European Journal of Scientific Research
ISSN 1450-216X Vol.51 No.2 (2011), pp.276-284

http://www.eurojournals.com/ejsr.htm

Secured Single Transaction E-voting Protocol: Design and Implementation

Kalaichelvi. V.
Asst. Professor (Ph. D Scholar), SRC- Sastra University, Kumbakonam
E-mail: kalaichelvi2k@yahoo.com

R. M. Chandrasekaran
Professor, Annamalai University, Annamalai Nagar

Abstract

In this paper, we propose a secure e-voting protocol. Our scheme does not require a special voting channel and communication can occur entirely over the current Internet. This method integrates Internet convenience and cryptology. In the existing protocols either the tallier has to wait for the decryption key from voter till the voting process is over or the verification process has to wait until the election is over. But in the proposed single transaction voting protocol the entire voting process as well as the verification process is done in a single transaction compared to multiple transactions in the existing protocol. The advantage of single transaction is that it consumes less time that results in overall speeding up the voting process. It is shown that the proposed scheme satisfies the more important requirements of any e-voting scheme: completeness, correctness, privacy, security and uniqueness.

Keywords: E-voting, Cryptology, Privacy and Internet

1.0. Introduction

Voting and elections are essential ingredients of modern communities. Unlike any other transactional event, the result of elections can have many positive and/or negative effects on these communities and their wellbeing. For many years, elections, in general, have suffered from declining participation rates due to the inconvenience of manual voting. Manual voting has several other drawbacks among which are inaccuracy in ballot counting and the delayed announcement of election results [1]. To overcome these drawbacks, the Electronic Voting (e-voting) technique, the use of computers or computerized equipment to cast votes in elections, has been proposed. Evoting automates and simplifies the election process, speeds it up, increases participation rates, reduces counting mistakes and minimizes the time it takes to announce results.

Three main approaches in the electronic voting scheme are 1.Blind Signatures: The involved parties in these schemes are the voters, the administrator, the counter and the bulletin board. In cryptography, a blind signature is a form of digital signature in which the content of a message is disguised before it is signed. The resulting blind signature can be publicly verified against the original unblended message in the manner of a regular digital signature. Blind signatures are typically employees in privacy-related protocols where the signer and message author are different parties. Examples include cryptographic election systems and digital cash schemes [2,3,4,5]. 2. Homomorphic encryption: It is a form of encryption where one can perform a specific algebraic operation on the plaintext by performing an algebraic operation on the cipher text. The Homomorphic property of various cryptosystems can be used to create secure voting systems, collision-resistant hash functions and private information retrieval schemes.There are several efficient Homomorphic cryptosystems, RSA cryptosystem, ElGamal cryptosystem, Gold Wasser- Micali cryptosystem, Benaloh cryptosystem, Okamoto-Uchiyama cryptosystem, Paillier cryptosystem, Naccachestern cryptosystem, Damgard-Jurik cryptosystem, Boneh- Goh- Nissim cryptosystem [6-10]. 3. Schemes using mixnets also known as Digital mixes: Digital mixes make hard to trace communication by using a chain of proxy servers. Each message is encrypted to each proxy using public key cryptography [11-12].

2.0. Existing Voting System

2.1. The Traditional Voting Process

We start from a traditional voting process that can be divided into four steps

Authentication – Alice walks into a voting precinct and authenticates herself by showing her voting credentials; this step is public and verified by the officials present in the room. At the end of the authentication process, Alice is given a paper ballot on which to write her vote.

Vote – The vote takes place in a protected booth where she cannot be seen by anyone. Alice casts her vote by writing it with a pencil on the paper ballot; she then folds the paper ballot and puts it in the ballot box where all the votes are mixed. Since no one can see what Alice writes and there are no marks on the paper ballots, Alice's vote is anonymous.

Counting the votes – At the end of the voting time, the officials open the box containing the paper ballots and publicly count the votes; the results are then announced.

Verification – Various types of verification are used or possible, most procedures are indeed public and overseen by representatives of competing parties. The opposite interests of the parties warrant the first level of protection against fraud. A recount is also possible if there is a presumption of fraud or error.

