Design, Analysis and Implementation of a Cyber Vote System

Khaled Elleithy and Ihab Rimawi
Computer Science and Engineering Department
University of Bridgeport
Bridgeport, CT 06601
elleithy@bridgeport.edu

Abstract

In this paper, we present the design and implementation of the CyberVote system. The CyberVote system gives voters a reliable and highly secure environment to cast their votes using Internet terminals, such as PCs, handheld devices, and mobile phones. Furthermore, it relies upon an innovative voting protocol that uses cryptographic tools.

The cryptographic protocol ensures authentication of voters, notification, and confirming the process afterwards, in a random time, in order to eliminate any probability of identity theft. Also, it guarantees the privacy and integrity of each vote during the registration process, transformation through the Internet, and during the counting and auditing process.

Furthermore, the CyberVote system includes a tool that resets the database before the voting process starts. When the elections time ends, voters cannot cast their votes, and they are not allowed to access their accounts during counting process. The counting process is fully automated, giving no chance for manipulation of the results. When the results are ready, it will be posted on the official election website along with statistic studies and graphs that explain the results.

1. Introduction

1.1. Background

The 2000 presidential elections forced most of the organizations around the world to think of a better way of voting that enables as much people to cast their ballots in a convenient way [1]. It was suggested to introduce a system that enables voters to use the internet to cast their ballots, since the internet is a cheap, fast, and effective way to transfer data. Many researchers have studied the benefits and threats of using internet for voting [2]. Most studies raised concerns about voters' authentication, security of ballots during transfer through internet, and maintaining the secret ballot, which means to separate the identity of the voter from the ballot [3].

Online voting is not a new concept. In the last three decades, studies tried to come up with a way to create online voting systems that enable peoples to vote while they are at their homes. It was not until the late 90's when the idea became practically possible. Internet revolution helped the idea to grow. Studies expect that online voting will replace the present voting systems sooner or later [4].

1.2. Advantages and problems of online voting systems

1.2.1. Advantages of Online voting systems

Online voting provides convenience, cost-saving, and saves the voters from dealing with heavy traffic, bad weather conditions, and postal service issues. Furthermore, it helps millions of disabled and blind people to cast their votes without any assistance [5].

1.2.2. Problems face applying Online voting systems

1.2.2.1. California Task Force

California formed a committee called California Internet Voting Task Force to study the feasibility of replacing the current voting system with remote online voting system. The taskforce released its report on January 2000. The report suggested that using a remote internet voting system will increase the number of voters due to the convenience it provides. It added, "However, technological threats to the security, integrity and secrecy of Internet ballots are significant" [2]. The taskforce divided remote online voting into two different types:

a- Using computers and LANs controlled by the state.

b- Using computers and LANs controlled by voters.

The task force concluded that the first type can be easily used, while the second needs more analysis and study because of the threat of Trojan horses, and back doors [2].

K. Elleithy et al. (eds.), Advances in Computer, Information, and Systems Sciences, and Engineering, 219–225.

1.2.2.2. Technical Problems

There are many technical problems that appear when applying remote online voting systems. The first issue that can be a threat is a coordinated network flood [7]. Another problem that prevents the implementation of online voting is the security on the other side of the system, the voter terminal. Even if we manage to secure the server and we have a secure ballot transmission over the internet, we can not secure the voters terminal. This is probably the toughest challenge facing the developers of those systems. Giving voters the chance to vote using internet will affect the secrecy of ballots, since other people can watch the voting process from behind the voters back [7]. Having access to computers and internet is another important issue, since access to internet varies from one class to another in the society which might not give accurate results [7].

1.2.2.3 Solving technical problems

Flooding any network can be solved by having a backup server that picks up as soon as the other server stops working. Furthermore, replacing major servers with smaller servers placed according to population of voters in different areas will help stopping any kind of coordinate network flooding [8].

Securing all the voters terminals could be an impossible mission, simply because voters run multiple applications on their terminals that might be capable of changing or manipulating the voting process. The most practical solution is to have an online scanning tool that scans the voters' computer from potential threats before the voters get to cast their votes. Another solution that can be more time efficient is transmission a tool to the voter's computer after that stops all the processes running on the machine, except for the processes the system runs. This solution will reduce the risk of having security problems on the voters' terminals, but it does not eliminate it. Having access to the internet should not have a huge impact on the voting process if we keep the old fashion way by going to polls where terminals are available, located in the areas where computer access is not available as much as other areas.

1.2.2.4 Identity Theft

Identity theft is a problem that affects any voting process no matter what kind of technology is used. Remote online voting will make identity theft task easier than before. In order to overcome this problem, the voter should be asked challenging questions that help authentication. Also, sending a physical notice to voters confirming the voting process associated with the time of voting, can reduce the risk of identity theft [8].

1.3. CyberVote

CyberVote is a remote online voting system that tries to overcome the problems of the present remote voting systems. It enables voters to cast their votes from their own Internet terminals, in a highly secured environment.

CyberVote uses different methods of encryption, which ensures the security of the data given to the system, and it ensures voters authentication. Separating the database server from the CyberVote server gives the system another security advantage. Furthermore, CyberVote follows the secret ballots criteria, which separates voter's identity from the ballot, which maintains the privacy of the voting process.

2. Design

2.1. Requirement Analysis

The CyberVote system was designed to fulfill the following functional requirements:

- Administrator specifies registration times and date(s)
- Administrator specifies voting times and date(s)
- Administrator adds candidates to CyberVote
- Administrator has access to population table in database
- Voters can register during registration period
- CyberVote System checks voters' eligibility to vote
- CyberVote stops accepting new registrations after its period is over.
- Voters can log into their accounts
- CyberVote authenticates users
- Voters cast their votes using official CyberVote website
- CyberVote encrypts received data.
- CyberVote saves the vote in a highly secured database
- CyberVote arranges confirmation process by different techniques such as Phone messages, email, SMS messages, or mail.
- CyberVote can deletes the voters who voted from the database
- CyberVote stops Voting process according to pre-specified date and time
- CyberVote counts the votes
- CyberVote posts results on official website.

Furthermore, CyberVote fulfills three non-functional requirements which are:

1. Reliability,
2. Usability,
3. Security.

2.2. System Design

2.2.1Design Diagrams

Figure 1 shows the UML diagram which explains explain how CyberVote system works.

