AN ELECTRONIC VOTING SCHEME WITH PHYSICAL MULTIPLE ADMINISTRATORS AND IDENTICAL BALLOT BOXES

P.S. Alefragis, S.K. Lounis, V.D. Triantafillou, N.S. Voros
Department of Applied Informatics in Management and Finance
Technological Educational Institution of Messolonghi
Nea Ktiria, Messolonghi 30200, Greece

ABSTRACT

Rapid world-wide growth in Internet and Web use has stimulated many initiatives aimed at applying information and communication innovations to create what has been called a “digital” of “electronic democracy”. Over the last years, the field of secure voting schemes has attracted much attention from researchers. Since many security requirements are involved, some of them are contradictory, there exists no obvious universal solution. This paper aims to provide a secure electronic voting scheme for multi-candidate elections in national and local authorities where the set of voters is predefined. The key concept introduced is the theoretical aspect of “Physical Multiple Administration (PMA)” which in combination with the “Identical Ballot Boxes (IBB)” technique empowers the security of the system. The IBB system aims at offering guarantees in terms of legitimacy, security anonymity and secrecy in the voting and tallying processes. The voting scheme has been developed taking into consideration the Greek legislation and the organizational details of currently applicable voting procedures.

KEYWORDS

Distributed Systems; Electronic voting schemes; Security; Privacy; Ballots;

1. INTRODUCTION

Rapid world-wide growth of Internet and the Web usage has stimulated many initiatives aimed at applying information and communication innovations to create what is called a “digital” of “electronic democracy”. Direct democracy schemes where citizens participate in the procedure of decision making will always be a main priority for social units, like local societies, whole states or even communities of nations. Proponents of electronic democracy, suggest that democratic governments and organizations can exploit the wide range of technological capabilities, provided by information and communication technologies, to facilitate closer links among citizens affecting the way of taking decisions with citizen’s interaction, permitting the public to take place in the political procedure. Elections serve as the official mechanism for people to express their views although it suffers from the low participation of citizens.

An Internet based Electronic Voting System is defined as *an election system that uses electronic ballots that allow voters to transmit their ballot to election officials over the Internet*. The provision of an electronic voting system may still be some way of, but the required components of the technology puzzle needed are now close to existence. Based on these components, developing a new voting method would be at least as secure as the current ballot system in use (Becker and Slaton, 2000), (Dutton et.al. 1999). For that reason a number of systems have been proposed and implemented.

Every e-voting system must have some attributes in order to be able to conduct a voting procedure, in a way that is widely acceptable and can be implemented. The main attributes for an “ideal” electronic voting system are presented in (Cranor and Cytron, 1998) and (Fujioka et al.,1992) and include: Accuracy, Democracy, Privacy, Verifiability, Convenience, Flexibility, Mobility and Cost Efficiency.

Accuracy: A voting system is considered accurate when (1) no one can alter a casted vote since it has been submitted to the system, (2) a valid vote can not be miscounted, deleted or removed from the final tally and (3) an invalided vote form can not be counted in the tallying procedure.

Democracy: A voting scheme is democratic when (1) the right to cast a vote in the system applies only to legit voters and (2) the system ensures that each legit voter has voted once.

Privacy: A system that supports voting procedures is considered private when (1) no one among the election authority can link a vote to the individual that cast it and (2) no one of the voters is able to prove that an individual voted in a certain way.

Verifiability: A system is verifiable since all voters independently can verify that all votes have been counted correctly during the tallying process.

Convenience: A voting system is considered convenient if (1) it is easy to use and (2) it does not require from the potential users to have explicit hardware.

Flexibility: A system is flexible when it allows a number of voting procedures.

Most of the approaches in electronic voting are oriented towards identifying the fundamental problems associated with the adequate level of security (anonymity, authentication, data security, tractability, etc.) and most of the literature concentrates on the ability of an electronic system to handle them (Cramer et.aj.,1996) (Shoenmakers 1999).

