A NOVEL VOTING SYSTEM USING SMS

Dr.M.Kamaraju, P.V.Subba Rao and T.Venkata Lakshmi

Dept.of Electronics and Communication Engineering
Gudlavalleru Engineering College, Gudlavalleru, Andhra Pradesh, India
{madduraju@yahoo.com,subbarao.4c6@gmail.com,tvlthota@gmail.com}

ABSTRACT

Electronic voting systems have the potential to improve traditional voting procedures by providing added convenience and flexibility to the voter. Numerous electronic voting schemes have been proposed in the past, but most of them have failed to provide voter authentication in an efficient and transparent way. 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 for mobile telephony, but also for other mobile applications that exploit the mature GSM infrastructure. In this paper, the electronic voting scheme using GSM mobile technology is presented. By integrating an electronic voting scheme with the GSM infrastructure, we are able to exploit existing GSM authentication mechanisms and provide enhanced voter authentication and mobility while maintaining voter privacy. The objective of this project is to avoid the queue in voting time. Voting machines provide easy access to cast the vote by using mobile phone.

KEYWORDS

GSM, Mobile, LCD, Subscriber Identity Module (SIM)

1. INTRODUCTION

Voting is a vital part of the democratic process. As such, the efficiency, reliability, and security of the Technologies involved are critical. Traditional voting technologies include hand-counted paper ballots. These paper-based systems can result in a number of problems, including: Unacceptable percentages of lost, stolen, or miscounted ballots, Votes lost through unclear or invalid ballot marks, Limited accommodations for people with disabilities

Today, the development and widespread use of information technologies is changing the way people view voting processes and, ultimately, the way they vote. At the forefront of these new technologies is poll-site direct recording electronic (DRE) voting and remote Internet-based voting. In democratic societies, voting is an important toll to Collect and reflect people's opinions. Traditionally, voting is conducted in centralized or distributed places called voting booths. Voters go to voting booths and cast their votes under the supervision of authorized parities.

Jan Zizka (Eds) : CCSIT, SIPP, AISC, PDCTA - 2013
pp. 297–303, 2013. © CS & IT-CSCP 2013 DOI : 10.5121/csit.2013.3634

The votes are then counted manually once the election has finished. With the rapid development of computer technology and cryptographic methods, electronic voting systems can be employed that replace the inefficient and most importantly error-prone human component. To increase the efficiency and accuracy of voting procedures, computerized voting systems were developed to help colleting and counting the votes. These include lever voting machines, punched cards for voting, optical mark-sense scanners and direct recording electronic (DRE) voting systems.

For a variety of reasons voters may be unable to attend voting booths physically, but need to vote remotely, for example, from home or while travelling abroad. Hence, there is grade demand for remote voting procedures that are easy, transparent and most importantly, secure. Today, the most common way for remote voting is postal voting, where voters their votes by post. However, it lacks proper authentication and involves a time-consuming procedure. To improve mobility, address security problems of remote voting procedures and systems. We present an electronic voting using GSM. With more than one billon users, the GSM authentication infrastructure is the most widely deployed authentication mechanism by far. We make use of well-designed GSM authentication infrastructure to improve mobility and security of mobile voting procedures.

1.1 Characteristics

Voting system using sms offer multiple advantages over traditional paper-based voting systems-advantages that increase citizen access to democratic processes and encourage participation.

Reduced costs - E-voting systems reduce the materials required for printing and distributing ballots. Internet based voting, in particular, offers superior economies of scale in regard to the size of the electoral roll.

Increased participation and voting options - E-voting offers increased convenience to the voter, encourages more voters to cast their votes remotely, and increases the likelihood of participation for mobile voters. Additionally, it permits access to more information regarding voting options.

Greater speed and accuracy placing and tallying votes -E-voting's step-by-step processes help minimize the number of miscast votes. The electronic gathering and counting of ballots reduces the amount of time spent tallying votes and delivering results.

Flexibility - E-voting can support multiple languages, and the flexible design allows up-to-the minute ballot modifications.

2. VOTING SYSTEM USING SMS

In this section, we review the GSM security features, in particular the authentication function.

2.1 Security Features in GSM

GSM is a digital wireless network standard widely used in European and Asian countries. It provides a common set of compatible services and capabilities to all GSM mobile users. The services and security features to subscribers are subscriber identity confidentiality, subscriber identity authentication, user data confidentiality on physical connections, connectionless user data

confidentiality and signalling information element confidentiality. They are summarized as follows: Subscriber identity confidentiality is the property that the subscriber's real identity remains secret by protecting his International Mobile Subscriber Identity(IMSI), which is an internal subscriber identity used only by the network, and using only temporary identities for visited networks. Subscriber identity authentication is the property that ensures that the mobile subscriber who is accessing the network or using the service is the one claimed. In our proposed GSM mobile voting scheme, communication between the mobile equipment and the GSM network uses standard GSM technology. Hence GSM security features apply. Among which, the subscriber identity authentication feature is particularly used in the protocol. A random challenge RAND is issued when a mobile subscriber tries to access a visited network. The Authentication Centre (AC) computes a response SRES from RAND using an algorithm A3 under the control of a subscriber authentication key K_i, where the key K_i is unique to the subscriber, and is stored in the Subscriber Identity Module (SIM) on the Mobile Equipment (ME), as well as the Home Location Register (HLR). The ME also computes a response SRES from RAND as well. Then the value SRES computed by the ME is signaled to the visited network, where it is compared with the value SRES computed by the AC. The access of the subscriber will be accepted or denied depending upon the result of comparing the two values. If the two values of SRES are the same, the mobile subscriber has been authenticated, and the connection is allowed to proceed. If the values are different, then access is denied.