There are lot of problems in conventional voting:

- Printing of ballot paper is expensive.
- Voting consumes lot of time
- Counting is prone to errors.
- Maintaining convenient poll booths is very difficult.
- There is no good relationship between the government and popular, popular cannot trust the government and depend on it, voter here is like a blind person that must rely on the other person to vote for him.
- Sometimes, government coerced and carries on the voters to vote for a particular candidate, and eliminate them from voting freely.
- Some candidates trying to win by buy the votes from the voters.
- Government can cheat by substitute the original ballot by derivative ones.

2.2. Requirement of E-voting

The requirement in conventional voting (paper vote) are also apply for e-voting, the requirements can expected to be universal, any system must try to apply these requirements:

Fairness: No one can learn the voting outcome before the tally.
Eligibility: Only eligible voters are permitted to vote.
Uniqueness: No voter should be able to vote more than once.
Privacy: No one can access any information about the voters vote.
Completeness/Accuracy: All valid votes should be counted correctly.
Soundness: Any invalid vote should not be counted.
Uncoercibility: No voter can prove how he voted to others to prevent bribery.
Efficiency: The computations can be performed within a reasonable amount of time.
Robustness: A malicious voters cannot frustrate or disturb the election.

In electronic voting system, which is an advancement over the conventional voting system, the problem of printing ballots and the problem of counting are solved, but maintaining convenient poll booths is still difficult. So there must be another way to solve these problems or reduce it as possible, and give the voters the confidence to believe of the system, from this point we think to use a new technology to improve the election by building a new system that is convenience for environment. The only alternative to overcome these problems is to make use of online voting system. With the advent of Internet and World Wide Web, it is easy to design a secure online voting system.

3.0. Our Proposed Electronic Voting System

Before talking about the proposed electronic voting system we need to define the biometric token (smart card) and the feature of it, and why we use it in our system, and how can it be useful for the voters in election.

In this system, smart card is used as a storage media to store the information of the voters, other personal data and the Unique Id (11-digit number TN/99/0000012 – In this, TN specifies the State, Next two digit specifies District Id and third one specifies the Unique id for each eligible voter) and Iris pattern (unique for each user-static one). But why smart token, why it is the best for electronic voting?. Because it is a temporarily store media, and an anonymous media, which provide a secure way to save the information of the cardholders.

In this system we are using 16 KBytes EEPROM ACOS 3 smart card. The memory area provided by the card chip is basically segregated in internal data memory and user data memory. The internal data memory is used for the storage of configuration data and it is used by the card operating system to manage certain functions. The user data memory stores the data manipulated in the normal use of the card under the control of the application. Memory area is possible within the scope of data files and data records. The maximum number of data files allowed in ACOS 3 is 31. A data file can contain up to 255 records. User data files are allocated in the personalization stage of the card life cycle. Once the personalization bit has been programmed there is no possibility of resetting the card back.

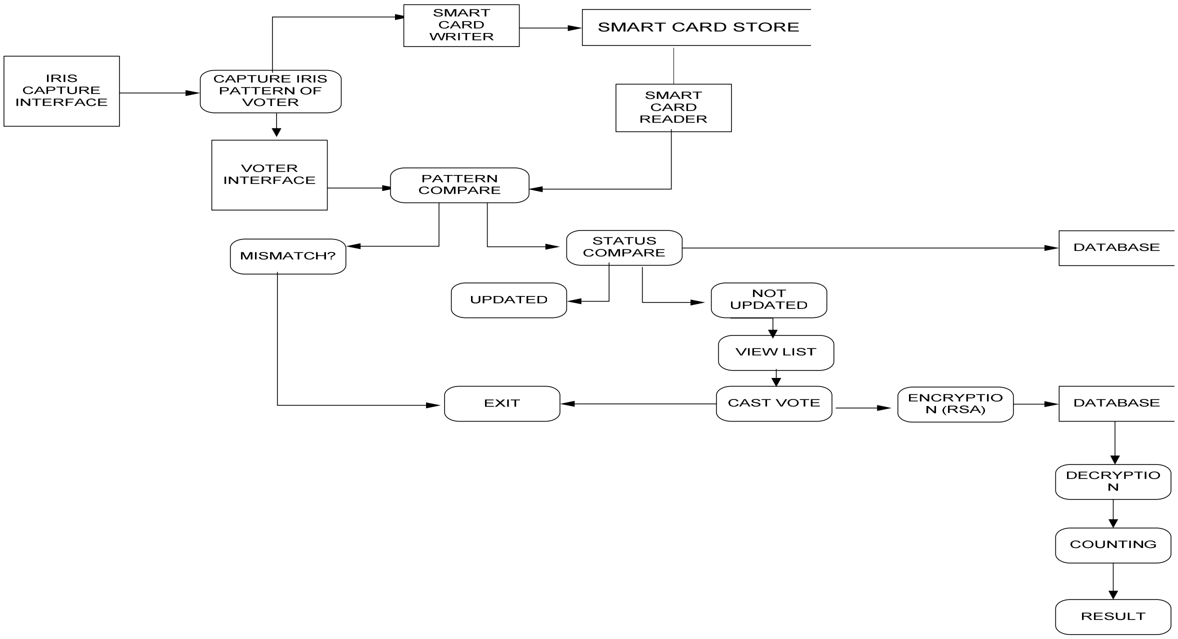
In the proposed electronic voting system we will use biometric with smart token and we will use the iris pattern as a template, to verify the voter in the election. Once the Smart card is inserted by the voter into the poll machine match the Iris pattern template that is stored in smart card with the real time Iris pattern taken via camera using VeriEye techniques automatically. If the captured iris pattern matches the iris pattern templates in the smart card, the voter will be verified for the system.