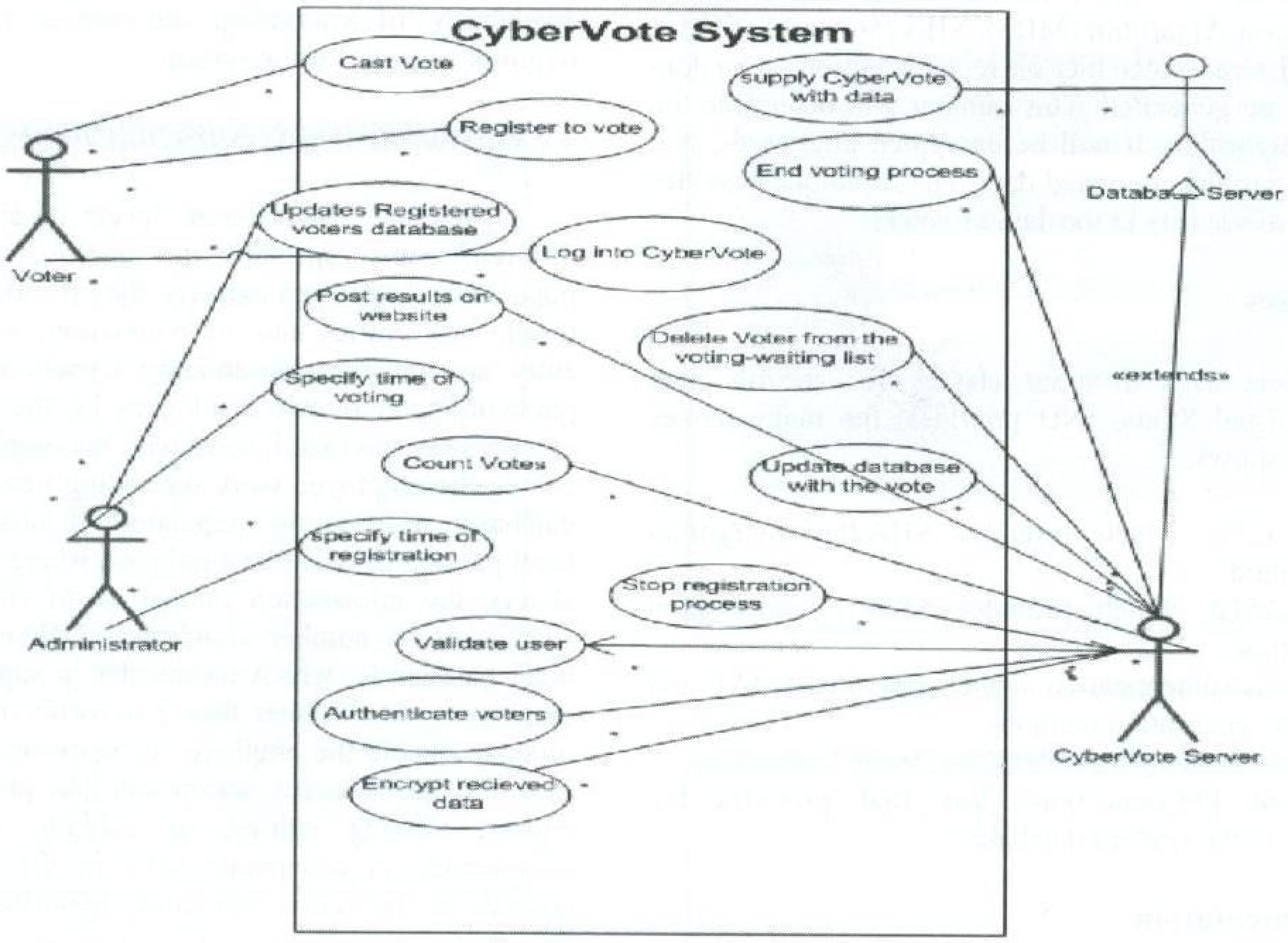


Figure 1: UML diagram of CyberVote system

2.2.2. Database Design

In order to separate the identity of voters from their ballots, a new technique is introduced in CyberVote system that deletes the data of voters from the registered Voters table as soon as they hit on vote button. Their vote will be stored in *casted* table, and their social security number will be stored in a separate table called confirm. That table will send the voters confirmations of the process, then the system will store in the population database that voter X voted in voting number Y, and so on.

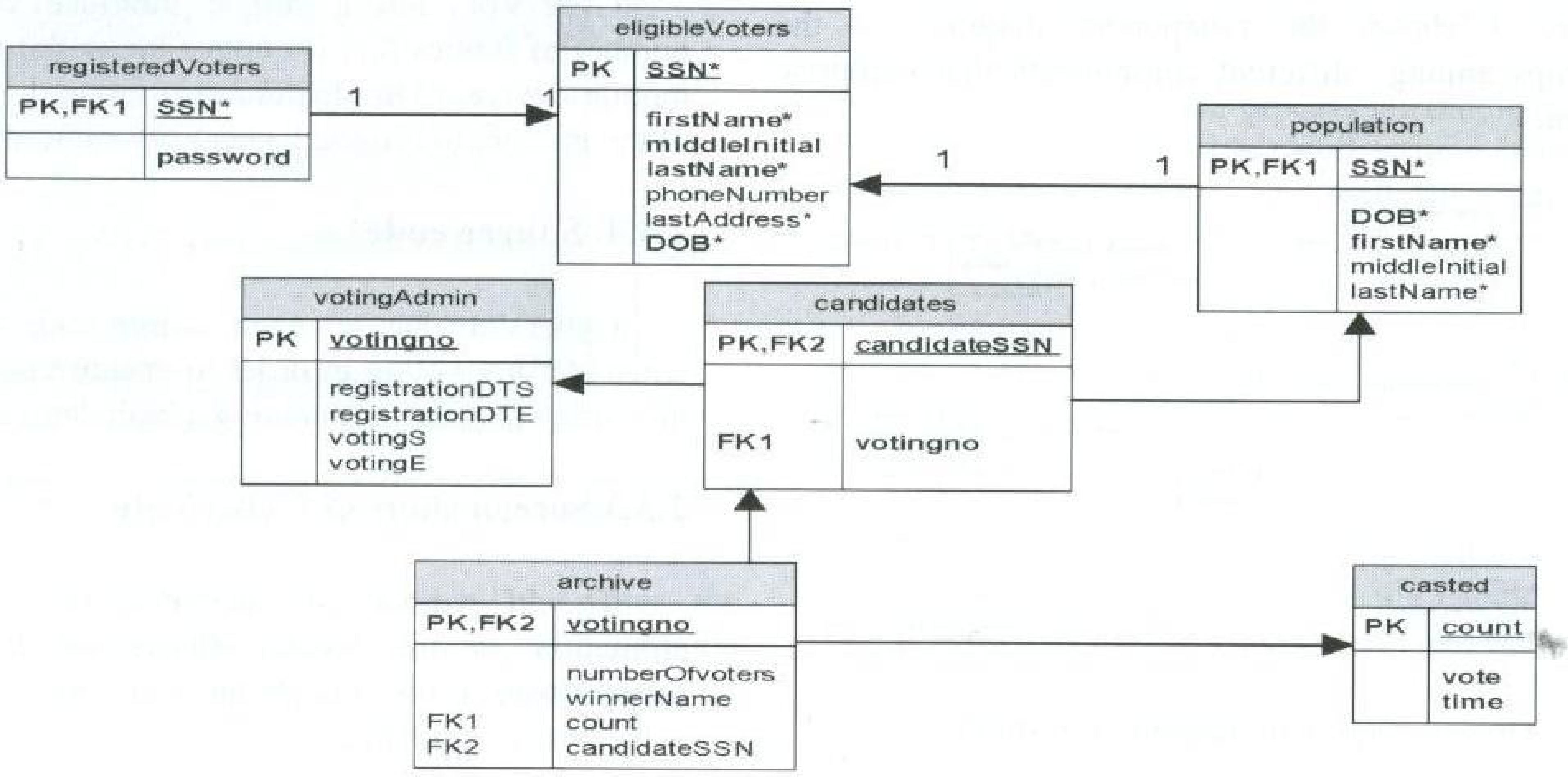


Figure 2: Relationships among the tables in CyberVote database.

2.2.3. Encryption Methods

CyberVote system uses different types of encrypting algorithms such as Secure Hashing Algorithm (SHA1), Message Digest Algorithm (MD5), SHA256, and SHA512. When a registered voter hits on register button, a random number will be generated. This number will determine the encryption algorithm. It will be encrypted afterwards, and will be added to the encrypted data. The technique provides high degree of security to the data of voters.

2.2.4. Classes

CyberVote uses different classes for security that Microsoft Visual Studio .Net provides, the main classes used are as follows:

1. SHA256, which provides SHA256 encryption method.
2. SHA512, which provides SHA512 encryption method.
3. FormsAuthentication, which provides SHA1 and MD5 encryption methods.

We used FbConnection class that provides the connectivity to the firebird database.

2.3. Implementation

The online voting systems use very complicated algorithms and methods trying to provide the security and privacy to voters. This complexity gives some doubts of having back doors in those systems. CyberVote system represents a very simple open source code system that ensures privacy and security of voters by providing the implementation phases step by step:

2.3.1. Component Diagram

Figure 3 shows the component diagram of the relationships among different components that comprise the system.

