate Management Unit) - This unit stores a voter's certificate containing a personal identification number. When e-voting process starts up, CRMU sends it to an e-voting device to prove that a voter is qualified to vote. This work is not done until a voter inputs a password or PIN to demonstrate that he

begins e-voting service using his own mobile terminal. Putting password prevents others from using the certificate fraudulently.

2. VIRU (Vote Information Receiving Unit) - VIRU receives a vote information and an encryption key from an e-voting device.

3. ENCU(ENCryption Unit)- This unit encrypts voter’s decision using the encryption key stored in VIRU and sends the encrypted vote content to the e-voting device.

C. Mobile Communication Server

A mobile communication server including SRU and PIDU connects a mobile terminal to an e-voting device over a mobile communication network.

1. SRU (Sending and Receiving Unit) -This unit receives an encryption key and vote information from the e-voting device and transfers it to the mobile terminal. Also, SRU receives encrypted vote content from the mobile terminal and sends it to the e-voting device.

2. PIDU(Personal Identification Deleting Unit) - It plays a part in deleting personal identification information received from the mobile terminal of voter before sending the encrypted content to the e-voting device.

In the e-voting system using a mobile terminal, a wireless certificate is used to verify a voter’s identity after a voter accesses to an e-voting device for the first time. So, the certificate should be beforehand issued by a certificate authority linked to ECU of e-voting device or by other authorized entity irrelevant to e-voting device. Also, it must be stored in the mobile terminal of voter’s own before a voter starts e-voting service. A wireless certificate can be used in other applications such as mobile commerce or mobile banking besides of e-voting service.

After verifying voter’s identity, an e-voting device selects one secret key among a group of secret keys or its public key and sends it to a mobile terminal of voter. A voter who received the key chooses one of vote information provided by an e-voting device and encrypts the vote content. At this time, encryption is done by using secret key shared between a mobile terminal and e-voting device or using public key of an e-voting device. And then, a voter sends encrypted vote content to the e-voting device. In this process, vote information on the screen of a mobile terminal can be different to voters according to voter’s place of residence, which is decided by referencing a current address of voter within a certificate.

When a mobile communication server receives encrypted vote content and ID of a mobile terminal, it always deletes ID of a mobile terminal and transmits only encrypted vote content to an e-voting device. And then, an e-voting device received an encrypted vote content can learn a vote content using a key which it created in the previous step.

IV. Voting Process Using Mobile Terminals

In this chapter, we propose e-voting process using a mobile terminal. Fig. 2 shows the procedure of e-voting between an e-voting device and a voter. It is as follows:

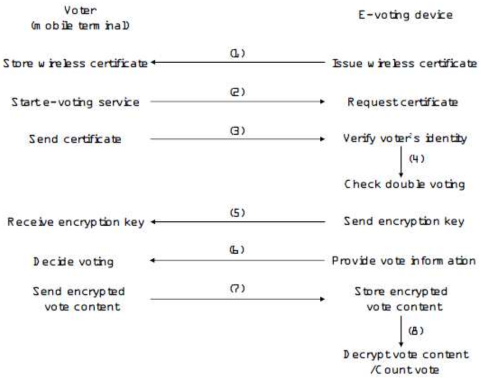

Fig. 2 E-Voting process using a mobile terminal

1. A wireless certificate is issued to a mobile terminal, that is, a voter has the certificate before commencing voting. The certificate should be kept in the mobile terminal for e-voting service.

2. E-voting service is started as soon as a mobile terminal connects to an e-voting device. If an e-voting device accepts the e-voting service, it requests a certificate to verify a voter’s identity.

3. A mobile terminal sends the certificate to the e-voting device. So, a voter proves that he is a qualified person to cast a vote.

4. If the voter's identity is verified and the voter is given the right to vote, an e-voting device checks if the voter is re-accessing an e-voting device.

5. The e-voting device selects and transmits an encryption key according to the encryption method to guarantee the confidentiality of the voter. Of course, this work is done after verifying the voter's identity and checking double voting of a voter.

6. After sending the encryption key, an e-voting device continuously transmits vote information containing a list of possible voting selections and supplemental information. And then, a voter decides his voting based on the vote information.

7. A mobile terminal encrypts the vote content and transmits the encrypted vote content to an e-voting device. An e-voting device does not reveal the encrypted vote content until voting time is finished. At this moment, a mobile communication server that received the encrypted vote content and the ID of a mobile terminal always deletes ID. That is, an e-voting device receives only content of voting.

8. When voting time has passed, an e-voting device decrypts the stored encrypted vote content and checks the voting selection to count the vote.