Surveying the literature, it is clear that electronic voting systems attempt to achieve at least the same level of security as ordinary elections. Voters want to be assured of anonymity; no one should be able to know both the origin and contents of a ballot. Election officials wish to prevent unauthorized persons from voting, and to prevent authorized persons from casting more than one ballot. In addition, the results of the election should be correct and verifiable by any concerned party.

(Free Referenda & Elections Electronically, 2003) is an open source system for conducting electronic votes and is designed to provide the means to implement easily and securely the task to run an election or referendum. EVote (Chelma et al., 1997) is a system that allows members of an e-mail list to conduct a poll between the members. Lately, the EVote system has applied multiple administrators for vote signing and aimed at improving security by preventing the administrator from forging votes. (True Ballot, 2004) although it does not offer on-line access, supports an electronic voting booth, vote–by–mail and vote-by-phone for use in non-governmental elections. The Italian Academic Community (Bonetti et al., 2000) voting system is a simple voting system to support voting in common matters for the Academic Community. Vivarto Voting System (Vivarto, 2004) is a system which aims to combine efficiency, democracy and expertise in governing large organizations with the help of modern information and communication technology. Sensus (Cranor and Cytron, 1997) employs a three-stage protocol in order that the vote gets tallied and presumes the use of a public key system for all voters. The system was developed in C and Perl and makes use of CGI scripts. In (Davenport et al., 1995) and Vivarto (Vivarto, 2004) secure web-based systems developed for undergraduate student elections are presented.

In the following sections we present a web-based database-oriented electronic voting system, which relies on the theoretical aspect of “Physical Multiple Administration (PMA)”, combined with a newly developed technique called the “Identical Ballot Boxes (IBB). The rest of the paper is organized as follows: in Section 2 we present the objectives of the system design goals of our system, including the problems that came up and their possible solutions. In Section 3 we illustrate the IBB system Process Architecture. Section 4 contains a system analysis and the implementation techniques of our system. Section 5 presents the system functionality. The last section presents conclusion and future work.

2. SYSTEM ANALYSIS

The system specifications where derived from an extensive process of discussions with the responsible people of different kinds of local authorities in Greece which represent the voting process followed in general or local elections. The IBB System is designed to emulate the classical pen and paper voting approach in a digital form. In elections, there is a certain pre-defined number of people that have the right (in some countries the obligation) to vote. Following this behavioral pattern, the IBB system can be accessed only from users who are characterized as legit voters. As soon as the authentication has been made, the user can proceed to the voting procedure. The user has the right to vote once, within predefined time limits, from any

computer with Internet access and a WWW browser. The presentation of the system specifications and requirements is based on the Unified Software Development Process (Jacobson et.al. 1999) and (Larman, 1998). The use case model is developed demonstrating current processes or what the system does. Further analysis will lead to the system object model revealing how the processes are performed.

The IBB system is *accurate* by preventing a vote to be altered, deleted, miscounted or not counted. The mechanisms used are described in the followings sections; the system does not allow an invalid vote to be inserted. One of the main concepts introduced the use of Physical Multiple Administration (PMA). With this technique we aim to empower all the candidates to make them equally responsible for the completion of the voting procedure. Since, every candidate has a direct involvement to the voting procedure, and considering the fact that all candidates compete for the same position, we conclude that it is to their interest that all parties will not try to alter the results. The direct involvement of each candidate arises from the introduction of a representative within the PMA body. These representatives form the Voting Authority (VoAut). In the beginning of the voting process all the representatives must provide the system with a personal four digit code, which will be used for the encryption and decryption of the ballots during the process. As explained in Figure 1, the Ciphering Key will be the combination of all the codes provided by the PMA members. The PMA has control of the application. To illustrate a possible situation, we assume that we have three candidates (Candidate A, Candidate B and Candidate C). Each representative in the PMA body, which is the prime authority of the procedure, offers a part of the Ciphering Key and is combined with a system generated random number as follows [(Code A_PMA+ Code B_PMA + Code C_PMA)] + random number = Ciphering Key]. The Ciphering Key will be used for the encryption and decryption of the votes through the system's ciphering algorithm.

