ELAN, an alternative approach to e-voting systems, focused on elections data analysis

Stavros Valsamidis, Athanasios Mandilas
Kavala Institute of Technology

Sotirios Kontogiannis, Alexandros Karakos
Democritus University of Thrace

Abstract

The growth of electronic services on the web, lead to the development of premier web applications that try to offer means of electronic democracy. Such aspects are: electronic elections, electronic debates, electronic pre-election concentrations, public speeches, electronic parliament, electronic government and others. Electronic elections are nowadays one of the most popular issues of e-democracy. That led to the development of applications and several security mechanisms to address such necessity. The problem that adheres is that such applications are created either on demand for a specific election process, or experimentally for scientific purposes.
In this paper we present ELAN, an application suitable of conducting electronic elections over the web. ELAN stands for ELections ANalyzer and it is a web PHP/MYSQL application based on its own security protocol and an elections specific data analysis component. Its features and innovations such as data analysis characteristics per election process, makes it, an alternative and practical solution to already introduced e-voting applications. It is ideal for communities, universities and organizations. ELAN is an attempt to familiarize the public with the aspect of the electronic voting, to promote the idea of electronic elections and attract developers, by offering the motive of an open framework, for further development.

Keywords: E-voting, Electronic Election Systems, Electronic Voting Systems, EVS data analysis.

JEL classifications: O33

1. Introduction

Rapid technological progress in the sector of information technology and communications has lead to the implementation of the Internet applications in areas such as e-banking, e-health, e-commerce, e-government e.t.c. On the other hand, the conventional type of holding elections is performed through the use of document ballot voting systems, which are provided to the voter by a specifically election committee, responsible to keep the ballots, to identify and verify the voter, to safeguard the uniqueness of each voter' vote, as well as to count the final voting result. Therefore, it is clear that in an election process, the more the number of voters increases, the more the financial cost of the whole electoral procedure, the complexity of the voting process, the identification of the voters, the delay in counting the result and the lack of integrity of the electoral results increase.

This project relates to the development of an EVS (Electronic Voting System), namely ELAN (ELections ANalyser). It is a secure application for the conduct of electronic elections through Internet. ELAN stands for ELections ANalyzer and it is a web PHP/MYSQL application based on its own security protocol. It also includes a data analysis component. ELAN EVS is ideal for small communities, such as universities, chambers, organisations etc. It uses as fundamental tools PHP and MySQL languages. On the one hand, it is modular and on the other hand tolerant enough to resist to anyone would attempt to violate security mechanisms. It offers a combination of new features, which renders it an alternative suggestion to existing and tested e-voting systems.
These features and the capability of data analysis of both candidates and voters justify the development of such a system. The data analysis module can distinguish important variables from the elections and help make predictions for the outcome based on selected variables. The last feature is its main advantage, compared to similar e-voting systems. None of the existing systems has integrated (embedded) a data analysis component.

The proposed e-voting system was applied and tested successfully in student elections (Theodosiou et al., 2011). The voting process was held in May 2010 and lasted 9 hours from 09:00 am to 06:00 pm. 349 students participated and voted. Data analysis was applied with the method of Linear Discriminant Analysis (LDA). The most important attributes that influence the outcome of elections were selected and a mathematical model to predict the outcome of the election, based on the selected attributes, was created.
With the ELAN we hope to generate interest in the public so that it will come closer to the electronic elections and through this system to stimulate and sensitize people so as to exercise their electoral rights easily and smoothly (government Blog, 2007; King, 2006; Norris, 2004).

The paper is organized as follows. Section 2 describes the background theory: the requirements of an e-voting system, the existing EVS (11Electronic Voting System) technologies along with their corresponding applications and the related work. Section 3 presents ELAN EVS in terms of design, structure, organization, security and implementation. Finally, section 4 deals with the remarks/conclusions emerged after the system application.

2. Background theory

In the information age, temptation to modernize the process of electing representatives is increasing. In this section the requirements of an EVS system are described in depth and EVS systems and publications are presented.