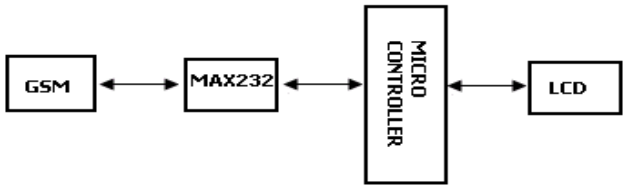


Fig.1. Block Diagram of Voting System using SMS

This paper is designed with Supporting GSM Modem LCD

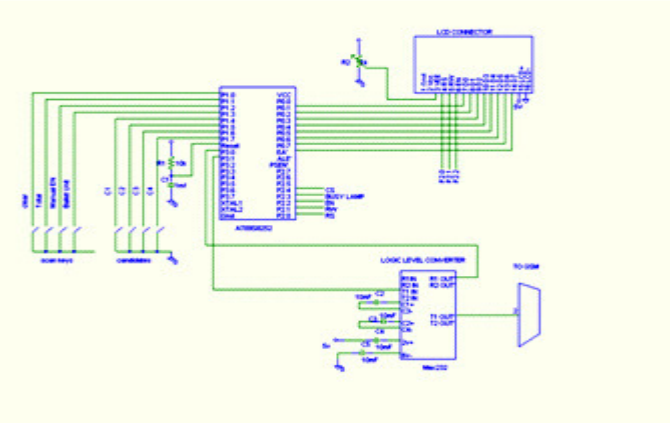
Here two mobile phones are used. One is transmitter another one is receiver. The receiver mobile is interfaced with Microcontroller AT89s8252. Transmitter mobile is voter's mobile. If the voter wants to vote, then he has to enter their correct voter ID number, password and then enter candidates ID number in this message for enrol his vote. If he sends his message along with these details to receiver mobile number, the microcontroller unit will read the message from the receiving mobile through serial port and checks the ID number, password; if both are matched the microcontroller will count the vote for selected candidate and store it in database. If the ID number doesn't matched or already voted means the microcontroller unit will reject that message and do not count the vote. Before this we have to create the database in microcontroller for this application in Assembly language.

3. IMPLEMENTATION

3.1 Hardware

The receiver mobile is connected to the microcontroller unit through MAX 232 com 3 port using DB9 connector. MAX 232 is used for converting the RS logic voltage which is coming from microcontroller to TTL logic voltage is given to Microcontroller and vice versa. Scan Keys are used to display the total number of votes in LCD if we gave the correct password.LCD is

connected to Microcontroller.LCD 3rd pin is connected to variable resistor to control the brightness of the LCD. It is a 32 characters display 16 characters per line. 9th pin is used to reset the Microcontroller for normal voting system. Microcontroller is operating at 12 MHZ clock frequency. Ballet unit is used for normal voting purpose. Fig.2.2 shows the circuit diagram of on-line voting system.



Power Supply

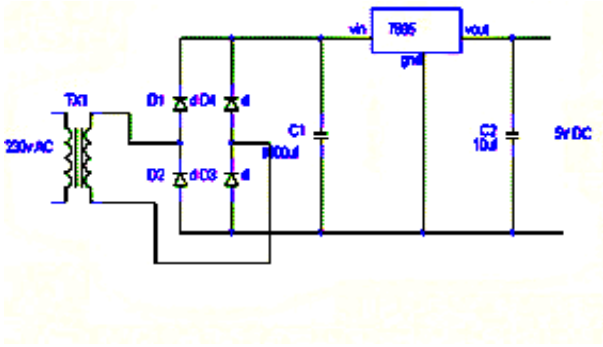


Fig. 2. Implementation of the Voting System using SMS

TABLE 1. Commands Description

Command	Description
AT	Check if serial interface and GSM modem is working.
ATE0	Turn echo off, less traffic on serial line.
AT+CNMI	Display of new incoming SMS.
AT+CPMS	Selection of SMS memory.
AT+CMGR	Read new message from a given memory location.
AT+CMGS	Send message to a given recipient.
AT+CMGD	Delete message.