The creation of the ciphering/deciphering key alone does not guarantee the accuracy of the votes. For this reason we introduce IBBs which are critical for the approach introduced. IBBs are a set of Identical Ballot Boxes within the voting scheme, which main attribute is that they are simultaneously updated for each submitted vote. The IBBs are stored on different machines within the private network of the voting service. Having given their part of the ciphering key, each representative is assigned to one of these Ballot Boxes. So they are automatically set responsible for the administration and the proper conduction of the election procedure. Since every one of the candidates is directly responsible and the representatives are assigned we can conclude that there is no way that a ballot can be altered or removed, due to the candidate's contradictive interests.

IBB is *democratic* due to an identification mechanism responsible for the evaluation of the people that request a connection with the IBB system. So, when a user requests for a connection, the system searches for the corresponding entry in the legit voter list that matches the specific user. After the user is identified as a legit voter, the voting applet is sent and the individual can submit the vote. After a successful vote submission, the list is updated and the user loses his voting right, being characterized as "ex-legit", thus can not reconnect to the system for this specific voting procedure.

The IBB system uses mechanisms to ensure *privacy* for that none can link a voter with his vote and that all votes remain secret, until the end of the voting process. IBB system has adopted an approach where the actual vote is cast using a stand alone applet which is dynamically downloaded by the voter, which runs on the voters computer. This technique provides anonymity since it involves no physical presence involved in the voting procedure as in the classic pen and paper voting approach. In this way, the system preserve the right of the voter to be anonymous. Yet in this implementation we have included a completely new feature, which encourages transparency in the voting procedure. One additional feature introduced is the "Verification Obligation". As soon as the voting process ends, the IBB system will randomly pick three voters, among those who voted. Then the voters will be called from the Voting Authority to cross-reference their votes. During the voting session, the legit voter is send the voting applet and is prompted by the applet to enter a four digit code, along with his vote. This code will be used to encrypt his ID through an encryption algorithm which is included in the applet. After the ID number is encrypted, it is linked to the specific vote. Yet this feature doesn't defy privacy because, since the ID number is ciphered with the code that only the voter knows, no one will be able to identify his ID number. This feature will be further analyzed in the Voting Procedure Section of the paper.

The system is verifiable because after the end of the voting procedure, and before the beginning of the tallying process, all IBBs are compared. In case of mismatch, the monitoring software will be able to point out which of the boxes may have been tampered and after the cross-reference the tampered box will return to

its original state. Finally all the IBBs are combined to form the final Ballot Box which will be used in the tallying process.

The IBB System interface design makes the system, easy to use and fault tolerant. It is designed in a way that enables all types of users, from expert computer user to non-computer literate persons to comprehend its usage in a mater of minutes. Further more the web applications requirements in software and hardware are minimal.