2.1 EVS Requirements

Electronic Voting Systems requirements fulfil generic functionalities and attributes of an electronic voting system (Bannet et al., 2004; Karlof et al., 2005; Rubin, 2001; Chen et al., 2004). System requirements define electronic voting system functionality and are depicted in Figure 1. As presented in Figure 1, these capabilities apply at three different phases of the voting process: Before voting process occurs, during voting process and after voting process completion for a voter x (Ghassan and Taha, 2007; Mitrou et al.,

2002). The pre-voting process requirements of an electronic voting system are the following:
Authenticity: That means that only selected voters may vote and the electronic voting system must provide proof with the use of appropriate authentication mechanisms that a selected voter is the one that casted the vote (Gritzalis, 2002).
Freedom: The electronic voting system must provide the ability to all selected voters to vote whatever candidate they wish, or none for an election process (Gritzalis, 2002).
Eligibility: Only eligible voters are permitted to vote (Cranor and Cytron, 1997; Dini, 2003; Fujioka et al., 1992; Gritzalis, 2002; Jan et al., 2001).

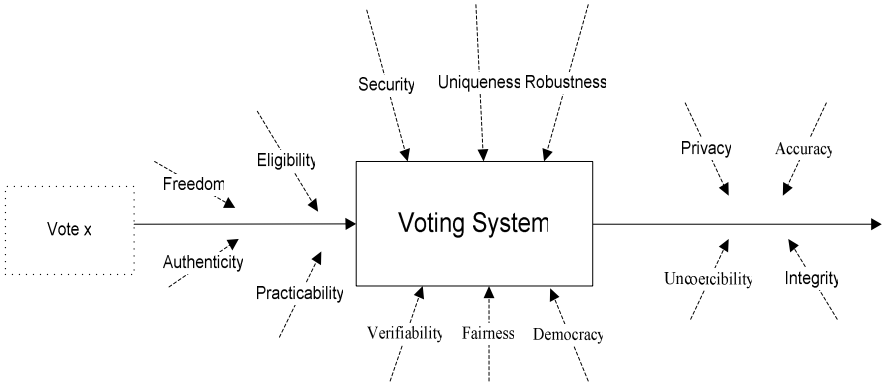

Figure 1: *Electronic voting systems requirements*

Practicability: No extra skills are required to vote and no additional equipment is required (Cranor and Cytron, 1997; Jan et al., 2001; Karro and Wang, 1999; Kofler et al., 2003).

During election processes, an electronic voting system must maintain a high standard of the following capabilities:
Robustness: The electronic voting system must provide all the necessary mechanisms to prevent interruption of the election process or system's denial of service. A malicious voter cannot frustrate or disturb the election (Fujioka et al., 1992; Chaum, 1987; Jan and Tai, 1997).
Security: During an election process the electronic voting system must maintain vote's integrity, voter's anonymity at the casted vote and encrypt the vote in order to prevent eavesdropping (Saleh et al., 2003; Saltman, 1988).
Uniqueness: The electronic voting system must provide appropriate mechanisms that ensure that voters are uniquely identified for an election process and vote only once (Cranor and Cytron, 1997; Dini, 2003; Fujioka et al., 1992; Gritzalis, 2002; Jan and Tai, 1997; Jan et al., 2001; Karro and Wang, 1999; Kofler et al., 2003; Lin et al., 2003).
Verifiability: The electronic voting system must provide the voter a proof receipt that his/her vote drop at the tally was acknowledged. This receipt may be used after the voting process by the voter to confirm that his/her vote was accounted by the election committee (Centikaya and Centikaya, 2007).
Fairness: The electronic voting system must not provide any information for the outcome of an election process during the election

process. No one can learn the voting outcome before the tally (Fujioka et al., 1992).

Democracy: All votes are equal and have the same weight. The principle: "One voter- one vote" must be sustained by the electronic voting system during an election process (Mitrou et al., 2002).

After an election process, there are also electronic voting systems requirements that must be fulfilled:

Privacy (anonymity): When the votes are verified by the election committee, the electronic voting system must provide anonymity mechanisms so that the voter could not be traced back by its vote. There is no way to derive a link between the voter's identity and the marked ballot. The voter remains anonymous (Chaum, 1987; Cranor and Cytron, 1997; Dini, 2003; Fujioka et al., 1992; Gritzalis, 2002; Jan et al., 2001; Karro and Wang, 1999; Lin et al., 2003).

Accuracy: All valid votes are counted correctly. The electronic voting system must count all votes and must count them as casted. A voter's vote cannot be altered, duplicated, or removed. Of course in a real electronic voting system appropriate error thresholds must be set that will indicate the validity of an election process (Saltman, 1988; Chaum, 1987; Cranor and Cytron, 1997; Dini, 2003; Fujioka et al., 1992; Jan and Tai, 1997; Jan et al., 2001; Karro and Wang, 1999; Lin et al., 2003).