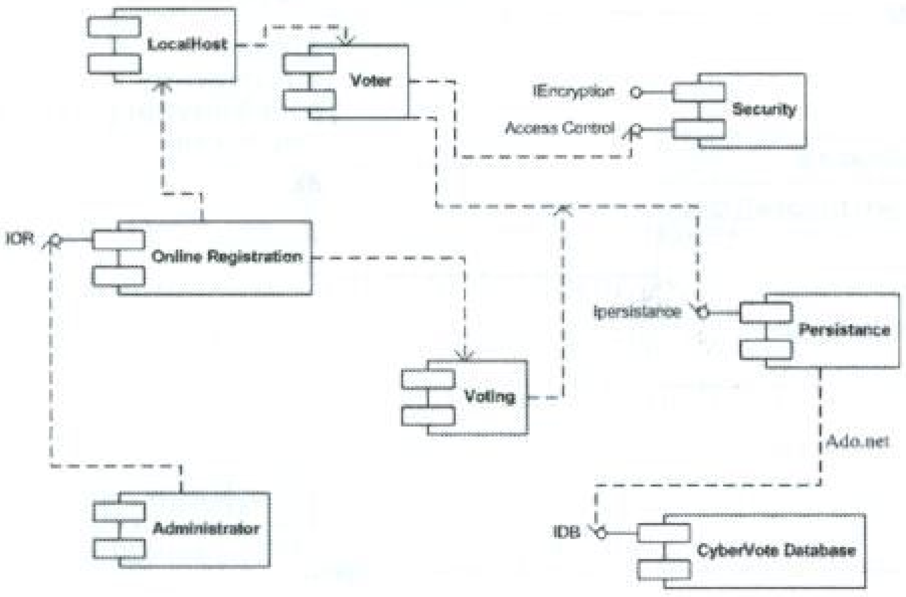


Figure3. Component diagram of CyberVote

We have implemented CyberVote using Firebird 1.5 database. Choosing this database was based on its open source code, which eliminates any probability of back doors. Also, it was implemented with ASP.Net due to the availability of encrypting algorithms that provide the required security for the system.

2.3.2. Administrator Authentication

CyberVote has different levels of authentication for different users, especially the employees controlling the population data. The emplyees they decide when and how to add new entries into the population, when to delete an entry, and when to alter an entry. CyberVote uses one level password given by two employees, i.e. the supervisor has to enter his/her password along with the employee in order to enable the employee work on adding new entries into the database. Altering the population database requires two level passwords from the employee, where altering can only change the information related to an entry, but not the social security number of an entry. Deleting requires three level passwords, which means that a supervisor and two employees should enter their passwords and usernames in order to enable the employee to work on deleting records from the database, any action will take place either adding entries, altering entries, or deleting entries will be documented in a separate table in the database, which consists of the action was done, Identification number of the employee working on this action, and a timestamp that shows the date and time of the update.

Another feature CyberVote is to ensure safety of its database is prompting the employees to change their passwords on regular bases. This feature increases the security of the system.

2.3.3. Layout of CyberVote

CyberVote has a simple interface with a minimal number of frames that is compatible with the handheld and mobile devices. This feature also helps the beginner users of the internet to browse CyberVote without any help.

2.3.4. Source code

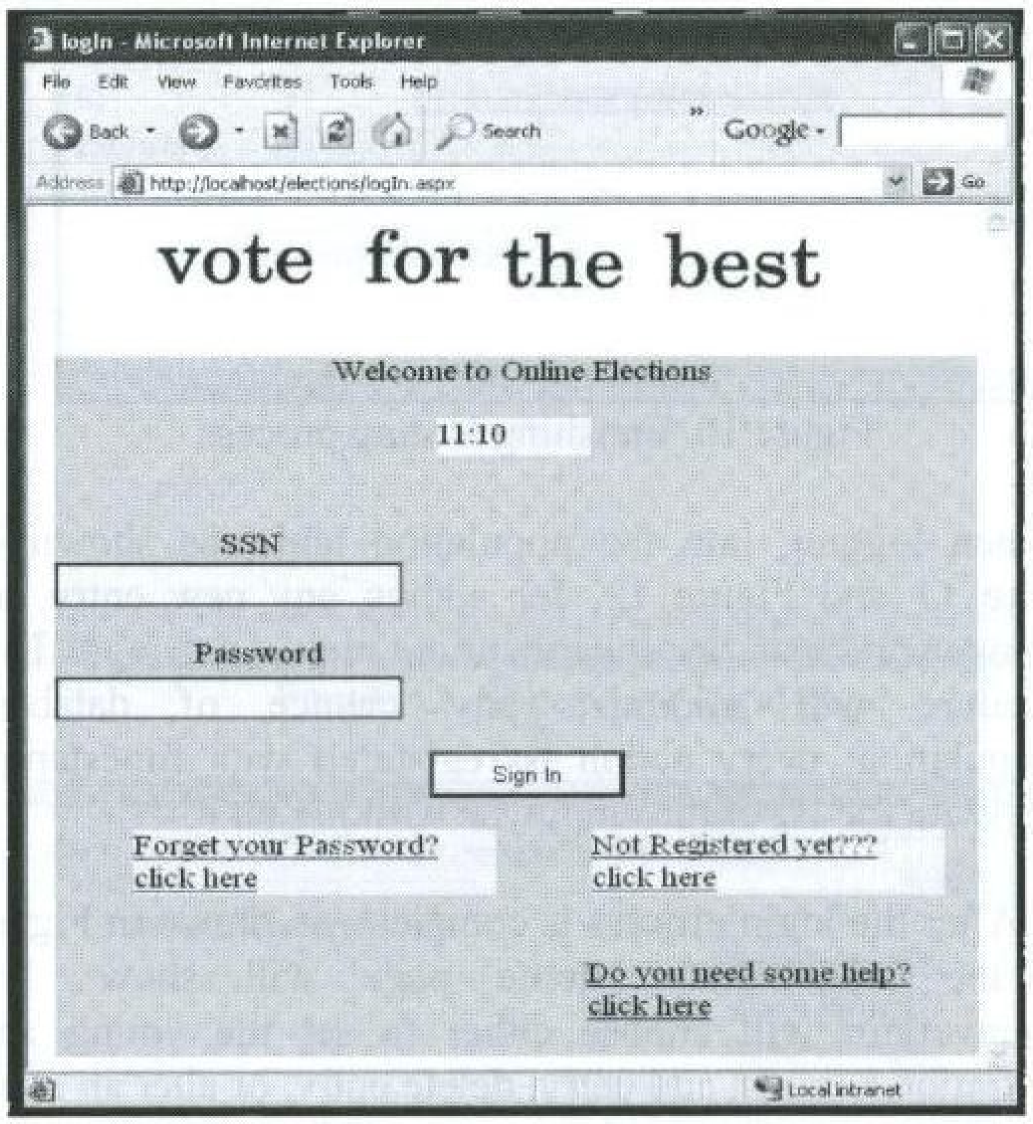
CyberVote has an open source code that is released when starting voting in order to ensure the transparency of the voting process maintaining a high degree of security.

2.3.3 Screen shots of CyberVote

The PC version of CyberVote has some light flash animation as the banner shows on the login page. Furthermore, it has a help link that comes in two different ways, text or animated.

2.3.3.1 Client Side

Web pages designed for voters should be easy to understand and use by all levels of society. It should consider other devices like handheld devices and mobile phones. The main logon page is shown in Figure 4.


