Secure Mobile Based Voting System

Manish Kumar[1]*, T.V.Suresh Kumar[1], M. Hanumanthappa[2], D Evangelin Geetha[1]

ABSTRACT

The foundation of a strong democracy is an informed and engaged citizenry. And what better way to both inform and engage citizens than through the power of today's information and communication technologies? Citizens around the world recognize and embrace the benefits of e-Government services such as online tax filing, license renewal, and benefits claims. Now governments are initiating strategies that support e-democracy-and in doing so, engaging more citizens in democratic processes. This brief addresses the highly formal processes of e-democracy-in particular e-voting to offer governments and democratic-based entities worldwide the infrastructures, applications, and services necessary to implement and manage reliable, secure e-voting systems. In this paper, an electronic voting scheme using GSM based 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.

Keywords: - Mobile Equipment (ME), International Mobile Subscriber Identity (IMSI), Home Location Register (HLR), Authentication Centre (AC), 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.

1.1. The benefits of e-voting

E-voting systems offer multiple advantages over traditional paper-based voting systems-advantages that

[1] Dept. of Master of Computer Applications, M. S. Ramaiah Institute of Technology, Bangalore-560 054, India
[2] Dept. of Computer Science and Applications, Central College Campus, Bangalore University, Bangalore-560 001, India
* *Corresponding Author:* (E-mail : manishkumarjsr@yahoo.com, Telephone: +91 9916925341)

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.
- **Greater accessibility for the disabled -** Because they support a variety of interfaces and accessibility features, e-voting systems allow citizens with disabilities-especially the visually impaired-to vote independently and privately.
- **Flexibility -** E-voting can support multiple languages, and the flexible design allows up-to-the-minute ballot modifications.

2. Background

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 signaling 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. This feature is to protect the network against unauthorized use.

Data confidentiality is the property that the user information and signaling data is not disclosed to unauthorized individuals, entities or processes. This feature is to ensure the privacy of the user information.

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.

The subscriber identity authentication in GSM is based on a challenge response 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 *Ki*, where the key *Ki* 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.

2.2 Basic Mobile Voting Scheme

In a mobile environment, the mobile device have limited computational abilities, so employing schemes with large computation is not practical. Therefore, we develop our GSM mobile voting scheme based on a blind signature voting scheme presented by Fujioka et al. in 1992. It is a prototype system based on blind signatures. It was intended as a practical secret voting scheme for large scale elections. There are voters, an administrator, and a counter participating in the scheme. In this scheme, digital signature, blind signature and bit-commitment mechanisms were used. As these mechanisms are also the primitive cryptographic elements, in our proposed scheme a brief description of these mechanisms is given :

Digital signature is an essential cryptographic primitive for authentication, authorization, and non-repudiation. It binds a message and a secret known only to the signer in a way that the public can verify that the message has been signed by the signer without knowing the secret. In a public-key encryption based digital signature scheme, the secret is the private key, and the information that is used by the public to verify the signature is called the public key.

Blind signature is a signature scheme with special functionality, where the signer has no knowledge of the message he signs and the signature. Hence, the signed message cannot be associated with the sender. A blind signature protocol usually includes three steps: blinding, signing and unblinding. For example, sender A wants to get a blind signature from signer B upon message m. Functions g and h are blinding and unblinding functions that are only known to A, and $SB(x)$ represents the normal digital signature of B on x. First, sender A blinds the message m with the blinding function g , namely $g(m)$, and sends it to signer B. Signer B signs $g(m)$ with B's signature, as $SB(g(m))$, and sends it back to sender A. Finally, A unblinds it with the unblinding function h, as $h(S\ B(g(m)))$, where $h(S\ B(g(m)))=S\ B(m)$. In the end, sender A obtains signer B's signature upon message m, without signer B knowing the message m and the signature on m, so the signer cannot link the signed message m to the sender A.