Integrity: The electronic voting system sustain the already sustained the voting process vote integrity (Saltman, 1988).

Uncoercibility: The electronic voting system may use appropriate mechanisms to prevent a user to prove how he/she voted (Benaloh and Tuinstra, 1994; Cranor and Cytron, 1997; Gritzalis, 2002; Hirt and Sako, 2000; Okamoto, 1997).

There are also system-specific requirements that must also be taken into consideration at the design of an electronic voting system. Such requirements are the following:

Accessibility: The electronic voting system must be accessible to voters regardless their geographical location or electronic equipment they use, so as to access the electronic voting system (computers, PDAs, cable TV, mobile phones et al. (Saleh et al., 2003; Bederson et al., 2003)).

Availability: During a voting process, the electronic voting system must maintain the same availability response for all voters. Today availability problems of Internet services are less network link related and more erroneous service design and service user sustainability related (Gritzalis, 2003; Saleh et al., 2003).

Reliability: Electronic voting system reliability is identified by a set of performance metrics.

Efficiency: The computations can be performed within a reasonable amount of time (Jan et al., 2001; Karro and Wang, 1999).

Mobility: There are no restrictions on the location where voters can cast their ballots. The electronic voting system must provide methods to cache user voting sessions in case of a voter faces roaming problems or interacts with the electronic voting systems over network interfaces with latency problems (satellite links, mobile phones, wearable devices (Cranor and Cytron, 1997; Jan et al., 2001; Karro and Wang, 1999)).

Multi language support: The electronic voting system must provide multi language support for voter registration, election process and election results display (Mercuri, 2002).

Care for Special Needs: The electronic voting system must provide ways of interaction with the system by people with special needs (Bederson et al., 2003).

There are also election-specific requirements depending on the conditions of conducting the electoral process. Formal example constitutes the exclusion of a candidate from the electoral committee of the elections.

2.2 Related work

We devide EVS systems into two major categories: DRE (Direct Recording Electronic) voting systems and Internet voting systems. DRE systems utilize touch screens, keyboards, NFC and smart card equipment for voter authentication and voting purposes. Voting process takes places into voting terminals, located at specific polling areas and which are directly connected, or not, to a central station (Dill et al., 2003). The votes are immediately added to a running tally stored at the remote central station, if this station exists or if not, in the DRE's storage system (hard disk, memory card). Mail voting systems also belong to this category. DRE systems have two unique distinct characteristics: (1) DRE systems combine hardware and software to one embedded device, keeping the implementation hidden for both hardware and software and (2) utilize physical security in terms of specific voting areas (polling stations) in order to assure EVS system authentication and security requirements. Existing DRE systems are presented in the following paragraphs.

One of the first DRE EVSs used is SENSUS DRE, created by Lorrie Faith Cranor in University St. Louis, Washington in 1995 (Cranor and Cytron, 1997). It uses blind signatures to assure that voters will vote only once. Its initial purpose was to replace voting by mail. Today it is considered quite old and it is abandoned. The company TrueBallot, Inc has presented the DRE system (Trueballot, 2003), which is used by companies, organisms, universities, associations and by teams of users for the conduct of electronic elections. The Trueballot system offers 3 basic operations: ScanVOTE / TouchVOTE Ballot-On-Demand which imitates physical voting, WebVOTE which uses Internet and TeleVOTE which uses phone as means for the conduct of voting. Another system named E-Vox (Trueballot, 2003) that combined the flexibility of a Vote by Mail (VBM) system was tested in MIT campus-wide student elections.
The DRE Diebold AccuVote-TS system (Diebold, 2004), used in US elections, combines into an embedded device both hardware and software so that a user by using a touch screen with a card reader may authenticate and vote, after being authenticated by polling officials (votes are casted at specific poll sites) (Bederson et al., 2003). The SureVote company (SureVote, 2005), provides a similar system, in which the users authenticate themselves and their right to vote using a numeric personal identification code and a numeric ballot code (Bederson et al., 2003). It also offers and a web-based Internet EVS system.

Internet EVS systems on the other hand, use computer or digital television or mobile phone (by any hardware means) with custom software provided by a central voting station or stations over the Internet (using Internet software technologies), for voting purposes. Elections are held everywhere using remote Internet voting thus increasing EVS system's availability usability and scalability. This, of course, may be contentious because it is difficult to verify that the voter is who they claim to be. Both anonymity and privacy may easily be compromised. This opens the door to voter coercion and vote buying. Such drawbacks lead to the implementation of more strict security mechanisms on Internet EVSs. Such systems are presented in the next paragraph.