logIn - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Google
Address http://localhost/elections/logIn.aspx
Go

vote for the best

Welcome to Online Elections

11:10

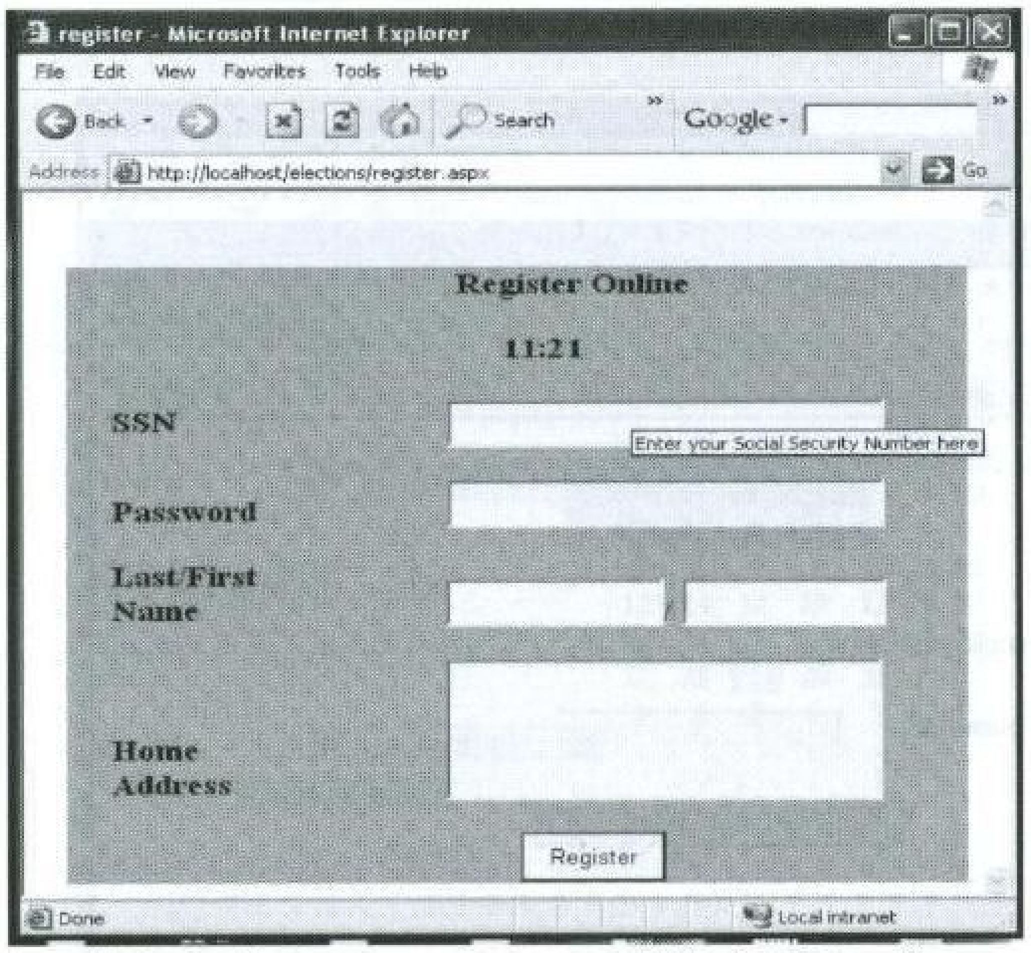
SSN

Password

Sign In
Forget your Password? click here
Not Registered yet??? click here
Do you need some help? click here
Local intranet

Figure 4. Login page of CyberVote system

If the voter is not registered yet, and registration period did not expire yet, voter should use the registration link that will invoke the registration module as shown in Figure 5.


register - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Google
Address http://localhost/elections/register.aspx
Go

Register Online

11:21

SSN: Enter your Social Security Number here

Password

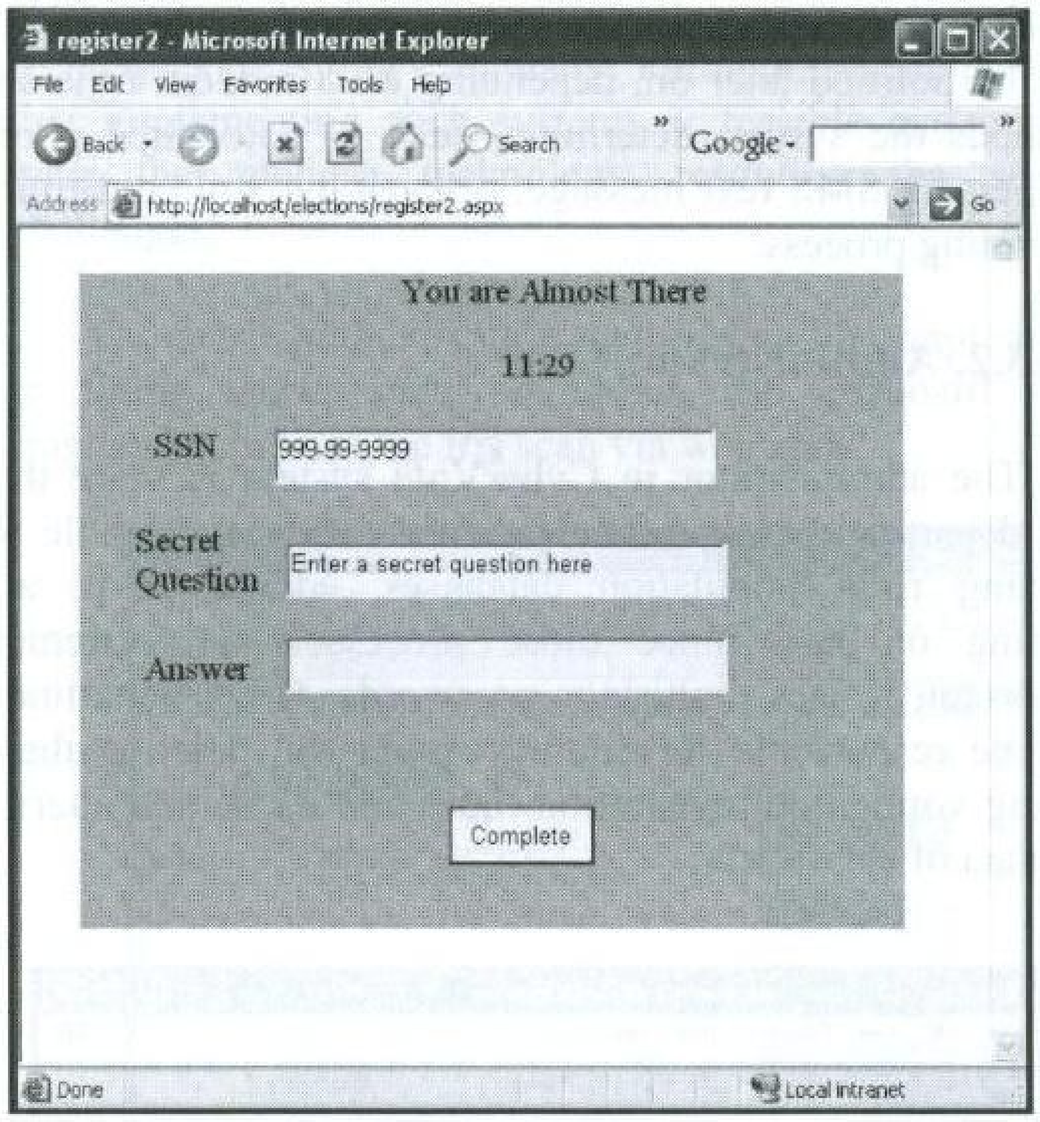
Last/First Name

Home Address

Register
Done
Local intranet

Figure5. Registration page of CyberVote System

After validating the data provided by the voter, the system will transform into the second step of registration asking for a secret question in case of the voter forgot the password as shown in Figure 6.


register2 - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Google
Address http://localhost/elections/register2.aspx
Go