The online voting system is designed to allow the voter to give vote securely over the Internet. The modules in the online voting system are the following:

- Administrator for registration by registrar and creation of new poll by pollster through the private network.
- Voter gives vote through Internet.
- Validator checks the validity of the voter and sends confirmation of the voter through the Internet.
- Tallier receives the vote through the Internet.

The various features that are incorporated in the protocol can be summarized into five categories namely Administrator module, Voter Module, Validator Module and Tallier Module.

Figure 1: Proposed Voting Model



Registration

The process of voter registration is always done by Administrator before few days of the election process as follows:

- Registration phase begins by storing the Voter information such as Voter ID, Name, Age, Sex, Address and District in the database.
- Obtaining the **Iris pattern** of users and storing it in the **Smart card**.
- Testing and Issuing of the Smart card to the voter.

This part is a preparation step for implementing this proposed system, only after the issue of the smart card after proper authentication and testing the smart card can be used. So, this step has to be started and completed before the process of election.

Validation

The voter identification is the first step in the process of voting according to this system. The step is similar to the login part of a project as the following operations are to be done in identifying the voter:

- Obtaining the iris pattern of user using an iris recognition device on the polling booths.
- Obtaining the approved iris pattern of the user from the smart card provide through smart card reader.
- Comparing the two patterns to know whether they match or not.
- On matching the user identification is confirmed and further steps are taken.
- On mismatch the user is notified regarding the mismatch and proper enquiry and alternate solutions is done.

Voting

Once the voter is authenticated then, the Validator sends the confirmation message to the Tallier. The Tallier performs the following operations during the voting phase:

- The Tallier interacts with the pollster to retrieve the poll name and the candidate names.
- Before giving the vote by voter the Tallier checks the validity whether the voter can give vote or not.
- It checks in the database where the voter IDs is stored who have already given vote and the status of the voter whether it is 0 or 1.

- If it the status=1 then it shows the error and the voter can't give vote.
- If the status=0 then Tallier provides the voting page to voter to give vote based on the voter ID.
- The voter selects the option by clicking the options.
- Immediately that vote will be updated in the local databases and the count will be incremented and the status=1 will be updated for that voter.
- The vote will be encrypted with the Public key and sends the encrypted vote through the network. By this time all the casted votes are stored in the local database of each booth and in this step the local databases are sent to the distributed database for further processing like counting, announcement of results and record maintains.