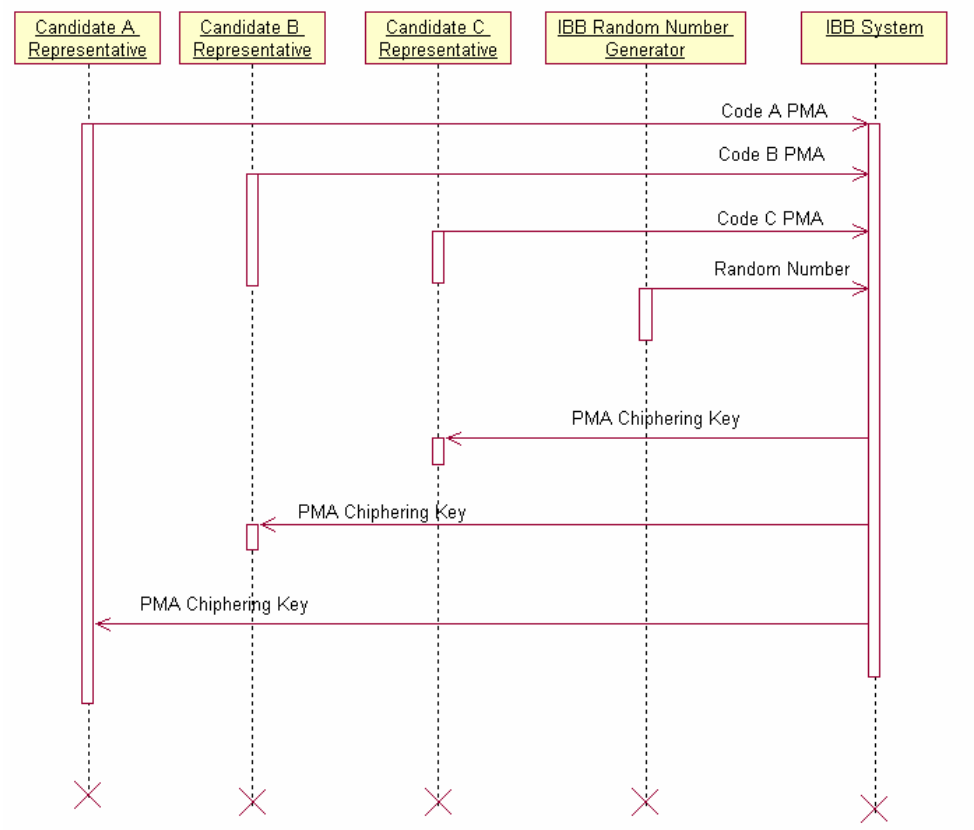

Figure 1. Creation of the PMA Ciphering Key

3. SYSTEM DESIGN

Preparation Procedure. This procedure implements the setup phase where the necessary structures, physical and technical, are initialized. This phase includes the creation of the Candidate List, the list containing information about the permissible candidates participating in the voting procedures. Following that, the PMA Authority is formed, including one representative per candidate. Finally, the Voters List is provided by the relative authorities and approved. This list holds information about the eligible voters. It voter is characterized by name, surname, ID number, parent names, address, phone, username and password. For the system to properly function, it is required to introduce one additional field which shows if the specific user has already voted or not. The system can support multiple elections with the application of a table which relates the voting procedure to the participation of the specific voter. Based on this field, each user is characterized as legit or ex-legit. This list is realized as a table in the Authorization_DB and is used for the authentication of the voter as an eligible voter. In the preparation phase, besides the Authorization_DB, we setup the IBBs. The IBBs are required to be simultaneously updated. They are responsible to hold the ballots and the ID number of the voters, both in encrypted form. In this stage, each of the IBBs is assigned to the corresponding representative. At the end of the preparation procedure, the Candidate List, the Voters List and the Identical Ballot Boxes are available and the system is ready for the voting procedure. Finally, the active

election time window, i.e. constraints for the start time and duration of the election process, are entered into the system.

Voting Procedure. The actual voting procedure begins when the members of the voting authority (PMA) enters their part of the ciphering key. The system also generates a random number to fulfill the ciphering sequence. After the ciphering key is generated, the system makes itself available. All voters can then remotely connect to the system and vote while the election process is still active. This process includes an authentication step and the actual voting process. The user through the voting interface casts his votes, while simultaneously inserting their private code to be used for the ciphering of their ID number. After they have voted, their vote is ciphered and stored to the IBBs. The system returns a successful vote response to ensure that the ballot has been enter into the Ballot Box and will be counted. Finally, the Voters List is updated, in order to make the specific user, ex-legit for the remaining of the voting duration. At the end of the election period, IBB System stops accepting connection requests, informs all interested citizens that the voting procedure is completed and that the results of the tally will be presented in a short while.