You are Almost There

11:29

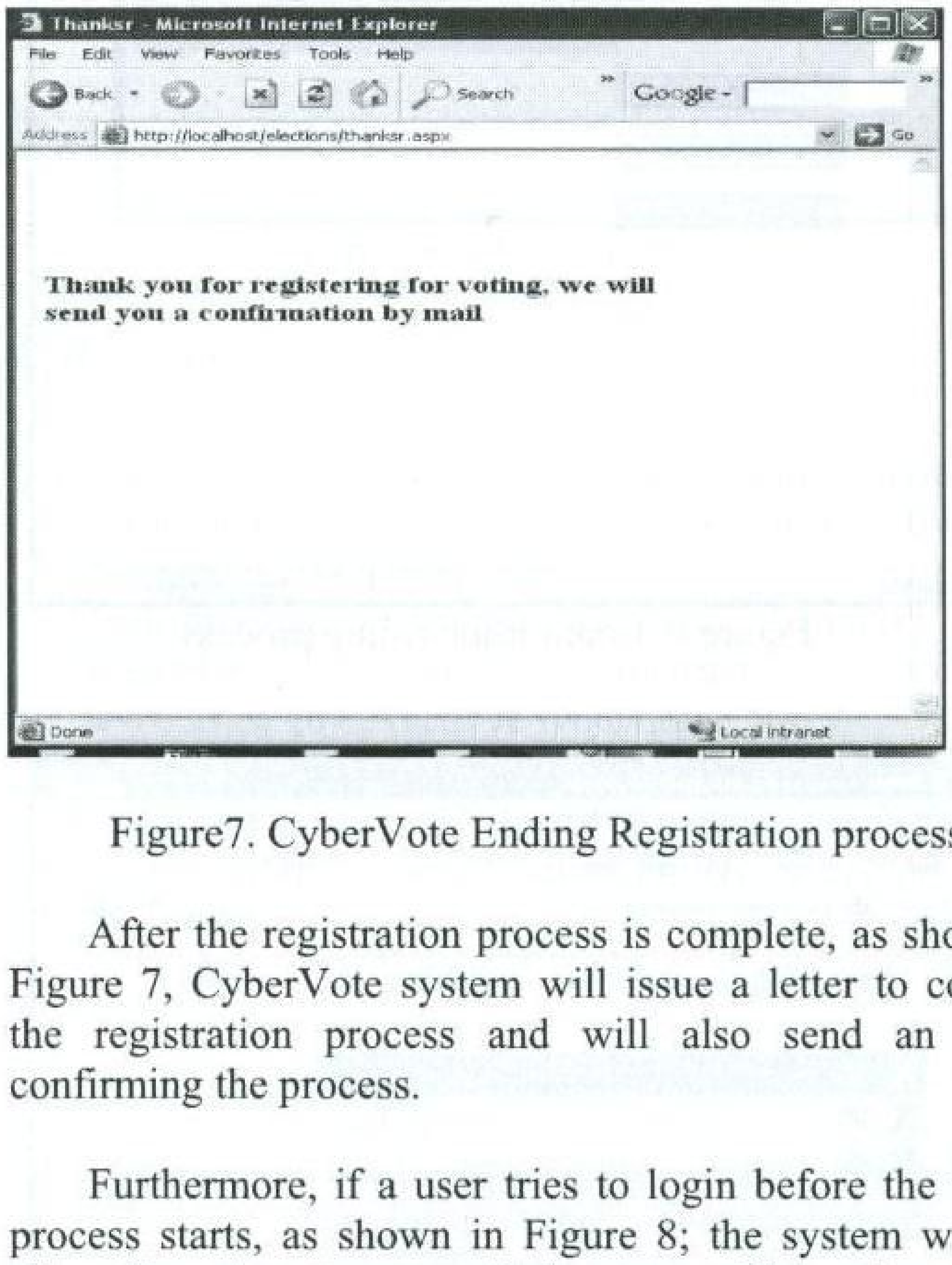
SSN: 999-99-9999

Secret Question: Enter a secret question here

Answer

Complete
Done
Local intranet

Figure 6. Registration page 2 of CyberVote System


Thanksr - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Google
Address http://localhost/elections/thanksr.aspx
Go

Thank you for registering for voting, we will send you a confirmation by mail

Figure7. CyberVote Ending Registration process

After the registration process is complete, as shown in Figure 7, CyberVote system will issue a letter to confirm the registration process and will also send an email confirming the process.

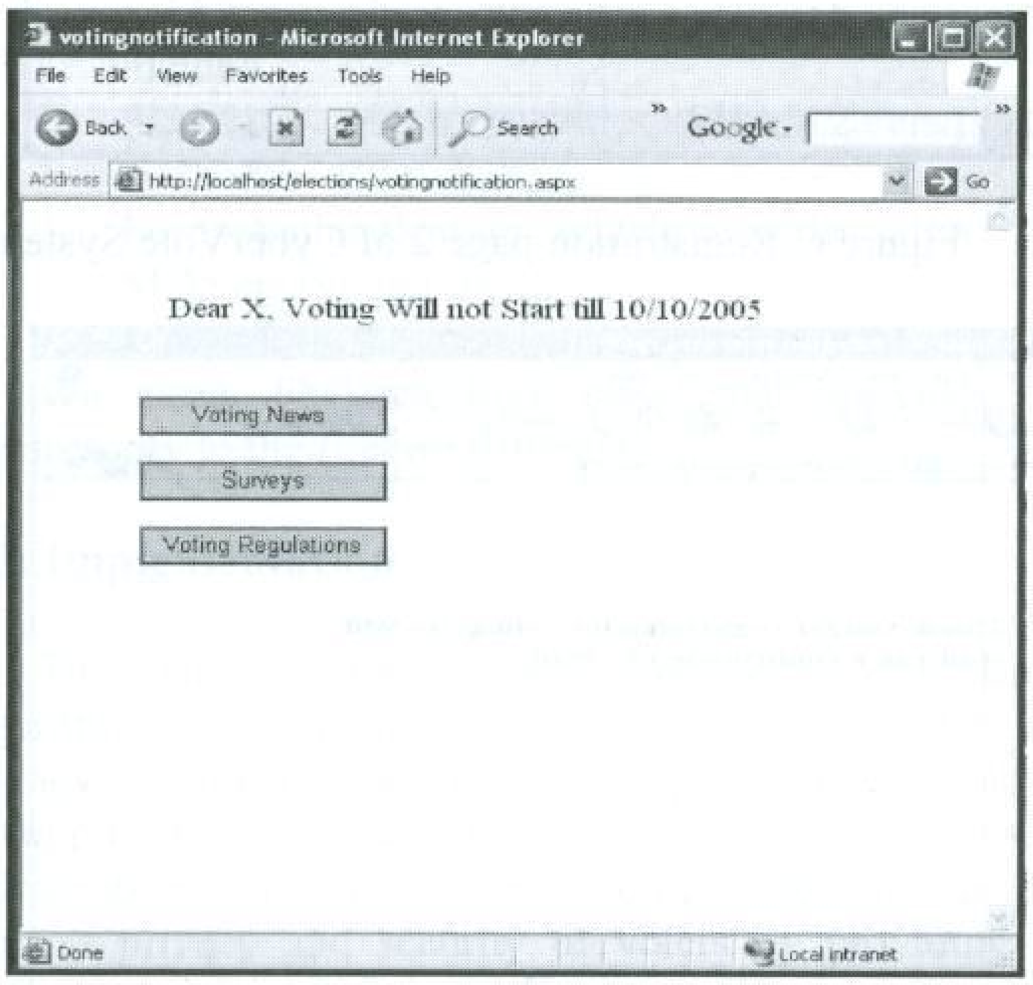
Furthermore, if a user tries to login before the voting process starts, as shown in Figure 8; the system will not allow the voters to access their pages, which enhances the security features of CyberVote security enhancement.

During the voting process, after signing into CyberVote, voters should choose the candidate out of the list as shown in Figure 9. Also, they get the chance not to choose any of the candidates.

When hitting on Vote, as shown in Figure 10, votes' data will be deleted from CyberVote database. The social security number will be added to the confirmation list, which is a list consists only of social security numbers that will be notified later on, depending on a random time and methods the system determine, such as automated phone call, email, SMS text message, or even by mail confirming the voting process.

