MOBILE BASED E-DEMOCRACY: THE IBB/PMA E-VOTING SYSTEM

Panayiotis Alefragis, Vassilis Triantafillou and Nikolaos Voros

Department of Telecommunication Systems & Networks
Technological Educational Institution of Messolonghi
Varia, Nafpaktos, Greece
{alefrag, triantaf, voros}@teimes.gr

Abstract

In the field of electronic democracy, significant part of the research activity focuses on the ability to conduct secure and trustworthy electronic election procedures. This paper presents the extension prototype of an electronic voting system, called *IBB/PMA Electronic Voting System* that enables cellular phones and mobile devices to act as voting casting devices. The system takes into consideration significant properties of modern e-voting schemes such as security, legitimacy and vote integrity. The aforementioned properties of the voting process are guaranteed through a brand new technique named *Identical Ballot Boxes with Physical Multiple Administrators*. The paper provides an overview of the system, design adaptations required to facilitate mobile devices and implementation experience.

Keywords: e-voting, electronic voting schemes, ballots, cellular phones, java micro edition

1. Introduction

The advent of internet and its penetration into modern societies has changed radically not only the way people behave, but also the traditional relationship among people. As a result, traditional social constructs are directly influenced by the appearance of modern technologies. Electronic democracy constitutes one representative example that indicates the aforementioned cultural evolution. Part of this trend, is the work presented in this paper, which refers to a mobile electronic voting system. An electronic voting system can be defined as *an election system that uses electronic ballots to allow voters to transmit their ballot to election officials over the Internet*. For systems belonging in this category, it is important to rely in state of the art infrastructure and technology in order to allow fair, secure and trustworthy electronic elections.

The next sections provide an insight in the design details of the system proposed. The rest of the paper is organized as follows: Section 2 provides the rationale of the IBB/PMA voting system, while in Section 3 the specifications of the system are presented. In Section 4 the underlying architecture is detailed. Section 5 and Section 6 present the system from the perspective of the administrator and the voter

respectively. Finally, Section 7 concludes by referring to the potential improvements of the IBB/PMA voting system.

2. Rationale

The proposed system is called *IBB/PMA Electronic Voting Scheme (Identical Ballot Boxes/Physical Multiple Administration Electronic Voting System)* and has been designed to allow large scale election procedures, in a manner that will be compliant with the traditional way of voting in national elections. The importance of the specific system is that it enables citizens to participate in the election process without essentially be physically present. The latter, can lead to a cost efficient election process for both governments and citizens.

In literature, there are several electronic voting schemes that address various issues of electronic election procedures [Dutton et al (1999)][Becker and Slaton (2000)]. Most of the existing approaches are oriented towards identifying the fundamental problems associated with the adequate level of security (anonymity, authentication, data security, tractability, etc.), while many of them concentrate on the ability of an electronic system to handle them [Cramer et al (1996)][Shoenmakers (1999)].

The main goal of the IBB/PMA Voting System is to implement an electronic voting process that resembles the traditional voting procedures. One of the main properties of the proposed system is the fact that, in contrast to existing similar systems, it relies on the use of a technique called *Identical Ballot Boxes with Physical Multiple Administration* [Alefragis et al., (2004), (2005)]. Its prime advantage is that it makes use of the aforementioned technique in order to prevent possible corruption of the voting procedure.

The aim of our late effort, was to create a working electronic voting system that uses cellular phones or mobile devices that can execute java micro edition (J2ME) bytecode as ballot casting devices. The proposed implementation is graphics based and provides the user with a simple, self-explanatory user interface. Older mobile voting applications, provided a elementary SMS-based interface where voting typically involved sending a SMS to an arbitrary number.