Tallying Procedure. Before the tallying begins, all the IBBs are compared and combined. If a mismatch is found, the faulty ballot box is checked with the monitoring tools which are installed on the IBBs and the error is fixed. The monitoring tool is an application that runs in the background on the machines that hold the ballot boxes. It is responsible for logging every performed activity on the specific machine during the election period. If a changed vote is found during the IBB verification process, the logs generated by the logging tools will be examined and the modification will be found and removed. After the completion of the comparison and combination of the IBBs into a final Ballot Box, the IBB System creates a new table that holds the ballots. The PMA Authority enters the ciphering key and the system decrypt the ciphered votes. A parser counts the votes for the Ballot while the candidate list is updated with the results. This list is used for the publication.

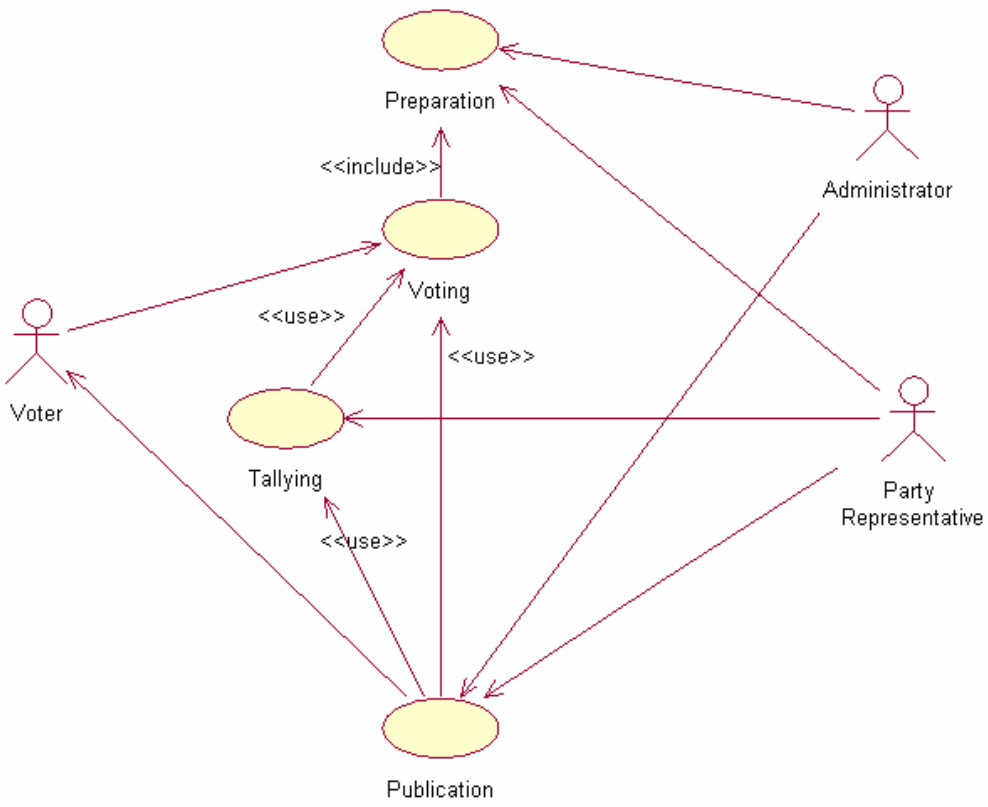

Figure 2. Use case diagram for the election procedure

Publication Process. All the results of the voting procedure are available after the end of the tallying process and are dynamically made public. A web page is generated by the system containing the voting results. Furthermore, the system provides statistics relating to the voting procedure. These statistics can be used for further study and future reference. The web pages are updated and the section "Results" is now accessible to all citizens. Before the publication of the results, the IBB system generates a small individuals list, in our use case three, with the identifiers of randomly picked persons from the voter lists which are called in. The voting authority calls them in a hearing and these persons are given the right to view and verify their ballot. The voter is allowed to enter his 4-digit code provided during voting process and the corresponding ID number. The voting list that holds ID numbers is deciphered using this number, and the one that matches his identification and the corresponding vote is shown. When the specific ID-vote pair is identified, the ciphered vote will be deciphered with the PMA voting authority key and the voter will be able to verify his vote. Yet, for privacy reasons, the voter will only be able to confirm his actual vote in a specific terminal and he won't be allowed to receive any kind of hard copy of his As a security measure, only the voter is allowed to see his vote and he can't get a copy of his vote. The voters can then verify that the process is not tampered in any way. The whole process is illustrated in Figure 2.

4. SYSTEM IMPLEMENTATION

IBB System follows the 4-tier model. The IBB system consists of a main server, responsible for the identification and authorization of the voters, a trusted server that is responsible for forwarding the voter's requests and the ciphered transaction of the vote chunks and a set of servers responsible for holding the votes called IBBs. The system follows an open platform architecture by supporting different operating systems and is designed under the international accepted standards. The web based design of the system makes it able to be used under all common and well known browsers. (iExplorer, Netscape Navigator, Mozzila, etc.), and so voters can simply access IBB System through their browser. The voting web application can be accessed through web pages and has an object oriented design and implementation. Since the system uses insecure communication channels, we want to ensure that the transmitted information won't be stolen or counterfeited. In order to achieve this security requirement between the voter and IBB System, we utilized the Secure