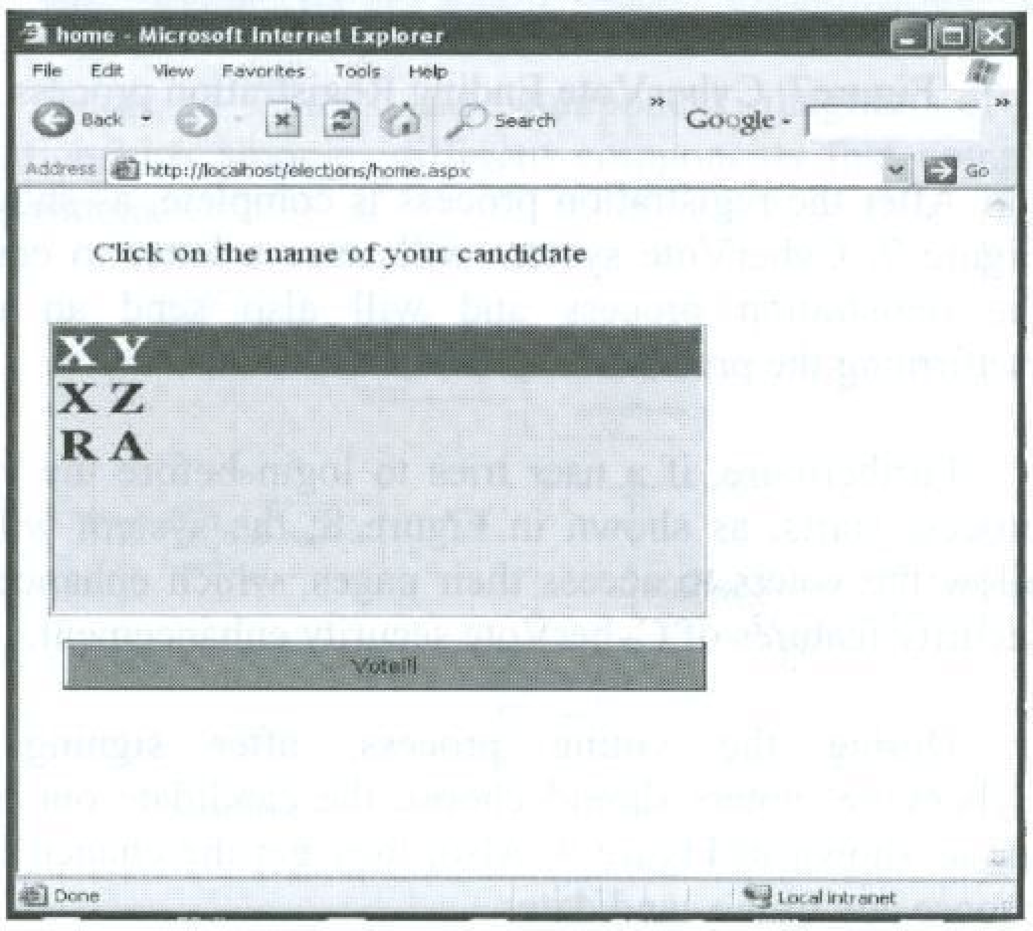
2.3.3.2. Administrator Side

The administrator in CyberVote system is more than one department. Administrator is an entity responsible for deleting from population databases, adding to it, and altering on it. Since those processes are extremely important, it uses multistage passwords. Other department will be responsible for adding candidates, deleting them, setting voting and registration times and dates, and altering the data of candidates.


votingnotification - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Google
Address http://localhost/elections/votingnotification.aspx
Go
Voting News
Surveys
Voting Regulations
Done
Local intranet

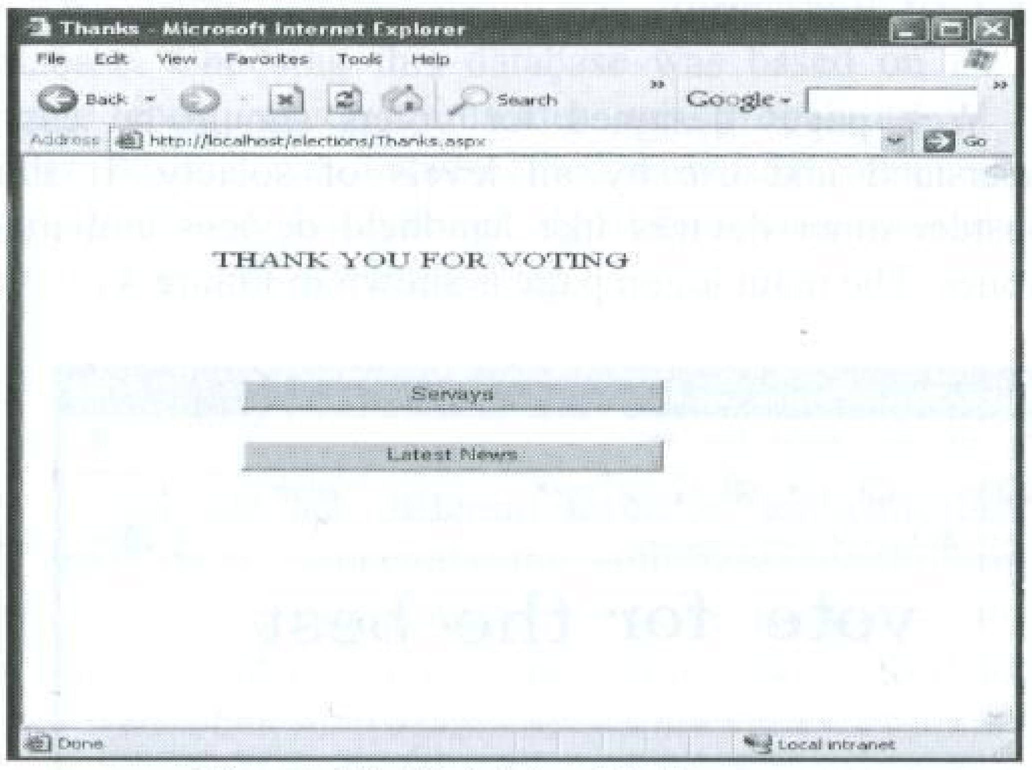
Dear X, Voting Will not Start till 10/10/2005

Figure 8. Login prior voting process


home - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Google
Address http://localhost/elections/home.aspx
Go
X Y
X Z
R A
Vote!!
Done
Local intranet

Click on the name of your candidate

Figure 9. Voting home page


Thanks - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Google
Address http://localhost/elections/Thanks.aspx
Go
Servays
Latest News
Done
Local intranet

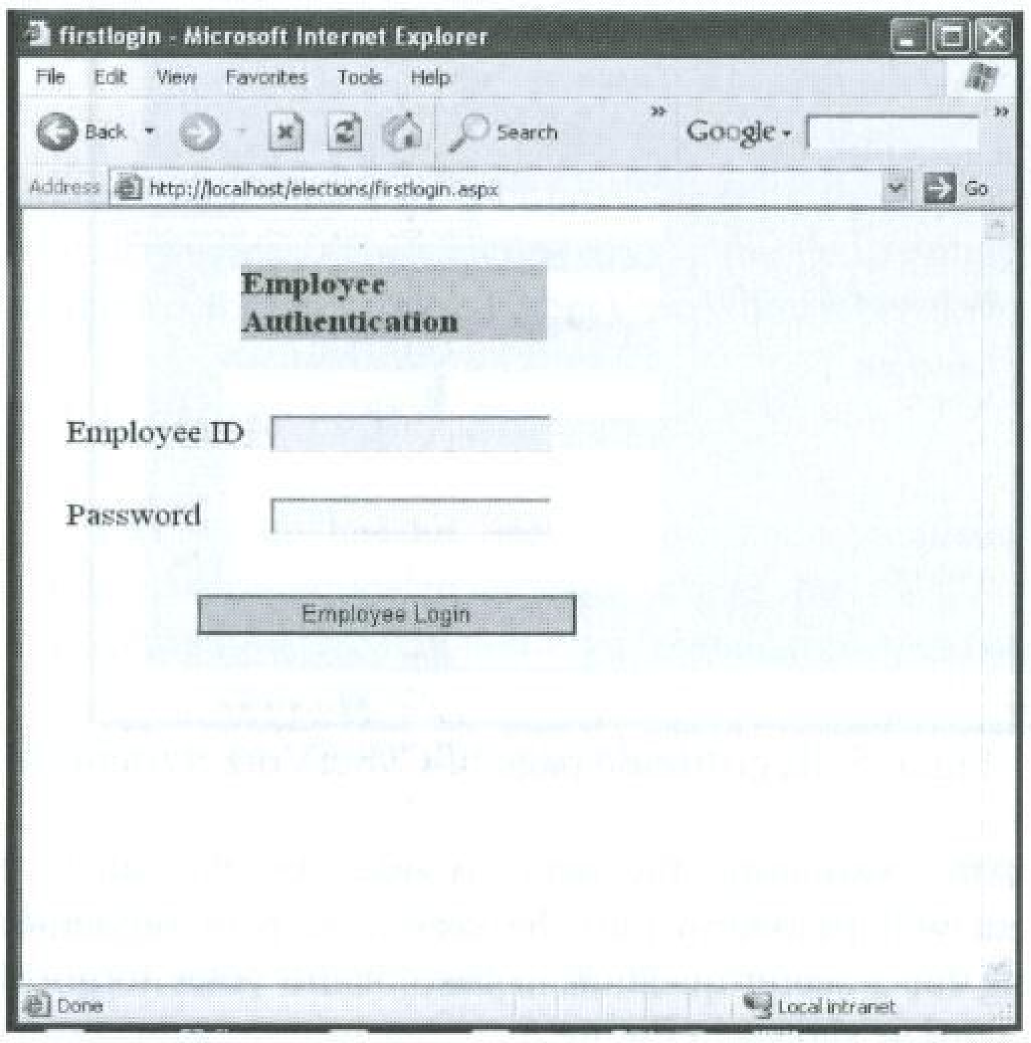
THANK YOU FOR VOTING

Figure 10. Finishing Voting process

When logging into the population table, as shown in Figure 11 and Figure 12, for adding any new entry, an employee and his / her supervisor are required to sign. This procedure will minimize any chance of database manipulation; every action is registered with timestamps along with the ID of the employee working on it.