Safevote is a software company offers a variety of products supporting both public and private elections using Internet voting (SAFEVOTE, 2006). The Rijnland Internet Election System (RIES) is a system designed for voting in public elections over the Internet (Gonggrijp et al., 2009). Moreover, browser based Agile E-Voting system is another effort to provide a practical, voter-friendly e-voting system (Simhalu and Takeda, 2007). The Global Election Company provides election.com (Company, 2003), which is global election software. It offers poll site voting and remote electronic voting. Finally, GNU FREE (Free Referenda and Elections Electronically (GNU, 1999)) is an Internet based system which started developing in 1999 as a free electronic voting EVS system. Its implementation is database and platform independent. Today this project has been abandoned.

Various publications have addressed the benefits and risks of e-voting systems (Mohen and Glidden, 2001, Phillips and von Spakovsky, 2001, Alvarez and Hall, 2004). Electronic forms of voting have been implemented at some scale in many different countries, though in very different ways (Pratchett and Wingfield, 2004, Rezende, 2004). The first electronic election scheme was proposed by (Chaum, 1981). Chaum, the inventor of eCash, describes a unique method where voters can positively confirm their ballots, both at the polling station and also after the election, to be sure they are correctly entered into the tallies, without revealing their choices. This groundbreaking work may eventually form the basis of secure and auditable future elections (Chaum et al., 2005). Mercuri has been investigating a wide range of electronic voting issues and addresses usability issues (Mercuri, 2002).

Remarkable is a paper which surveys issues relating to usability of electronic voting systems and reports on a series of studies (Bederson et al., 2003). It was an early indication of machine failures with the Diebold equipment. Another interesting paper, which details the requirements, design and implementation of a special type of electronic voting systems, the remote on-line voting system, suitable for university setting where students can cast their votes anytime, anywhere and using fixed and mobile electronic devices including personal computers, personal digital assistants and smart and regular phones, is proposed by (Qadah and Taha, 2007). The usability issues in various election systems, with the conclusion that newer technologies are not necessarily an improvement for voters is proposed by (Susan King Roth, 1998). The use of distance electronic voting systems, in the support of not political elections, has been searched in many works (Draper and Brownw, 2004; Stuart, 2004). Analysis of an Electronic Voting System was proposed (Kohno et al., 2004). Overview of voting security threats and vulnerabilities along with an assessment of strengths and weaknesses of potential solutions is presented by Fischer (2003).

The application of ELAN and the evaluation of its use by 349 users and its data analysis, as well, is described by (Theodosiou et al., 2011).

3. ELAN Architecture

ELAN EVS was implemented with the use of open source tools PHP and MySQL. The specific platform was chosen due to ease of use, popularity, security when administered correctly, and expandability.

ELAN high lever architectural design, major modules and components are presented in Figure 2.