Sockets Layer (SSL) protocol, which is universally accepted for authenticating and encrypting communication between clients and servers. For the implementation of the Web interface the HyperText Markup Language (HTML) and the Active Server Pages (ASP) are used. The applet that is used in the voting procedure in implemented using JDK 1.4.1. In order to provide the system with efficient means of data manipulation a Data Base Management System (DBMS) is required as the back-end of the system.. The DBMS has three databases .The first tracks the legit voter list contains all the necessary information about the legit voters (personal and identification information). The second tracks and replicates the Identical Ballot Boxes (IBB) which contains the ciphered votes and the ID numbers of all the voters. Lastly, there is the Result database, where statistical measures are kept for presentation along with the final results.

5. PROCESS ARCHITECTURE

The voting procedure in IBB System conforms to the characteristics of a classical voting procedure while introducing some necessary additional steps. This process is illustrated in Figure 3.

The collaboration diagram presents the voting process using an intermediate trusted server. The schema is based on the assumption that the authentication server should have no session knowledge in order to leverage the audience trust in using the server. If this was not the case the authentication server could relate a session to a voter and thus making possible to identify the voter's choice. Using an independent intermediate trusted server the authentication server only knows that a specific voter requested to vote. On the other hand, the trusted server does not know the identification information of the voter as it is encrypted using the public PGP key of the authentication server. This mechanism ensures that unencrypted vote and voter identifier information does not simultaneously exist on a single system.

Firstly, the Voter, contacts the system through his web interface with the use of the voting applet, which exists in the user PC. The voting applet on behalf of the voter contacts the trusted server and requests for

authentication and the session voting keys. The Trusted Server forwards the key requests to the Authentication Server, which returns the Public PGP Key and the Session voting Keys. After a secure connection is established, the voter inserts the Identification Information (Name, surname and Identification Codes). This information is locally encrypted with the authentication server public key and the applet forwards this set of data to the trusted server. Then the encrypted information is send to the Authentication Server which decrypts it using its private key. The system searches for that user into the legit voter list. If the person exists, it is given the right to proceed with the voting; otherwise the system returns a terminating signal.

The citizen, who has been classified legit voter, can then proceeds to the voting phase of the applet. After entering his ballot into the applet, the ballot is encrypted with the use of the PMA ciphering key. Furthermore, the ID number of the citizen is ciphered with the 4-digit key that he entered through the Personal Number Based Encryptor field of the applet. These two encrypted chunks are combined and form the vote. This vote is send to the Trusted server for forwarding. Once the Trusted Server has received the vote, it forwards the chunk (Encrypted vote and Identity) for distribution to the IBBs. In parallel, the legit voter list is updated and the citizen's right to vote is removed. The system can cope with multiple simultaneous voters requests as each request is realized in different sessions.