3. IBB/PMA System architecture

The IBB/PMA system is implemented as a web based application system that follows the 4-tier model. The system was implemented using J2EE5 [Sun Microsystems (2005)] using Hibernate [Hibernate (2005)] for the persistence mechanisms and Bouncy Castle [Bouncy Castle (2006)] as the security library. The system is organized in 4 different layers (client–tier, presentation-tier, application-tier and data-tier) [Sun Microsystems, (2000)]. The system relies on an open platform architecture

by supporting different operating systems and is designed under the international accepted standards for HTML [W3C Recommendation, (2002)], Servlet 2.4 and JSP 2.0 [Sun Microsystems (2003)].

As in every e-voting system, security concerns play the main role in designing the IBB/PMA System. In order to achieve the required security level (Alefragis et al., 2004) HTTPS over SSLv3.0 has been employed in the communication sessions between the clients and the servers of the system. The exact architecture of the IBB/PMA System is outlined in Figure 1.

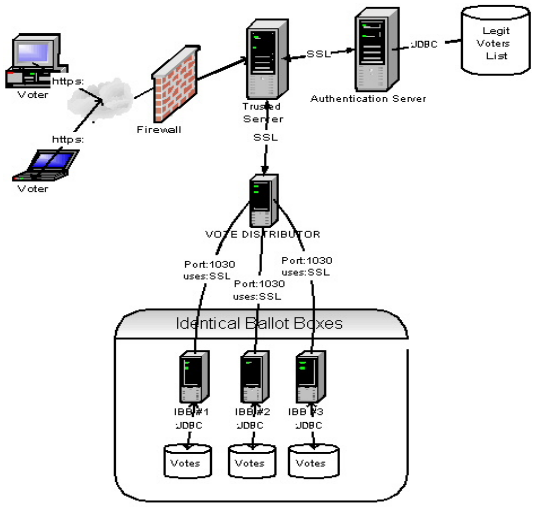

Figure 1 Architecture of the IBB/PMA System

3.1 Authentication Server

The authentication server is responsible for the initiation and culmination of the voting procedure, is responsible for the authentication of users, from its legit voters list and the acceptance of voting sessions. Moreover, the authentication server maintains the PMA voting key pair to decipher the votes and proceed to the tabulation of the results.

3.2 Trusted Server

The trusted server functions as the intermediate level between the voter, the authentication server and the Identical Ballot Boxes. It is considered as one of the most significant elements of the IBB/PMA Voting System as it ensures that both privacy and democracy attributes are met (Alefragis et al., 2004). It guarantees the secure communication (using SSL 3.0 protocol) among the constituent parts of the

IBB/PMA System. To support the mobile environment, an SMS gateway module was implemented in order to support mobile phones that do not have a GPRS connection. The SMS gateway, has been implemented to use simplified XML based messages and creates a transparent layer for the application to communicate with the mobile devices.

3.3 Vote Distribution Server

The vote distribution server is responsible for multiplication of the submitted vote, before the copies are registered with the Identical Ballot Boxes. It receives an encrypted message that consists of the encrypted vote and control information, replicates the vote and casts it in the IBBs. Upon successful completion, it returns a completion message, informing the voter that his/her vote has been registered and that it will be tallied in the tallying procedure.

3.4 Identical Ballot Boxes

The Identical Ballot Boxes hold ciphered votes, encrypted with the PMA voting key and the ciphered Identification Card Number, encrypted with a user supplied 5 digit key. It is designed to accept connections from the vote distribution server and ensures an acceptable level of security as far as remote vote manipulation is concerned. In the current version of the system, it has been implemented using Hibernate, JDBC 3.0 and MySQL v5.

3.5 Mobile Voting Application

The mobile voting application is responsible to interact with the voter. It performs the connection to the trusted server, allows legitimate voters to perform the voting procedure, informs them on the state of their voting session and returns to the user a receipt that may be used in the verification phase. It is equipped with an encryption algorithm responsible for both vote and personal identification information encryption.