Tallying

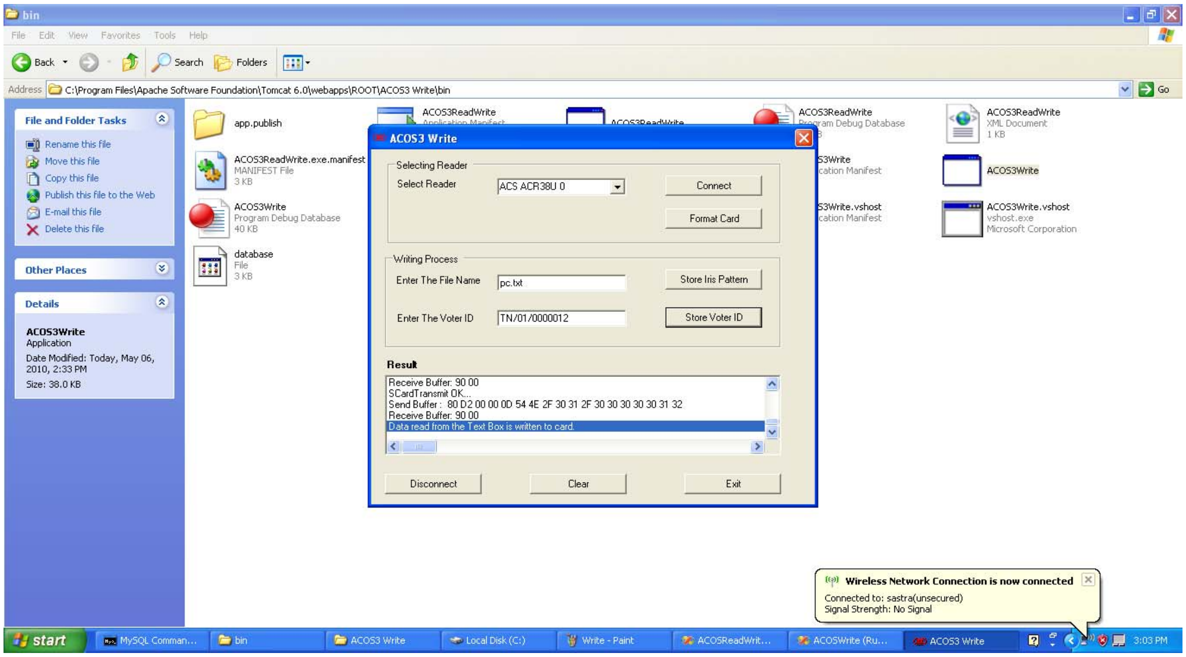
This part is completely hidden to the voter and this process is started only when the time for polling is over. After receiving the encrypted vote the Tallier performs the following operations during counting phase:

- Tallier gets the private key and decrypts the vote.
- Immediately that total number of vote will be counted in the distributed databases and will be updated.

Since the data are in the form of digital nature the counting process becomes very easy and the possibility of error in counting is negligibly small.

Experimental Results

Smart card – Writer Form



Address: C:\Program Files\Apache Software Foundation\Tomcat 6.0\webapps\ROOT\ACOS3 Write\bin