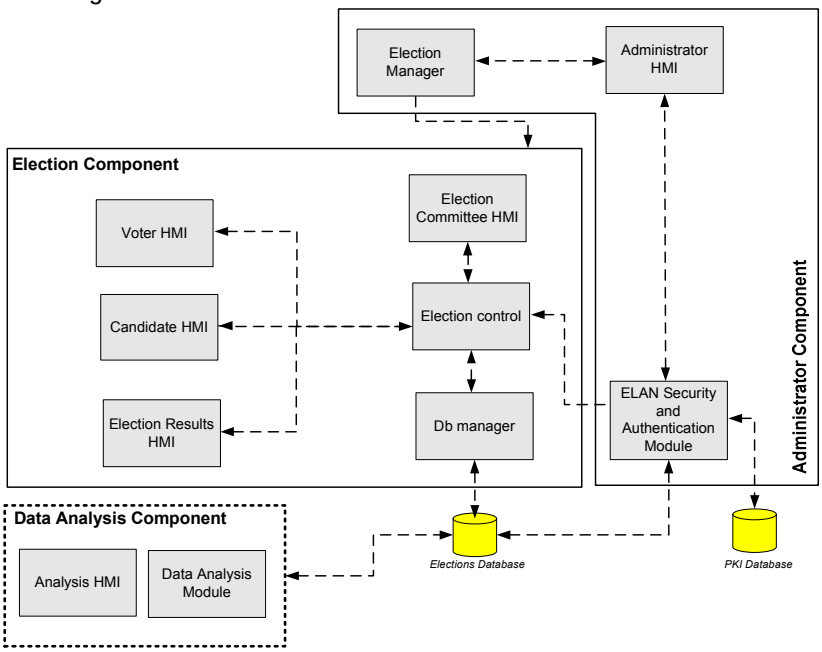

Figure 2: ELAN architectural design - major components, modules and HMIs

The ELAN application is divided into three major components as depicted in Figure 2: The election, data analysis and administration components. Election component includes modules and HMIs used for an election process. Data analysis component is an independent component controlled by the ELAN administrator that performs data analysis on voters preferences per election process, preserving voters anonymity. It also keeps statistical records such as voter's voting time, voter's uncertainty (going back and forth an election process without voting), voter's age and gender and voters social popularity (the number of elections a voter participates). Finally, the administration component administers voter authentication, security and privacy per election process and supervises all registered election objects by the election component.

The following entities are supported by ELAN application: Administrator, voters, candidates and election committees. For every election process, an election authority is responsible for its supervision via the Election control and the election results are announced via the Election results HMI as depicted in Figure 2; ELAN application administrator is responsible for setting up, running, and supervising all the election processes via the administrator component (administrator HMI and elections manager-Figure 2). In depth, administrator authority is responsible for the management of voters, candidates, assignment of election committees per election process, management of election processes and registration of RSA keys per election process via the security and authentication module PKI infrastructure (Figure 2).

Voter eligibility per election process is performed by the election committee assigned by the administrator authority. These committees through the Election control, and Election committee HMI (Figure 2), approve the voters by performing identity checks and send message digests to the voters generated by the security and authentication

module. ELAN security module and data analysis component are described in detail in the following section.

3.1 ELAN Security and Administration module

The heart of a voting system apart from voting rules of election, election protocol, is its security protocol/schema that has to adequately fulfil several requirements, shown at section 2.1. Despite of the extensive work and the number of electronic voting security mechanisms that have been proposed, no complete solution manages to extend as a bullet proof practical implementation for all election protocols or cover in extend election process requirements. In this section we present the major voting security protocols used for electronic elections and our proposed security protocol used by ELAN application.

The first voting security protocol was proposed by Chaum (Chaum, 1981, Chaum, 1987, Lin et al., 2003) called mix-net permutation and decryption. This protocol uses N authorities that are in fact mix-servers $M_1,M_2,\ldots,M_N$ with their public RSA keys $E_1,E_2,\ldots,E_N$. The voter V_i sends a message m through anonymous channel as: $E_1(E_2(\ldots.E_n(m)\ldots.))$ to M_1. M_1 waits for the arrival of T encrypted messages and then removes its level of encryption, shuffles them and sends them to M_2 and so forth. Finally, the last server decrypts the messages and calculates the result. Mix net security protocols have many drawbacks. At first, a mix net environment is difficult to implement since a proof of correct decryption should be presented at each mix net step by the decrypting mix server and secondly, failure on decryption of a single voter will disrupt the whole election process. Imagine the case that some votes have been published and due to a decryption error caused by a mix server the voting process must be restarted. The up until now voting outcome will definitely affect the voting process to come.

Another form of security algorithms, with less implementation complexity, uses one or at least two mix net servers and verifies voters with the use of blind signatures. This joint schema is called: anonymous channels with blind signatures. Such security protocols are described at: (Fujioka et al., 1992, Radwin, 1995, Juang et al., 1998). On the FOO scheme (Fujioka et al., 1992), an administrator and a collector manage the elections. The collector collects the votes and publishes the election results, while the votes are blindly signed by the administrator and are sent back to the voter in the form of tokens. Then the voter sends his/her token, encrypted vote and decryption key anonymously to the collector. The collector publishes the accounted tokens along with the vote results (decrypts the encrypted votes). Also the administrator announces the number of voters whose votes have been blindly signed.

The Radwin protocol (Radwin, 1995) uses one reliable authority that acts both as administrator and as collector. Unlike FOO scheme the token does not contain the actual vote but instead a voter pseudonym and a random binary vector issued by the administrator authority is used for vote verification and a vector key handshake between voter and administrative authority is performed. Voters' pseudonym is given to the voter by the administration authority upon registration phase. With this mechanism the possibility for a voter to vote twice is prevented.