All MIDP 2.0 implementations support HTTPS over SSLv3. Our server has already been using SSLv3 to communicate with the web based client. If a GPRS connection is available, the mobile application can use the same mechanism, so we decided to provide it as an option for the mobile application as well. The client protocol at the application level uses XML based messages. In J2ME, as in J2SE, IO streams are the primary available mechanism to read and write streams of data. The MIDP generic connection framework creates a platform that abstracts the details of networking mechanisms and protocols from the application. If no GPRS connection is available, the same protocol is emulated by sending and receiving SMS messages to/from the

trusted server transparently from the main application. In Figure 2 a high level class diagram of the mobile application is presented.

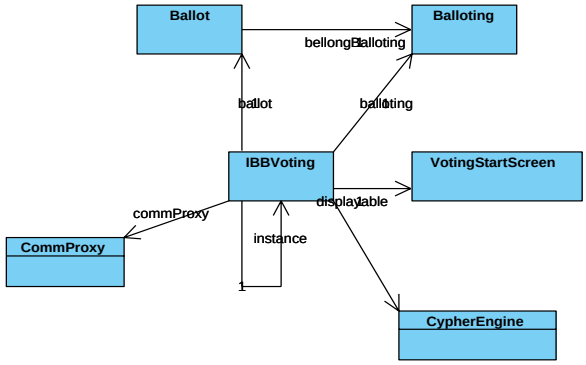

Figure 2 High Level Mobile Applications Class Design

4. IBB/PMA System specification

The IBB/PMA Voting System complies with laws of the Greek legislation both for national and local voting procedures. The system specifications have emerged as a result of an extensive analysis of the election processes followed in both cases. With respect to the ACM Statement of Voting Systems [ACM Council, (2004)], the IBB/PMA Voting System is designed to emulate the classical pen and paper voting approach in a digital form, as a method with enhanced security and procedure clarity. In any given election procedure there exist pre-defined constraints:

- a voting session is valid for a specific time,
- people have the right (in some countries the obligation) to vote,
- the voting authority is responsible for conducting the election procedure, yet must not interfere with any specific voter/candidate
- all votes must be counted as soon as the voting procedure finishes.

4.1 Definition of the PMA voting key

One of the key features that constitute the underlying security mechanism of the proposed voting system is the use of Physical Multiple Administrators (PMA). The PMA authority is the set of individuals, who are responsible for (a) creating the PMA voting keys and (b) administrating an IBB. The PMA Authority consists of a representative from each candidate party in a given election. The idea behind the use of PMA authority is that *if all candidates are equally empowered through their direct involvement in the voting procedure, it will be difficult to falsify the voting process.*

The key generation formula applied is a simple concatenation of the provided keys and a system generated random number. Based on the key, a private/public key pair is generated. The PMA voting key pair is used for the encryption and decryption of the ballots during the voting process. The public part is embedded inside the mobile voting application to encrypt the ballot and the private is kept for the tallying process.

4.2 Security issues

The PMA mechanism alone, can not ensure the level of security required by a national wide election procedure. So in order to enhance the overall security, the IBB/PMA system supports a technique, called *Identical Ballot Boxes.* Most electronic voting systems reported in literature, reside their ballots in one ballot box. In the context of the proposed system, the IBB mechanism takes the vote, before it is casted, and multiplies it to the number of the IBBs. Then it casts one of the Identical Ballots to each one of the boxes. Since all IBBs contain exactly the same ballot, and there is one person per candidate responsible for each IBB (as a member of the PMA voting authority), it can be deduced that any possible altering of a vote will not fake the final tally. The integration of Physical Multiple Administrators with Identical Ballot Boxes provides the system with an advanced level of security, given that the latest ciphering algorithms are employed. In this way, the system becomes resistant to misuse and fault tolerant.

Having ensured that the ballots remain intact in the system throughout the election session, the system also has to guarantee complete anonymity for each voter. For mobile applications, the user authentication process has a significant difference compared to a web based one, because of the fundamentally different relationship between the user and the device. Ownership is the key difference. While Web applications are designed to be used from an available computer, J2ME applications run on that devices belong to people. Most MIDP devices today are cellular phones acting as constant companions of their owners. Given this relationship, we have to provide the means to ensure the anonymity of the voter. In that direction, the IBB/PMA Electronic Voting System incorporates a subsystem, called *trusted server*, which acts as a proxy between the server responsible for the authentication and the voting application.