ACOS3 Write

Selecting Reader

Select Reader: ACS ACR38U 0

Writing Process

Enter The File Name: pc.txt

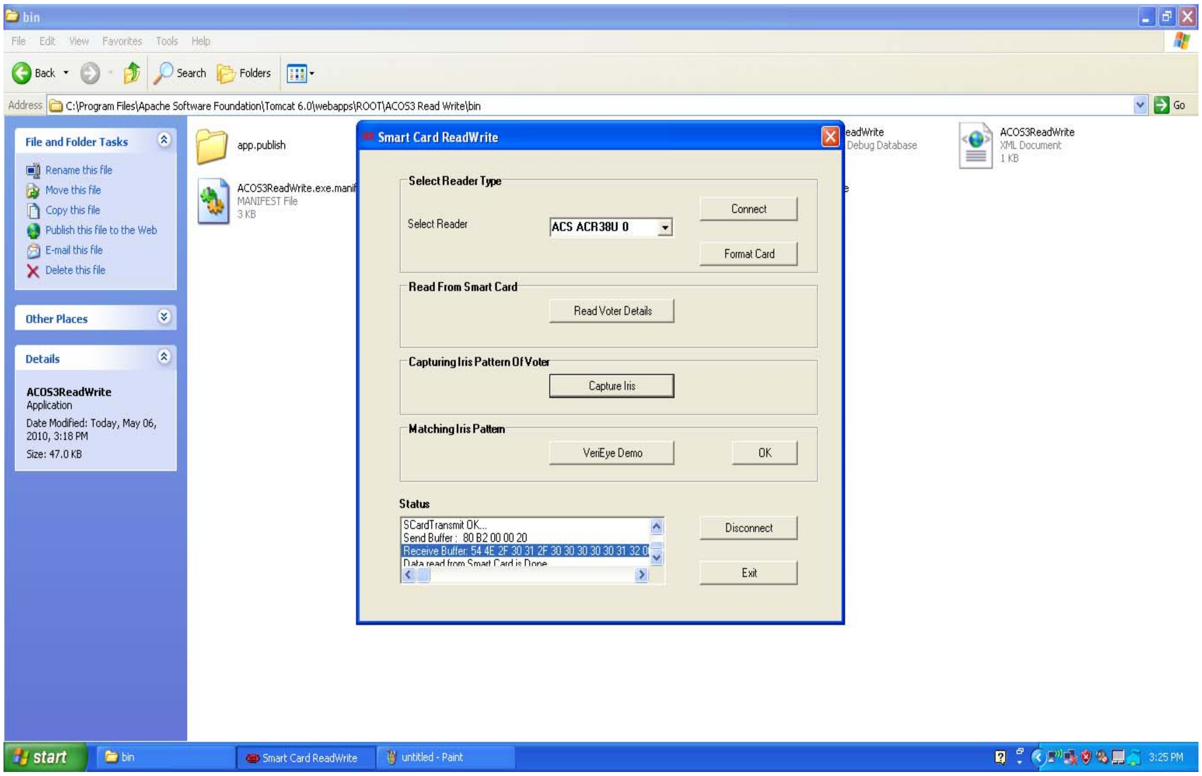
Enter The Voter ID: TN/01/0000012

Result

```
Receive Buffer: 90 00
SCardTransmit OK...
Send Buffer :  80 D2 00 00 0D 54 4E 2F 30 31 2F 30 30 30 30 30 31 32
Receive Buffer: 90 00
Data read from the Text Box is written to card.
```

Wireless Network Connection is now connected
Connected to: sastra(unsecured)
Signal Strength: No Signal

Smart Card – Reader Form



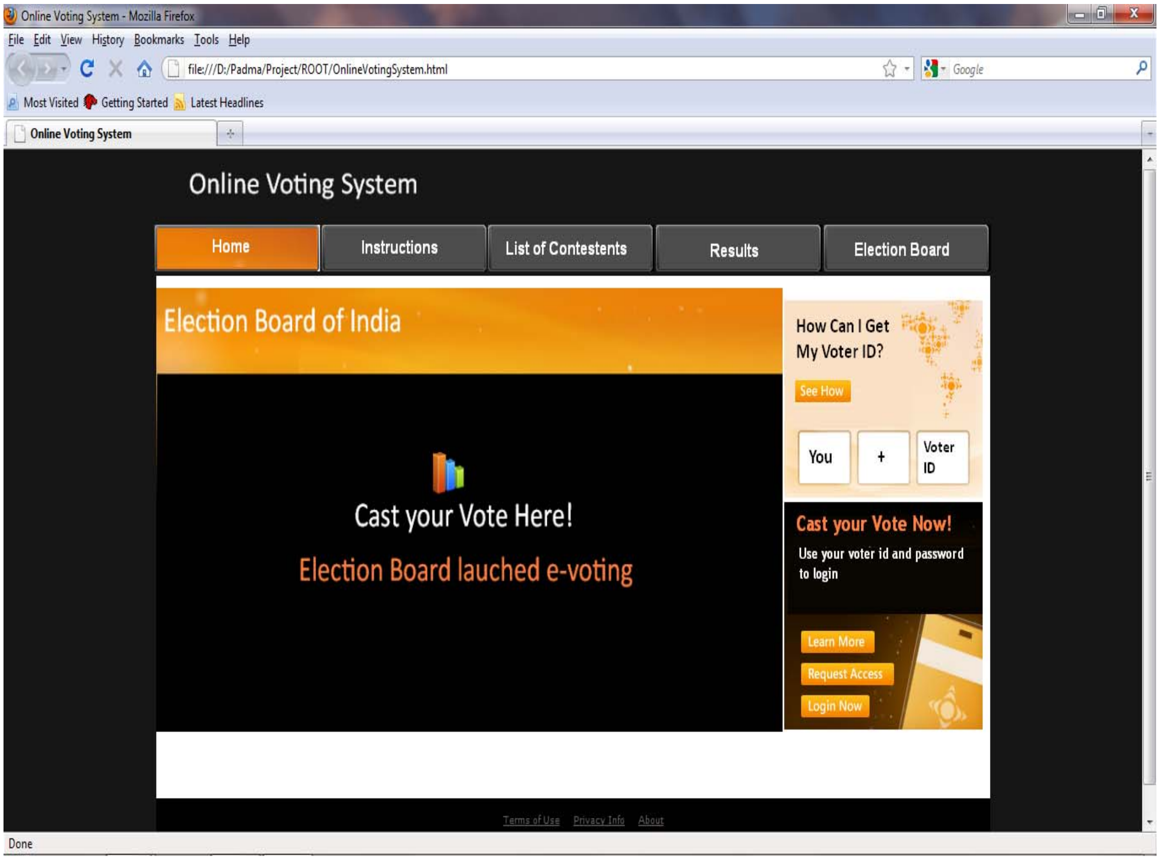
Address: C:\Program Files\Apache Software Foundation\Tomcat 6.0\webapps\ROOT\ACOS3 Read Write\bin