After the login process is complete, as shown in Figure 13, the administrator home page will show. The Administrator will choose either to set the voting and registration periods, add entry, delete entry, or alter an entry as shown in Figure 14. The previous page, will enable the administrator to specify the times and dates for both registration and voting processes.

When adding a candidate, as shown in Figure 15, the candidate will be validated according to the voting regulations, and then will be added to the candidate database.


firstlogin - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Google
Address http://localhost/elections/firstlogin.aspx
Go
Employee Login
Done
Local intranet

Employee Authentication

Employee ID

Password

Figure 11. An Employee should login first

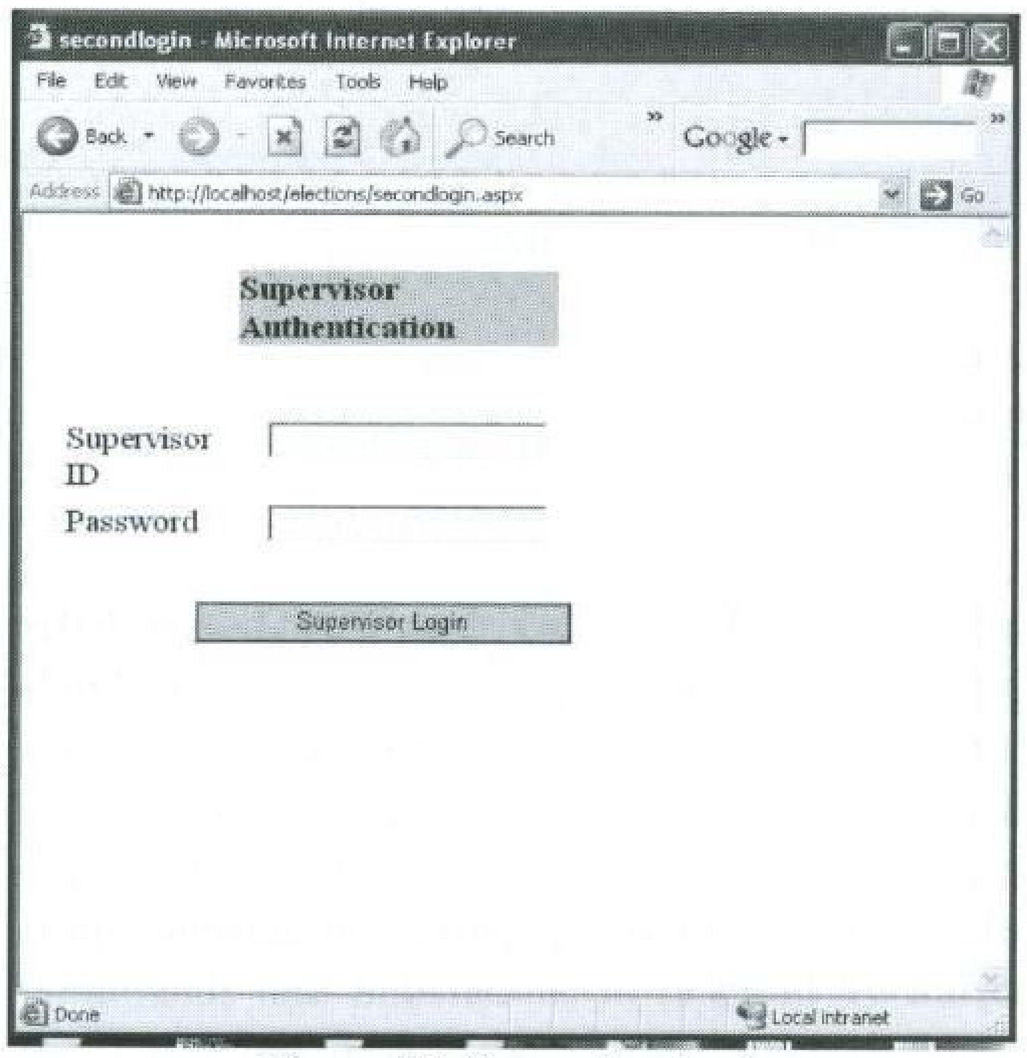

secondlogin - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Google
Address http://localhost/elections/secondlogin.aspx Go
Supervisor Authentication
Supervisor ID
Password
Supervisor Login
Done
Local intranet

Figure 12. Supervisor login page

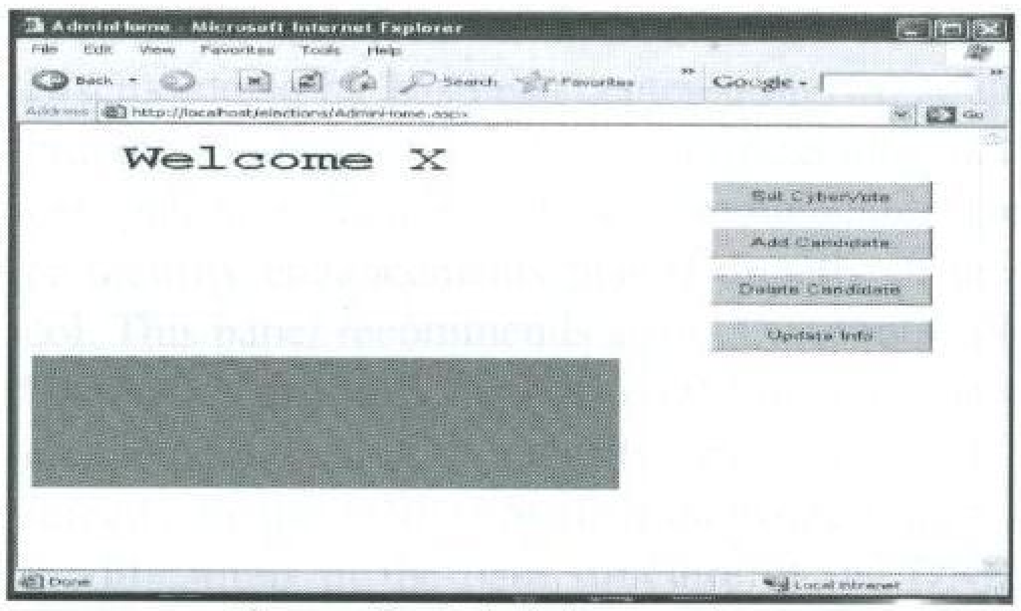
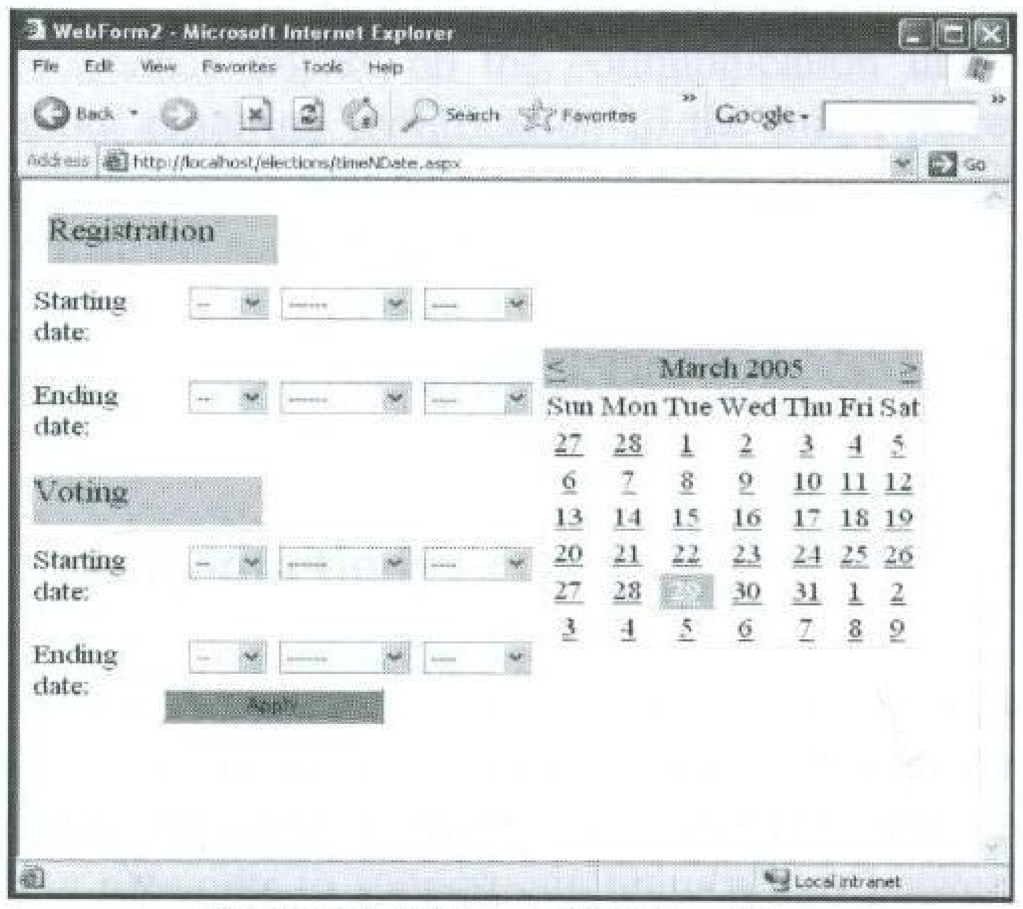