The JL-protocol utilizes one manager and N scrutineers (Juang et al., 1998). The role of scrutineers is to share the threshold ElGamal key used for vote encryption and an RSA key that is used for issuing blind signatures by the manager. In this schema the encrypted vote is a part of a token that contains random bits, one way function for the voter id and an election id tag (RD) that prevents the voter to re-use voting tickets from previous elections.

Voting protocols that use homomorphic encryption followed anonymous channel encryption protocols. These schemes utilize more security properties and present further communication complexity. In addition election systems that use such protocols may support only yes-no and 1-out of-L voting cases. Homomorphic voting protocols are Benaloh's (Benaloh, 1987; Benaloh, 2006), Shoomaker's (Schoenmakers, 1997) and CGS (Crammer et al., 1999), for yes-no voting election and HS scheme for 1-out of-L voting election (Hirt and Sako, 2000). All these homomorphic encryption protocols are presented as draft cryptographic cases and no feasible implementation of these protocols is a part of existing election software and/or systems, due to their limited functionality (yes/no elections, 1-L elections).

ELAN security protocol module uses an algorithm similar to the FOO protocol (Fujioka et al., 1992) that uses one authority that acts as administrator and another as vote collector (election committee). The voter is given a username and password by the administrator with which may login to the system as a simple user. Then the registration for an election process follows. During voter registration process, 3 cryptographic keys are created, which are: passkey, public key, and private key. The passkey is sent to the voters e-mail account, and the public key is sent to the PKI system (a Public Key Infrastructure that holds voter RSA keys per election process).

The voter logs in to the system, using the username and password, as a simple user and then the voter enters the elections using his/her passkey. The voter applies for participation to the specific election process and the election committee is notified, checks voter's record and gives the voter access to the relevant election process, while a message digest is sent to the voter by the election committee, using as fields voter id, voting time and voter personal information. This message digest is used by the voter so as to create a digital signature, using voter public key and the message digest received from the election committee.

Vote Casting and Verification is performed as follows: The voter fills in the ballot, signs it with the digital signature, and sends it to the election committee, while the voter applies a crypt key. Then the ballot is encrypted using voter's secret key from the PKI and temporarily saved on the ELAN system. Once the ballot is successfully validated and counted a blindly signed by the administrator ticket vote is sent back to the voter. The voter can use this ticket vote in order to make sure that the ballot was successfully counted. At the end of the voting process, all voting tickets of votes have been successfully accounted for by the election committee and blindly signed by the administrator, are announced at the election bulletin board. If a voter does not find the corresponding ticketvote on this board, may fill in an application and send it to the election committee in order to reexamine the ballot.

3.2 ELAN Data Analysis component

Statistical data processing and data mining of electronic voting data is done in ELAN. Data analysis concerns both candidates and voters. System encrypts and stores user data so as to eliminate the possibility of the inverse procedure, retrieval and decryption. It is emphasized that data analysis does not come contrary to the objective of the system that is the maintenance of anonymity, checked only from abusive and/or malicious use.

The statistical jobs include calculation of indexes per category as gender, age, time, duration, means of voting etc. The mining of knowledge extracted from the data that originate from anonymous system users, in our case, students. This data, because of their big volume and their authentic characteristics, provide the possibility of applying methodologies and techniques of data mining.

Data mining allows the extraction of useful conclusions but also the detection of interesting tendencies of the users and the correlation of tendencies with parameters as gender, age, time, duration, and means of voting.

4. Remarks/Conclusions

This paper presents an alternative Internet electronic voting system (EVS), called ELAN. In this EVS system, a new security protocol has been implemented in order to maintain secure electronic elections over Internet. It also includes a data analysis component which is capable of analyzing an election process.

ELAN system involves a combination of new features with basic advantages, the implementation in open software, its modular organization covering functional requirements and the capability of data analysis of candidates and voters.

It was applied and tested successfully in student elections. None user complained about its functionality and ease of use. The data analysis which was applied with the method of Linear Discriminant Analysis (LDA), predicted the outcome of the election after the selection of the most important attributes and the creation of a mathematical model.

As future work, we intend to extend the ELAN EVS, so that other equipments such as personal digital assistance (PDAs), mobile phones, and cable TV to be applicable. Special concern will be taken for disabled people.

References

Alvarez, R. M. and T. E., Hall, 2004, Point, Click and Vote: The Future of Internet Voting. Brookings Institution Press.

Bannet, J., D., Price, A., Rudys, J., Singer, and D., Wallach, 2004, Hack-a-vote: Security issues with electronic voting systems. In proc of the IEEE Symposium on Security and Privacy, volume 2, pages 32–37.