In the process 5, the encryption key management unit of an e-voting device creates a secret key and a key identifier and transmits them to a mobile terminal. This key is sent if encryption scheme based on symmetry key is applied. On the other hand, if e-voting process employs the scheme based on public key, that unit transmits the public key of an e-voting device to a mobile terminal. If a secret key is used for each voter, the relation between a voter and his key is revealed. This makes anonymity of a voter not to be satisfied. Thus, to avoid this, one encryption key can be generated on a time period basis and then the same encryption key is assigned to voters who access at a certain time period. As well, the same encryption key can be assigned to voters in the same district by checking the address of voters from their certificates. Same encryption key identifier is used for identifying the encryption key.

Fig.3 is a table showing an example of encryption keys depending on time periods, localities, or time periods and localities. Encryption keys can be generated by creating several encryption key groups.

V. Advantages of GSM SMS Voting to the Polling System

A. Reduced costs:

Instead of having thousands of polling stations scattered all over the country which will involve enormous logistics to is deployed deploy, the only 'polling stations' will be one counting center per service provider where the election polling software system, this makes it easier to monitor.

B. Increased participation and voting options:

People can vote from home or offices so no need of public holiday to enable people vote. Participation will be higher because people do not have to leave their home and stand on long endless queues. Participation will generally be higher than ever before. Many people do not vote just because of the stress involved.

C .Reduced Risk:

The risks associated with road travel such as road traffic accidents and late arrival of electoral resources due to unforeseen delays during deployment of polling stations will be avoided.

D. Reduced time Consumption:

Due to its electronic nature, the results of the Poling will be available immediately after voting with the GSM sms voting.

E. Greater speed and accuracy placing and tallying votes:

Possibility of rigging will be very low as compared with the ballot box system. The reasons are:

1) Every political office candidate will be allocated a number eg. NCP candidate: sms to 3005, BJP: sms to 5604, Congress: sms to 1009 etc.

2) An electronic voters' register (which is a primary requirement for the GSM sms system) will be used to control the rigging. Every voter will also register a particular GSM phone number in which he would use for voting during the elections.

3) To vote, voters will type their registration number as a sms message eg. 00030611 and send to the number of their candidate of choice. To confirm the vote, the voter will receive a confirmation message from the Counting Station that their votes have been received. This is the voting receipt.

4) During registration voters who don't have phones can register with designated handsets to be provided by service providers or use numbers of well-known friends. Once a number is used, it cannot be changed until after the voting exercise.

5) Possibility of multiple voting is not possible since voter registration number must match the GSM number used.

F. Provide Equal Opportunity:

Best of all, this process will guarantee that a new generation of political leaders will emerge at last. Since, it will provide an equal opportunity for all the political parties.

REFERENCES

[1] R. Storn and K. Price, Differential evolution – a simple and efficient heuristic for global optimization over continuous spaces. Journal of Global Optimization, 1997, vol.1, No. 4, pp. 341-359.

[2] https://encrypted.google.com/advantages of Gsm sms voting to Polling system

[3] X. Y. Cerone and P. Y. Zhang,‖Secure Electronic Voting for Mobile Communications,‖ Vehicular Technology Conference, 2006. VTC 2006-Spring. IEEE 63rd, Vol. 2, 2006, page(s):836 – 840.

[4] Hemlata Sahu, Anupam Choudhray,‖ Intelligent Polling System Using GSM,‖ International Journal of Engineering Science and Technology (IJEST), Vol. 3 No. 7 July 2011, pages 5641-5645

[5] Gentles, D and Suresh, S (2011). "Biometric Secured Mobile Voting", Proceedings of Second IEEE/IFIP Asian Himalayas International Conference on Internet, Kathmandu, Nepal.

[6] R. C. Eberhart and J. Kennedy, New optimizer using particle swarm theory, Proceedings of the 6th International Symposium on Micro Machine and Human Science, 1995, pp. 39-43.

[7] Y.Shi, Empirical study of particle swarm optimization. Proceedings of IEEE International Congress on Evolutionary Computation, 1999, vol. 3, pp.101-106.

[8] A. Ratnaweeta, S. K. Halgamuge and H. C. Watson, Self-organizing hierarchical particle swarm optimizer with time-varying acceleration coefficients. IEEE Transactions on Evolutionary Computation, 2004, Vol. 8, No. 3, pp.240-255.

[9] Hong-qi Li and Li Li, A Novel Hybrid Particle Swarm Optimization Algorithm Combined with Harmony Search for High Dimensional Optimization Problems. 2007 International Conference on Intelligent Pervasive Computing, 2007, pp.94-97.