3.2 Software

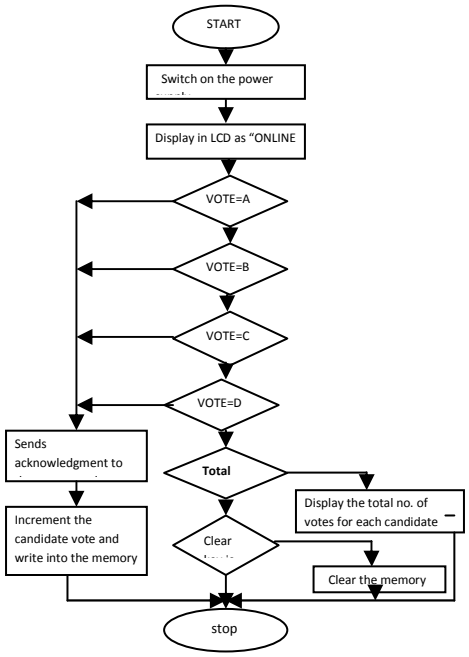


Fig. 3 Flow chart of Voting System using SMS

Switch on the power supply, display in LCD as "VOTING SYSTEM USING SMS". If received vote is "A", send acknowledgement to the corresponding voter as "THANKU FOR VOTING". Increment the candidate vote and write into the memory. The procedure is same for different candidates. If total key is used to display the total no. of votes for each candidate and the total no. of votes. Finally counting is over, clear key is used to clear the memory.

4. RESULTS

By using this project conduct voting and count the total number of votes per a particular candidate. The voter can vote to the particular candidate from any place in a given time. If the voter sms the correct password then his or her vote is counted and got acknowledgement as "Thank you for voting". If the voter sms the wrong password then his or her vote is not counted and will not provide any acknowledgement. Fig.3 shows the Photograph of Voting System using SMS.

Fig. 3 Photograph shows Voting system using SMS

Acknowledgments. Fig.4 shows the Photograph of Acknowledgement given **to** the Voter

Fig.4. Photograph shows Acknowledgement given to the Voter

Fig.5 shows the Photograph of total number of Votes for each candidate.

Fig. 5. Photograph shows the Total Number of Votes

5. CONCLUSION

By using this paper security performance is improved, avoid the security tensions and also avoid the queue in the voting time at polling booth. Voter can cast his or her vote easily from any place in given time. It can saves the time of the voter and avoid the forgery votes. Authentication is always a difficult requirement to fulfil for remote voting schemes, most of which apply a public-

key based signature scheme for voter authentication. In our scheme, by using the existing GSM authentication infrastructure, the public-key overhead is largely reduced. Our scheme also enhances the security and provides more mobility and convenience to voters. In this paper, we presented the basic structure and protocol of our GSM based mobile voting system.

REFERENCES

[1] Burmester, M., Magkos, E., :Towards secure and practical e-elections in the new era. In D. Gritzalis, editor, Secure Electronic Voting, pages 63–72. Kluwer Academic Publishers, (2003).

[2] Chaum, D.,: Untraceable electronic mail, return addresses, and digital pseudonyms. Communications of the ACM, 24(2):84–88, February (1981).

[3] Rivest, R., Sherman, A., editors, Advances in Cryptology—Crypto '82, pages 199–203, New York,. Plenum Press, (1983).

[4] Chaum, D., : The dining cryptographers problem: Unconditional sender and recipient untraceability. Journal of Cryptology, (1):65–75, (1988).

[5] Cranor, L., Cytron,L.F., Sensus: A security-conscious electronic polling system for the internet. In Proceedings of IEEE 30th Hawai'i International Conference on System Sciences (HICSS-30), pages 561– 570, January (1997).

[6] ETS 300 506. Security aspects (GSM 02.09 version 4.5.1), Digital cellular telecommunications system (phase 2), (2000).

[7] Fujioka, T., Okamoto, K.,Ohta :A practical secret voting scheme for large scale elections. In J. Seberry and Y. Zheng, editors, Advances in Cryptology—Auscrypt'92, volume 718 of Lecture Notes in Computer Science, pages pp. 244–251, Gold Coast, Queensland, Austrailia, 13-16 December 1992. Springer Verlag,(1992).

[8] Hirt ,M., Sako, K.,: Efficient receipt-freesvoting based on homomorphic encryption. In B. Preneel, editor, Advances in Cryptology— EUROCRYPT '00, volume 1807 of Lecture Notes in Computer Science, pages 539 556. Springer-Verlag, May (2000).

[9] Jefferson, D., Rubin, A. D., Simons, B., D. Wagner.,: A Security Analysis of the Secure Electronic Registration and Voting Experiment (SERVE), (2004).

[10] Lin, Y., Chlamtac,I.,:Wireless and Mobile Network Architectures. Wiley, (2000).

[11] A. J. Menezes, P. C. Van Oorschot, and S. A. Vanstone. Handbook of Applied Cryptography. CRC Press, Inc., (1996).

[12] Naor, M.,: Bit commitment using pseudo-randomness (extended abstract). In G. Brassard, editor, CRYPTO '89: Proceedings on Advances in cryptology, pages 128–136. Springer-Verlag New York, Inc., (1989).