4.3 Automating the voting process

As far as the actual voting process is concerned, the system is provided with:

- a list that contains the identification information of the legit voters,
- a balloting configuration that contains party and candidates information and
- the PMA voting key pair.

- temporal information concerning the voting process

Based on the above information, the system is initialized and legit voters can cast their vote of preference.

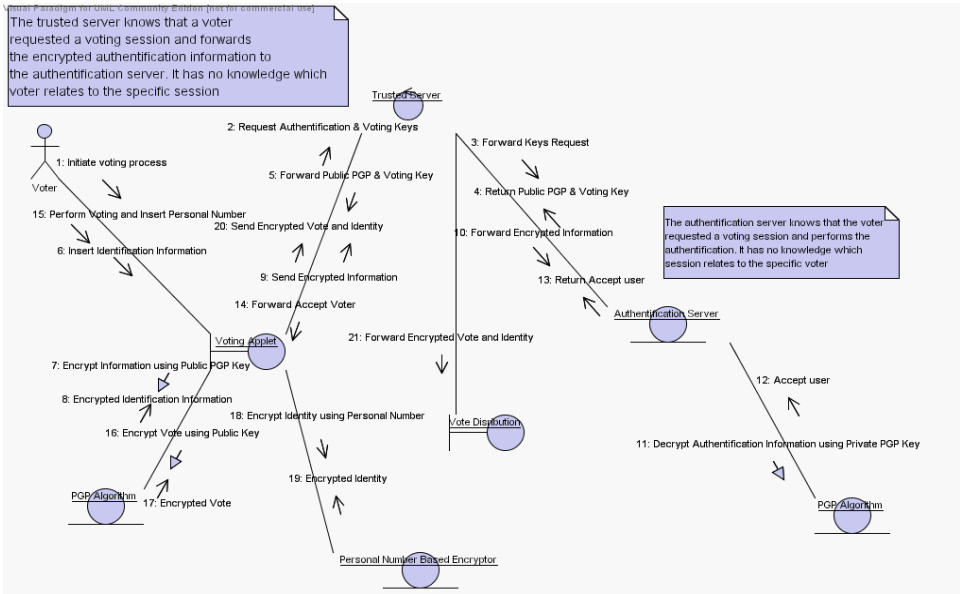

Figure 3: Processes in the IBB/PMA Voting System

As illustrated in Figure 3, at the beginning of every voting session the user contacts the trusted server, requesting a connection. User credentials are locally encrypted with the public key of the authentication server and are forwarded to the trusted server which sends the authentication request to the authentication server. The authentication server decrypts the identification information received with its private key and searches the legit voters list for an entry that corresponds to the voter. Once found, it returns an XML message to the trusted server that wraps providing information (a) if the user is legitimate, and (b) on the balloting configuration. If the user is legitimate, the trusted server returns the balloting configuration to the user. The user then selects his/her voting preferences and enters a five digit code. The latter, is used by the application as the key in the encryption of user credentials. After the user credentials have been ciphered, they are combined with the PMA voting key encrypted .The next step is to send the combined ciphered messsage to the trusted server, which forwards it to the vote distributor for replication to the Identical Ballot Boxes. As soon as the vote has been successfully entered into the IBBs, the user is informed for the successful completion of the voting session and receives a voting receipt. The trusted server informs the authentication server that the transaction was complete and characterizes the user as *Ex-Legit Voter*. This serves as a measure of

assuring that none will be allowed to vote more that one time in a given election procedure. The advantage of the proposed schema is that the trusted server is not aware of the user's identity for a particular connection, while the authentication server can not directly correlate a particular session with a certain user, as there is no direct connection to the client application.