Bit-commitment is the basic component of many cryptographic protocols. In a bit-commitment scheme, the sender A sends an encrypted message m to the receiver B in such a way that when later on A sends B the key to decrypt the message, B can be confident that it is the right key to the message m and the decrypted message B gets is the same message m that A committed to with B.

3. Security Requirements for Voting Schemes

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.

4. Proposed Mobile Voting Scheme

In this section, we introduce our GSM mobile voting scheme. In this scheme, GSM is used for the voting system to introduce voter mobility and provide voter authentication. We start by introducing the different components of the scheme, followed by stating a list of assumptions on which the protocol is based. Then the proposed voting scheme is described in detail.

4.1 The Components

- **Mobile Equipment/Voting Device (ME)**: In electronic voting schemes, voters need to use dedicated voting devices to cast their votes electronically, for instance, Internet connected computers or DRE machines. In our scheme, the voting device corresponds to the GSM mobile equipment (ME), which consists of a GSM SIM card .
- **Authentication Centre (AC)**: AC is an entity within the GSM network. AC generates the authentication parameters and authenticates the mobile equipment.
- **Verification Server (VS)**: VS belongs to the voting authority, who organizes the voting event. It verifies the legitimacy of the voter and issues a voting token to the voter.
- **Collecting and Counting Server (CS)**: CS is the server that collects and counts the votes to give the final result. CS's action need to be audited by all candidate parties.

Our system is based on a number of assumptions. We assume that the proposed Mobile Voting scheme is part of a voting system, and that voters can choose to vote through different methods, for example, the voting booth. If voters want to vote through Mobile, they have to be registered subscribers. This means that the voters have already registered their real names and addresses with their mobile operators by presenting their eligible credentials at the time of subscription. We assume that the Mobile operator is trusted to authenticate the mobile users for the purpose of voting and send the correct information to VS and CS.

4.2 Overview

In this section, we outline our GSM mobile voting scheme.

Voters Authentication Phase:- In this phase GSM service provider is responsible to verify the authenticity of the voters. If the voter is authentic then only he will be allowed to participate in the next steps of voting. This phase is default phase and it works automatically once user try to use the services of particular GSM service provider.

Voting Phase: In this phase, the voter installs the application, fills in the ballot, and obtains a voting token from VS without revealing the vote. In this paper, we consider the ballot an electronic equivalent of a paper ballot, which is an electronic form with the voter's choice of the candidates. We also define the voting token as the encrypted ballot signed by VS.

- The voter fills in the ballot, encrypts the ballot, blinds it using the blinding technique of a blind signature scheme, and sends it to AC through Mobile.

- AC authenticates the voter, signs the encrypted ballot and forwards the encrypted ballot along with the signature to VS.
- VS checks the signature of AC and the eligibility of the voter, signs the encrypted ballot with its private key. Here VS generates one ID for this ballot with one asymmetric key. VS encrypt the ballot, ballot ID and public key of generated asymmetric key which is generated for this particular ballot and sends the signed encrypted ballot with added attributes back to the voter. VS also send the pair of ballot ID with the encrypted private key (using CS public key) to CS .
- The voter checks the signature and retrieves (unblind) the VS- signed ballot, ballot ID and Public key from the message using the retrieving (unblinding) technique of the blind signature scheme.
- The voter sends the voting token along with ballot ID and the public key correspond to this particular ballot ID to AC, this three items ballot, ballot ID and Public key will be encrypted with CS's public key to avoid AC decrypting the ballot and compromising the privacy of the voter.
- Upon receiving the encrypted key and the voting token, CS keeps its safe till counting start as per the predefined schedule.

Counting Phase At the scheduled time of counting CS decrypt the ballot and checks whether the voting token is valid or not. If it is valid it will be counted else it will be rejected.

In entire process describe above it is strongly require that whenever AC is sending data to VS. Sender Identification will not be revealed at any time. So even if some body track a ballot can be identified with the particular AC but not with the particular User and a single AC can have number of users.