Bederson, B. B., B., Lee, and R. M., Sherman, 2003, Electronic voting system usability issues. In Human Factors in Computing Systems: Proceedings of CHI, pages 145–152.

Benaloh, J., 1987, Verifiable Secret Ballot Elections.

Benaloh, J., 2006, Simple Verifiable Elections. Technical report, Microsoft research.

Benaloh, J. C. and D., Tuinstra, 1994, Receipt-free secret-ballot elections (extended abstract). In STOC, pages 544–553.

Centikaya, O. and D., Centikaya, 2007, Verification and validation issues in electronic voting. The Electronic Journal of e-Government, 5(2):117–126.

Chaum, D., 1981, Untraceable electronic mail, return address, and digital pseudonym. Communications of the ACM, 24(2):84–88.

Chaum, D., 1987, Elections with unconditionally-secret ballots and disruption equivalent to breaking RSA. In proc of Computer Science on Advances in Cryptology-EUROCRYPT, pages 177–182.

Chaum, D., P. Y. A., Ryan, and S. A., Schneider, 2005, A practical voter-verifiable election scheme. In ESORICS, pages 118–139.

Chen, Y.-Y., J., Jan, and C.-L., Chen, 2004, The design of a secure anonymous internet voting system. Computers & Security, 23(4):330–337.

Company, 2003, Global Election Company, Election.com. http://www.election.com/.

Crammer, R., R., Gennaro, and B., Schoenmakers, 1999, A secure and optimally efficient multi-authority election scheme. In proc of Advances in Cryptology CRYPTO, pages 148–164.

Cranor, L. F. and R. K., Cytron, 1997, Sensus: A security-conscious electronic polling system for the internet. Hawaii International Conference on System Sciences, 3:561.

Diebold (2004), Diebold electronic voting machine information sheet. http://w2.eff.org/Activism/E-voting/20040818_diebold_accuvote-tsv0.8. pdf.

Dill, D., R., Mercuri, P., Neumann, and D., Wallach, 2003, Frequently asked questions about dre voting system. http://www.verifiedvoting. org/drefaq.asp.

Dini, G., 2003, A secure and available electronic voting service for a large-scale distributed system. Future Generation Comp. Syst., 19(1):69–85.

Draper, S. W. and M. I., Brownw, 2004, Increasing interactivity in lectures using an electronic voting system. Journal of Computer Assisted Learning, 20:81–94.

Fujioka, A., T., Okamoto, and K., Ohta, 1992, A Practical Secret Voting Scheme for Large Scale Elections. In Workshop on the Theory and Application of Cryptographic Techniques: Advances in Cryptology, volume 718, pages 244–251. Springer-Verlag.

Fischer, 2003, Election Reform and Electronic Voting Systems (DREs): Analysis of Security Issues, Congressional Research Service, The Library of Congress, November 4, 2003.

Ghassan, Z. and R., Taha, 2007, Electronic voting systems: Requirements, design, and implementation. Elsevier Computer Standards and Interfaces, 29(1):376–386.

GNU, 1999, Gnu free referenda and elections electronically. http://www.gnu.org/software/free/ (abandoned).

Gonggrijp, R., W.-J., Hengeveld, E., Hotting, S., Schmidt, and F., Weidemann, 2009, Ries - rijnland internet election system: A cursory study of published source code. In VOTE-ID ’09: Proceedings of the 2nd International Conference on E-Voting and Identity, pages 157–171, Berlin, Heidelberg. Springer-Verlag.

government Blog, 2007, H. E. Disco sarko and le pen de mort – e-democracy in the french presidential elections. http://www.headstar.com/egblive/?p=31.

Gritzalis, D., 2002, Principles and requirements for a secure e-voting system. Computers & Security, 21(6):539–556.

Gritzalis, D., 2003, Secure Electronic Voting: Part III, Trends and Perspectives, Capabilities and Limitations. Kluwer Academic Publishers.

Hirt, M. and K., Sako, 2000, Efficient receipt-free voting based on homomorphic encryption. In proc of Advances in Cryptology EUROCRYPT, pages 92–107.

Jan, J., Y.-Y., Chen, and Y., Lin, 2001, The design of protocol for e-voting on the internet. In IEEE International Carnahan Conference on Security Technology, pages 180–190.

Jan, J. and C.-C., Tai, 1997, A secure electronic voting protocol with ic cards. Journal of Systems and Software, 39(2):93–101.