The voting procedure continues for the duration of the pre-defined amount of time. Once the time limit is reached the authentication server stops accepting calls for remote connection from the trusted server. On the completion of the voting phase and before the beginning of the tallying, all the IBBs are checked and cross-referenced. After the examination of the IBBs, the final Tally_IBB is created.

4.4 Vote Tallying and Verification

For tallying, using the private PMA voting key, the votes take their actual (countable) form, they are counted and the voting results are updated. The authentication server randomly selects, from the legit voter list that have participated in the voting procedure, a number of voters. These voters are notified by the PMA voting authority for the verification procedure. The verification phase deals with the necessity that all citizens should be able to cross-reference the legitimacy of their votes and the fact that these votes have actually been counted. The verification is based on a process, where the PMA voting authority sends the user the user credentials that correspond to the vote number provided by the user. If the user knows his/her secret key, (s)he can decrypt his identity provided with the five digit code. Based on the deciphered credentials, the user receives the corresponding vote information and (s)he can confirm if this was his original vote or not.

5. Voting Administration

While the voting authority is responsible for the administration of the IBB/PMA voting system, the authentication server is not accessible after the voting process officially begins and its front-end only serves for monitoring the voting procedure. During voting a detailed log file of all transactions that have taken place is recorded. Figure 4 illustrates a snapshot of applying the IBB/PMA system in practice. The information presented refers to the availability of the system, the duration of the voting procedure and the state of the Identical Ballot Boxes. Moreover, the condition of the legit voters list is reported, while the system is also equipped with the ability to identify errors that may occur during the voting procedure e.g. possible failure to establish a link to the trusted server. The monitoring of the IBBs, is accomplished by sending and receiving encrypted messages to the machines that the IBBs reside on.

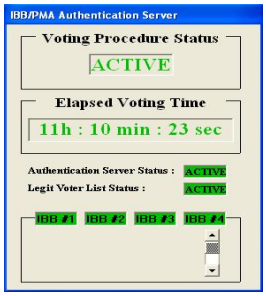

Figure 4 The IBB/PMA Authentication Server Application

After the conclusion of the voting process, the authentication server stops accepting incoming session requests from the trusted server, which directly results in the termination of the voting procedures. It sends a voting termination signal to the IBBs, through the trusted server, forcing them to stop accepting voting data. The trusted server enforces the Tallier to tally the votes. The latter, connects to the Distribution Server and a parser goes through the entries of all the IBBs, one at a time, comparing the ciphered data. Each entry that has been found identical in all the IBBs advances to the final IBB, which will be used for the final tallying of the votes. In the case of a mismatch, the entry found is compared with the rest of the Identical Votes in the remaining IBBs, it is cross-referenced and restored, in accordance to the other.

After the creation of the final IBB, using the PMA private Voting Key, the votes in the final IBB are decrypted and the results database is created. Based on this database, analytical voting results are presented to the election officials. To ensure verification of results, the described verification phase commences, and if no problem is encountered the results are reported to the public.

6. Voting from the user perspective

The mobile voting application (illustrated in Figure 5) is initially responsible to communicate with the authentication server, through the trusted server, to request to participate in a voting session. The voting application prompts the user to enter his/her identification information, which are sent to the authentication server. Given the insecure nature of the underlying communication infrastructure, the voting application encrypts the identification information of the voter with the public key of the authentication server and utilizes a secure socket layer connection to send the data to the trusted server. The trusted server just forwards this information to the authentication server. After the voter is characterized a legit voter, the user is given the right to proceed with the voting procedure. The voter is presented with a simple and understandable voting step-by-step wizard like interface. At the beginning, the user selects the corresponding party or a white vote. Based on the selected party, the user is presented with the party's candidates, where (s)he can select more that one

based on the constraints imposed by the voting authority. Once the user have selected his/her favorite candidates, the user is presented with his/her choice and is prompted to enter a five digit code, that is used to encrypt his/her ID Card Number. The encryption algorithm then encrypts the selection of the voter with the PMA public key and the ID Card Number with the personal five digit code. Figure 5 illustrates the step-by-step prototype of the mobile voter application.