AdminHome - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Google
Address http://localhost/elections/AdminHome.aspx Go
Welcome X
Set CyberVote
Add Candidate
Delete Candidate
Update Info
Done
Local intranet

Figure 13. Administrator home page


WebForm2 - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Google
Address http://localhost/elections/timeNDate.aspx Go
Registration
Starting date:
Ending date:
Voting
Starting date:
Ending date:
Apply
Local intranet

<			March 2005			>
Sun	Mon	Tue	Wed	Thu	Fri	Sat
27	28	1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30	31	1	2
3	4	5	6	7	8	9

Figure 14. Time and Date setting

3. Conclusion and future work

In this paper we presented CyberVote system. CyberVote is a new step in the development of remote online voting. In this technique we separate the voters from their ballots. Similar systems will replace the traditional techniques of voting eventually. Furthermore, studies show that implementing such systems is feasible and practical with the modern technology resolving the security challenges.

Biometric authentication methods will be implemented in future work, such as adding the keyboard stroke fingerprint and use the iris scan via webcams.

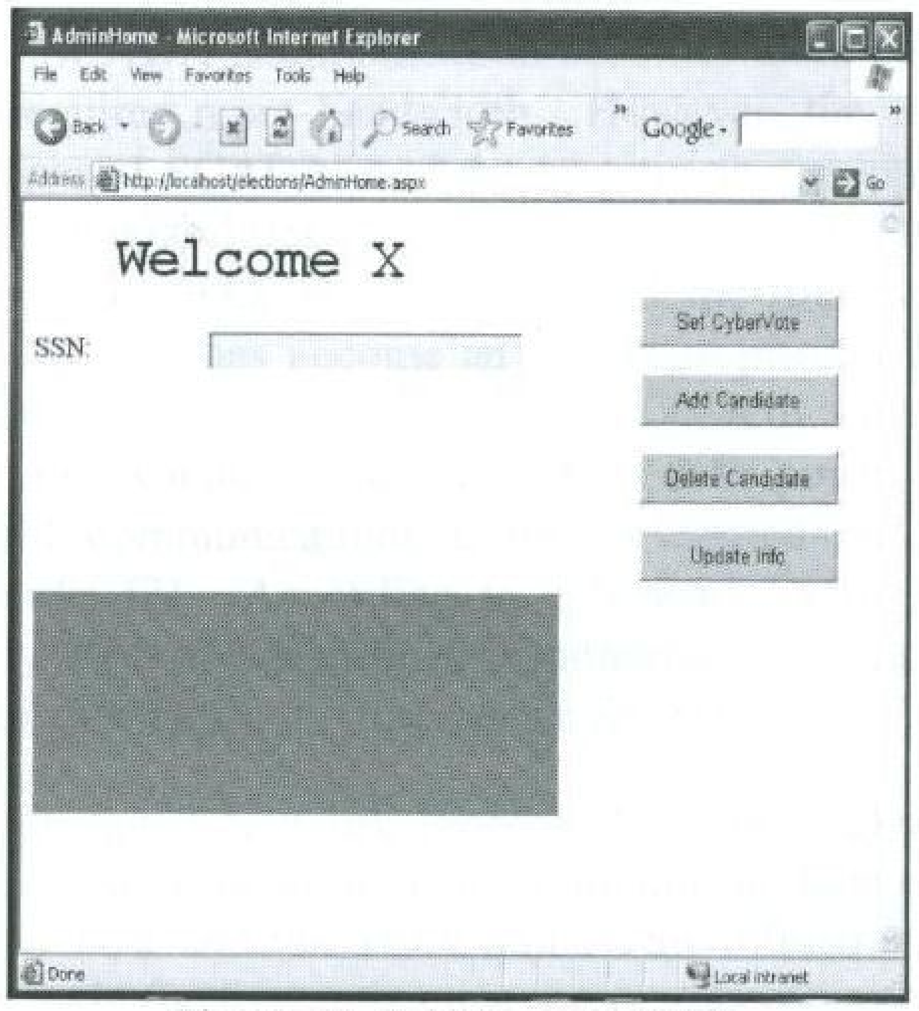

AdminHome - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Google
Address http://localhost/elections/AdminHome.aspx Go
Welcome X
SSN:
Set CyberVote
Add Candidate
Delete Candidate
Update Info
Done
Local intranet

Figure 15. Adding a candidate

4. References

[1] Rebecca Mercuri, "Inside risks: voting automation (early and often?)", *Communications of the ACM*, 43, November 2000, page: 176.

[2] California Internet Voting Task Force, "A report on the feasibility of Internet voting", www.ss.ca.gov/executive/ivote/home.htm

[3] Workshop on Privacy in the Electronic Society, *Proceedings of the 2004 ACM workshop on Privacy in the electronic society,* Washington DC, USA, pp.: 33 – 34, 2004.

[4] Computers, Freedom and Privacy, *Proceedings of the tenth conference on Computers, freedom and privacy: challenging the assumptions,* Toronto, Ontario, Canada pp. 219 – 223, 2000.

[5] L. Hoffman and L. and Cranor, "Internet Voting for Public Officials: Introduction", *Communications of the ACM*, 44, January 2001, pp. 69-71.

[6] Tom Pender, UML Bible, John Wiley & Sons, 2003.

[7] Phillips and Spakovsky, "Gauging the risks of internet elections", *Communications of the ACM,* 44, January 2001, pp. 73-85.

[8] Joe Mohen and Julia Glidden, "The case for internet voting", *Communications of the ACM,* 44, p.44.

[9] Aviel D. Rubin," Security Considerations of remote electronic voting", *Communications of the ACM,*45, December 2002, pp. 39- 44.