Juang, W.-S., C.-L., Lei, and P.-L., Yu, 1998, A verifiable multi-authorities secret elections allowing abstaining from voting. In proc of International Computer Symposium, pages 210–218.

Karlof, C., S., Naveen, and D., Wagner, 2005, Cryptographic Voting Protocols: A Systems perspective. Proceedings of the Fourteenth USENIX Security Symposium (USENIX Security 2005), August 2005. URL= http://www.cs.berkeley.edu/~nks/papers/cryptovoting-usenix05.pdf

Karro, J. and J., Wang, 1999, Towards a practical, secure, and very large scale online election. Computer Security Applications Conference, Annual, 0:161.

King, J., 2006, Democracy in the information age. Australian Journal of Public Administration, 65(2):16–32.

Kofler, R., R., Krimmer, A., Prosser, and E., Prosser, 2003, Electronic voting: Algorithmic and implementation issues. In in Proceedings of the 36th Hawaii International Conference on System Sciences.

Kohno, T., A., Stubblefield, A., Rubin, and D., Wallach, 2004, Analysis of an electronic voting system. pages 27–40.

Lin, I.-C., M.-S., Hwang, and C.-C., Chang, 2003, Security enhancement for anonymous secure e-voting over a network. Computer Standards & Interfaces, 25(2):131–139.

Mercuri, R., 2002, Humanizing voting interfaces. http://www.notablesoftware.com/Papers/UPAPaper.html. Paper presented at the Usability Professionals Association Conference, Orlando, Florida.

Mitrou, L., D., Gritzalis, and S. K., Katsikas, 2002, Revisiting legal and regulatory requirements for secure e-voting. In SEC ’02: Proceedings of the IFIP TC11 17th International Conference on Information Security, pages 469–480, Deventer, The Netherlands, The Netherlands. Kluwer, B.V.

Mohen, J. and J., Glidden, 2001, The case for internet voting. Communications of the ACM, 44(1):72–85.

Norris, P., 2004, Deepening democracy via e-governance. Technical report, Harvard University.

Okamoto, T., 1997, Receipt-free electronic voting schemes for large scale elections. In Fifth Workshop on Security Protocols, volume 1, pages 25–35. LNCS.

Phillips, D. M. and H. A., von Spakovsky, 2001, Gauging the risks of internet elections. Communications of the ACM, 44(1):73–88.

Pratchett, L. and M., Wingfield, 2004, Electronic voting in the united kingdom: lessons and limitations from the uk experience. Electronic Voting and Democracy, Palgrave Macmillan, New York, NY, pp. 172-189.

Qadah, G. Z. and R., Taha, 2007, Electronic voting systems: Requirements, design, and implementation. Computer Standards & Interfaces, 29(3):376–386.

Radwin, M., 1995, An untraceable, universally verifiable voting scheme. Technical report, Dept. of C.S. Indian Institute of Technology.

Rezende, P., 2004, Electronic voting systems: is brazil ahead of its time? RSA CryptoBytes, 7(2).

Rubin, A., 2001, Security considerations for remote electronic voting over the Internet. The Magazine of USENIX and SAGE, 1(26):20–28.

SAFEVOTE, 2006, Safevote secure login ballot evs. http://safevote.com/public_elections.htm.

Saleh, K., C., El-Morr, A., Mourtada, and Y., Morad, 2003, Specifications for a mobile-agent platform and an internet-based mobile electronic voting application. In International Conference on Internet Computing, pages 730–736.

Saltman, R., 1988, Accuracy, integrity, and security in computerized vote-tallying. U.S. Department of Commerce, National Bureau of Standards.

Schoenmakers, B., 1997, A simple publicly verifiable secret sharing scheme and its application to electronic voting. In proc of Advances in Cryptology EUROCRYPT, pages 112–124.

Simhalu, S. K. and K., Takeda, 2007, Browser based agile e-voting system. In ASIAN, volume 4846 of Lecture Notes in Computer Science, pages 62–69. Springer.

SureVote, 2005, Surevote company evs system. http://www.surevote.com/.

Theodosiou, T., S., Valsamidis, G., Florou and A., Karakos, 2011, 24th Pan-Hellenic Statistic Conference, 27 April – 1 May 2011 (in Greek).

Trueballot, 2003, Trueballot company: Evox voting system. http:// theory.lcs.mit.edu/ cis/voting/voting.html,http://www.trueballot.com