4.3 The GSM Voting Protocol

In this section, we describe the GSM mobile voting scheme in detail.

Initially, voter *Vi* fills in a ballot generated by the application on the mobile voting device ME. The ME completes the ballot by committing it to *xi* as $xi = B(vi, ki)$ using a randomly chosen key *ki*, and blinds *xi* by computing $ei = g(xi\ ri)$. Here, *ri* is a randomly chosen blinding factor. Both *k i* and *r i* are generated by the ME within the application. Then *Vi* sends $< ID\ I\ , ei >$ to AC through Mobile

Upon receiving the message from voter *V i*, AC authenticates the ME and checks the Home Location Register (HLR), where the subscriber's information is stored. Then AC applies its signature and forwards it to VS along with its ID as $< IDi\ , ID\ AC, S\ \ AC(e\ i) >$.

By checking the signature of AC, VS is confident that AC has already authenticated the voter. It then verifies the eligibility of *V i* to vote by checking the database to see if the voter has voted before, and adds *Vi*'s information to the database as $< ID\ i,\ e\ i >$. Most importantly in this phase, VS issues a voting token to the eligible voter without revealing the vote *vi*, so after verifying the eligibility of the voter,VS generates one ID for this ballot with one asymmetric key. VS encrypt the ballot, ballot ID and public key of generated asymmetric key which is generated for this particular ballot and sends the signed encrypted ballot with added attributes back to the voter. VS also send the pair of ballot ID and the encrypted private key to CS. So VS sends back to the voter *V i* as $si = S\ (ei,,\mathrm{ID}ei,,Pu)$.Where P*u* is public key of generated asymmetric key which is generated for this particular ballot ID. VS also send the pair of ballot ID with the encrypted private key (using CS public key) to CS $(\mathrm{ID}ei, E_{Pu}(Pk))$

Upon receiving the message from VS, the voter *Vi* unblinds *si* to obtain the signature $y\ i = h(si, ri)$. If *y i* is a valid signature of VS upon *xi*, the voter can use it as a voting token to cast the vote in the Voting Phase.

Otherwise, voter *Vi* reports to the voting authority, in provision of the evidence of < *xi,yi* >.

Now voters can cast their votes with the verified token anytime they want before the voting deadline.

Vi encrypts $y\,i = h(si,ri) = (ei,,\mathrm{ID}ei,,\mathrm{P}u)$ with the CS's public key $\mathrm{P}_k\,CS$ as $f = \mathrm{P}_k\,CS\,(ei,,\mathrm{ID}ei,,\mathrm{P}u)$, and send it to AC. By encrypting $y\,i$ with $\mathrm{P}_k\,CS$, AC cannot observe the voter *Vi*'s vote, and only CS can reveal $y\,i$ by decrypting $f\,i$ with its private key.

After receiving the message, CS checks if $y\,i$ is a valid VS's signature on $x\,i$. If it is, CS publishes the list of valid ballot ID which individual user can use to confirm that whether there vots has been accepted or not.

After the voting phase CS reveals $f\,i$ using P*kcs* (CS's private key).CS can verify the authenticity of each ballot with the ballot ID and public key pair with the correspondent ballot ID and private key pair received from the VS.

5. Security Analysis

In this section, we discuss how and to what extent the protocol fulfils the security requirements .

- **Authentication** *Only the authorized voters can vote.* First, voters are authenticated through GSM, which assures that voters are who they claim to be. The authentication of the voter is as good as Mobile Service provider or GSM can provide. Second, the eligibility of voters is checked by VS. This prevents voters from voting more than once.
- **Privacy** *All votes remain secret while the voting takes place and each individual vote cannot be linked to the voter who casts it.* The proposed scheme is divided into three phases, and they are separated in time. In the voting phase, a blind signature is applied to the vote in a way that vote is not linkable with voter and is signed by the AC without revealing the vote and in the same way it is signed by the VS. In the next step the communication between voters and CS achieves anonymity with the help of AC. The voter $V\,i$ sends the vote encrypted with CS's public key *kCS* to AC, so the AC is not able to reveal vote $v\,i$. Also, CS has no direct communication with voter *Vi*, so CS cannot tell which voter casts the vote. Hence, for all the components of the voting system, if the Voters cannot be linked with the vote *vi*, the privacy of the voter is protected.