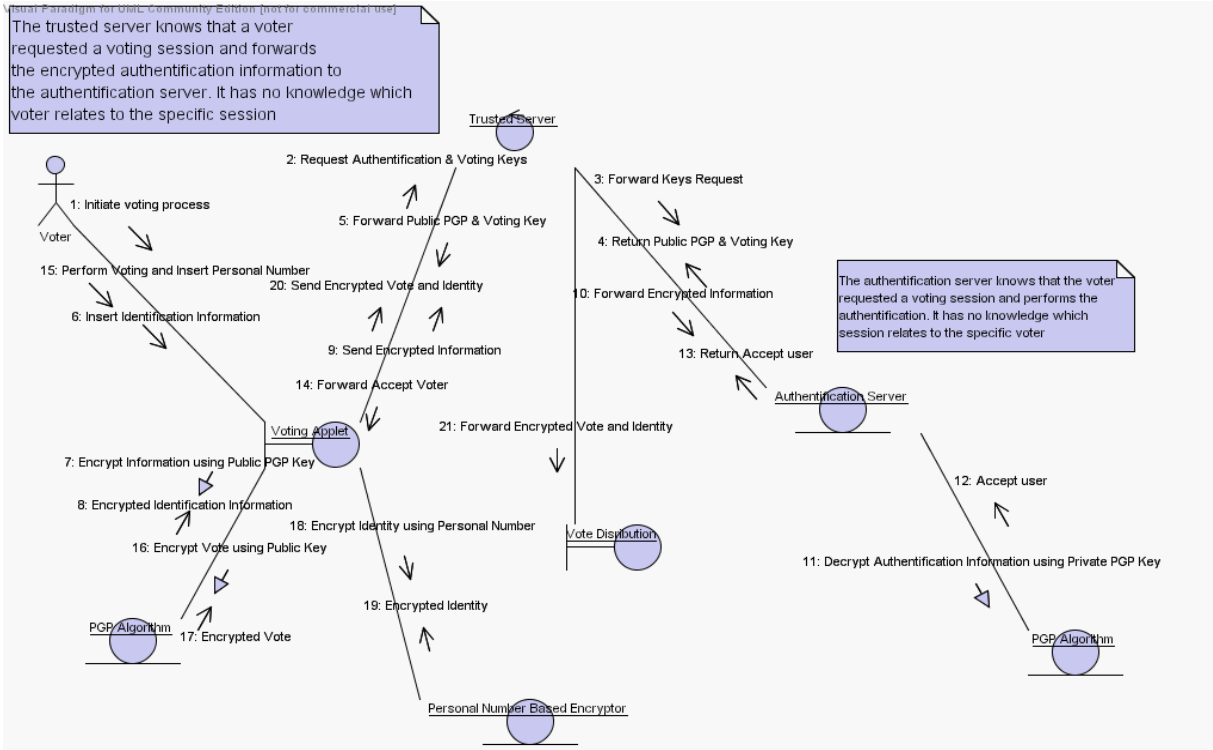

Figure 3. The IBB Process Architecture

The process that includes the transmission and replication of the ballots to the Identical Ballot Boxes (IBBs) is one of the key features of IBB System. The system expands the idea of Multiple Administrators for Electronic Voting (DuRette, 1999). After the voter has successfully voted, the vote is stored in several Ballot Boxes. For each of the IBBs, a different Administrator is responsible. Besides all security mechanisms (as monitoring software and keyloggers on the IBBs servers), these administrators, have contradictive interests and so vote forging is highly discouraged due to the IBB comparison phase during the tally.