Figure 5: The Voting Applet Interface

When the voter has casted the vote and the vote has been replicated and inserted in the Identical Ballot Boxes, a voting receipt is presented (see Figure 5). The voting receipt contains the vote number and the personal five digit code required by the verification process. The voting receipt does not disclose any kind of vote – sensitive information, which can be used to reveal the voter's choice.

The IBB/PMA mobile voting application considers the levels of difficulty in introducing e-Voting to a wide range technology unaware audience and so it aims to present e-Society with a simple interface that supports minimal data entry in order to achieve unsupervised voting (Xenakis and Macintosh, 2004), with high levels of fault tolerance and easy to use.

7. Conclusions and future work

In the previous sections we presented an electronic voting system that supports mobile devices, called *IBB/PMA Voting System*, which has been designed and implemented to perform election procedures both at a local and state level. The proposed voting system complies with the main characteristics of a secure electronic voting scheme, and introduces an e-voting process that relies on Physical Multiple Administration with Identical Ballot Boxes technique, which constitutes the key features of the IBB/PMA System.

Future research objectives related to the proposed system include the integration of server side modules to conduct detailed statistical processing and the integration of modules to support voting for the visually impaired.

ACKNOWLEDGMENTS

We would like to thank the Technological Educational Institution of Messolonghi for the donation of the equipment required for the development of the IBB/PMA Voting System. In the near future, IBB/PMA Voting System is planned to be used during the student's elections that will take place at Technological Educational Institution of Messolonghi.

References

Alefragis P.S., S.K. Lounis, V.D. Triantafillou and N .S. Voros (2005), *Electronic Democracy in Practice: A Web Based Voting System Relying on Identical Ballot Boxes with Physical Multiple Administration*, IADIS International Conference e-Society 2005, 27 - 30 June 2005, Qawra, Malta, pp 155-162, ISBN 972-8939-03-5, IADIS

Alefragis P.S., S.K. Lounis, V.D. Triantafillou, N.S. Voros (2004). *An Electronic Voting Scheme With Physical Multiple Administrators and Identical Ballot Boxes. IADIS International Conference WWW/Internet 2004*. Madrid Spain pp. 99-106

ACM Council (2004), *ACM Statement on Voting Systems*, Communications of the ACM, *v*ol. 47, no. 10, pp. 69-70

Alexandros Xenakis and Ann Macintosh (2004), *Levels of Difficulty in Introducing e-Voting, EGOV 2004*, LNCS 3183, pp. 116–121

Bouncy Castle v1.34 (2006), http://www.bouncycastle.org

Becker, T. and Slaton C. (2000). *The future of teledemoacracy. Prager*, Westport, CT

Cramer, R. Franklin, M. Schoenmakers, B. Yung (1996), *M. Multi-authority secret ballot elections with linear work*. in Advances in Cryptology-EUROCRYPT' 96, LNCS 1070, pp. 72-83, Berlin, Springer-Verlag

Dutton W.H., Elberse A. and Ohta K. (1999), *A case study of a Netizen's guide to elections*, Communications of the ACM, vol.42, no 12, p.p. 49-54

Hibernate 3.0 (2005), http://www.hibernate.org/

Schoenmakers B. (1999), *A simple publicly verifiable secret sharing scheme and its application to electronic voting*, in Advances in Cryptology-CRYPTO'99, LNCS 1666, pp.148-164, Berlin, Springer-Verlag

Sun Microsystems, Inc.(2000), *Scaling the N-Tier Architecture whitepaper*, Solaris Infrastructure Products and Architecture

Sun Microsystems, Inc. (2003), JavaServer Pages™ Specification Version 2.0

W3C (1999), HTML 4.01 Specification