6. Concluding Remarks

We proposed a mobile voting scheme, where the Mobile service provider authentication infrastructure is used to provide voter authentication and improve voter mobility. Authentication is always a difficult requirement to fulfill for remote voting schemes, most of which apply a public-key based signature scheme for voter authentication. In our scheme, by using the existing authentication infrastructure. Our scheme also enhances the security and provides more mobility and convenience to voters. Where the voters' privacy is protected by applying a blind signature scheme. However, further work is needed to address the importance we place in the trust on the AC. In future work, we will discuss more on end-user device (ME) and application security.

References

1. Fujioka, T. Okamoto, and K. Ohta. (1992) A practical secret voting scheme for large scale elections. In J. Seberry and Y. Zheng, editors, Advancesin Cryptology Auscrypt'92, volume 718 of Lecture Notes in Computer Science, pages pp. 244–251, Gold Coast, Queensland, Austrailia, 13-16. Springer-Verlag.
2. Chaum. D (1983) Blind signatures for untraceable payments. In D. Chaum,R. Rivest, and A. Sherman, editors, *Advances in Cryptology*—Crypto'82, pages 199–203, New York, 1983. Plenum Press.

3. Jefferson, D., Rubin, A D, Simons, B. and Wagner. D (2004) A Security Analysis of the Secure Electronic Registration and Voting Experiment (SERVE), ETS 300 506. Security aspects (GSM 02.09 version 4.5.1), *Digital cellular telecommunications system* (phase 2), 2000.
4. Hirt M and Sako, K. (2000) Efficient receipt-free voting 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,
5. Lin, Y. and Chlamtac, I. (2000) *Wireless and Mobile Network Architectures*. Wiley Publications

About the Authors

Manish Kumar is a faculty in MCA Department, M.S. Ramaiah Institute of Technology, Bangalore, India. His areas of interest are Cryptography and Network Security, Distributed and Parallel Processing, Mobile Computing, E-Governance and Open Source Software. His specialization is in Distributed Parallel Processing. Before joining teaching profession, he worked on various software development projects for the government and private organizations. He worked on the R&D projects related on theoretical and practical issues about a conceptual framework for e-mail, website and cell phone tracking, which could assist in curbing misuse of information technology and cyber crime. He has published several papers in International and National Conferences.

T V Suresh Kumar is working as a Professor and HoD in Department of MCA, M.S.Ramaiah Institute of Technology. His areas of interest are Software Performance Engineering, Object Technology, Distributed Systems and Reliability Engineering. He worked on various software development and research project of DRDO,CASSA etc.. He is visiting faculty in various universities and reputed software development organization. He has published many papers in National, International conferences and Journals.

M. Hanumanthappa is currently working as a faculty with the Department of Computer Science and Applications, Bangalore University, Bangalore, India. He has over 12 years of teaching (Post Graduate) as well as industry experience. His areas of interest include mainly Data Structures, Data Base Management system, Data Mining and Programming Languages. Besides, he has conducted a number of training programmes and workshops for computer science students/faculty. He is also the member of Board of Studies/Board of Examiners for various universities in Karnataka, India. He has published many papers in National, International conferences and Journals. He is also doing his PhD in Data Mining.

D Evangelin Geetha received MCA degree from Madurai Kamaraj University,India in 1993. Pursuing Ph.D in Computer Applications from Visvesvaraya Technological University, Belgaum, India. Her areas of interest are software performance engineering, Object Technology, Distributed Systems. She is Currently working as Assistant Professor in MCA Department, M S Ramaiah Institute of Technology, Bangalore. She has published several papers in National, International conferences and Journals.