The decryption server holds the program that parses the entries of all IBB's and compares them one to one. After the comparison is finished and the returned result is satisfactory, the IBB's are combined and the Tallying List is formed.

6. CONCLUSIONS AND FUTURE WORK

IBB System can perform election procedures at a local or state level. The work reported in this paper is preliminary and the analysis, design and functionality of the system is presented. It complies with all characteristics of a secure electronic voting scheme, provides a sound basis for future research, and introduces the notion of Physical Multiple Administration (PMA) and the Identical Ballot Boxes (IBB) techniques. These techniques are the key features of the IBB System, establishing a higher trust level to the voting individuals. The system must be enhanced with the capability to conduct detailed statistical processing. This will be realized by providing relevant interfaces to existing statistical software already available in the market or by developing a more advanced processing tool. The current system implementation partially deals with the range of security issues and safety mechanisms that should be applied, in order to secure it against possible misuse. Future work will focus on further developing a working prototype using open software technology in order to evaluate its potential. The initial implementation of the system will be applied during the forthcoming elections in the Technological Institution of Messolonghi. Another direction that we intend to expand the application range of IBB System is to support voting using wireless devices. The information explosion and the rapid growth of wireless communications have turned people into using handheld devices. For this portion of citizens, we want to implement a system that will enable them to perform their voting sessions directly from their mobile devices.

REFERENCES

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

Bonetti P., Ravaioli S. and Piergallini S. 2000. The Italian academic community's electronic voting system. Proceedings of TERENA *Networking Conference 2000 "Pioneering Tomorrow's Internet"*, Lisbon, 22-25 May 2000

Brandon William DuRette, Multiple Administrator for Electronic Voting, accessed 2002, theory.lcs.mit.edu/~cis/theses/DuRette-bachelors.pdf

Chelma, L., Davis, M., Jacq, J., MacElroy, C., 1997. Features For Freedom: A Report From eVote, Developers. *In: The First European Conference on Voting and Rating on the Internet*, Vienna, 21–22, April 1997.

Cramer, R. Franklin, M. Schoenmakers, B. Yung, 1996. M. Multi-authority secret ballot elections with linear work". *In Advances in Cryptology-EUROCRYPT' 96. Lecture Notes in Computer Science*, Vol. 1070, pp. 72-83, Berlin, . Springer-Verlag

Cranor L.F., Cytron R.K. (1997). Sensus: A security –conscious Electronic polling system for the Internet. *Proceedings of the Hawaii I International Conference on System Science*, January 7-10, Wailea, Hawaii, USA

Davenport, B., Newberger, A., Woodard, J., 1995. Creating a secure digital voting protocol for campus elections. In: Undergraduate Applied Cryptography Seminar, Princeton.

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

FREE, Free Referenda & Elections Electronically, accessed 14 April 2003, http://www.thecouch.org/free

Fujioka, A., Okamoto, T., Ohta, K., 1992. A practical secret voting scheme for large scale elections. In: Seberry, J., Zheng, Y. (Eds.), 1992. Advances in Cryptology—AUSCRYPT _92, 13–16 December, vol. 718. Lecture Notes in Computer Science, Gold Coast, Queensland, Australia. Springer-Verlag, pp. 244–251.

Jacobson, I. Booch, G. Rumbaugh, 1999, J. *The Unified Software Development Process*, Addison Wesley

Larman, G. 1998, *Applying UML and patterns.* Prentice Hall

Schoenmakers B. 1999. "A simple publicly verifiable secret sharing scheme and its application to electronic voting" *In Advances in Cryptology-CRYPTO' 99, Lecture Notes in Computer Science*, Vol. 1666, pp. 148-164, Berlin, Springer-Verlag

True Ballot, accessed 1 May, 2004. The most advanced elections systems available today. http://www.true ballot.com/.

Vivarto NetConference Plus—A New Dimension in Decision-Making & Democracy, accessed 2004, http://www.vivarto.com/o2/eng/index2.html.