ACOS3ReadWrite
Application
Date Modified: Today, May 06, 2010, 3:18 PM
Size: 47.0 KB

Select Reader: ACS ACR38U 0

```
SCardTransmit OK...
Send Buffer :  80 B2 00 00 20
Receive Buffer: 54 4E 2F 30 31 2F 30 30 30 30 30 31 32 0
Data read from Smart Card is Done
```

Voter – Home Page



file:///D:/Padma/Project/ROOT/OnlineVotingSystem.html

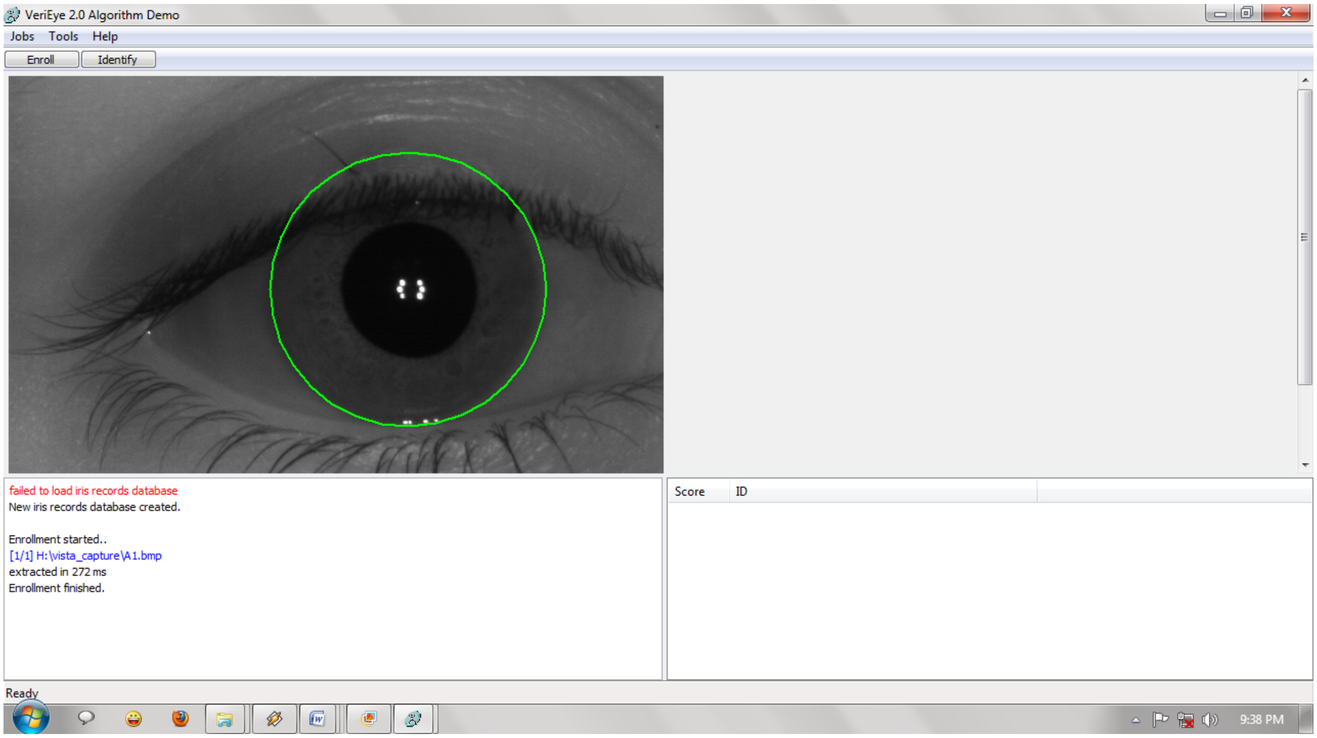
Cast your Vote Here!

Election Board lauched e-voting

Cast your Vote Now!

Use your voter id and password to login

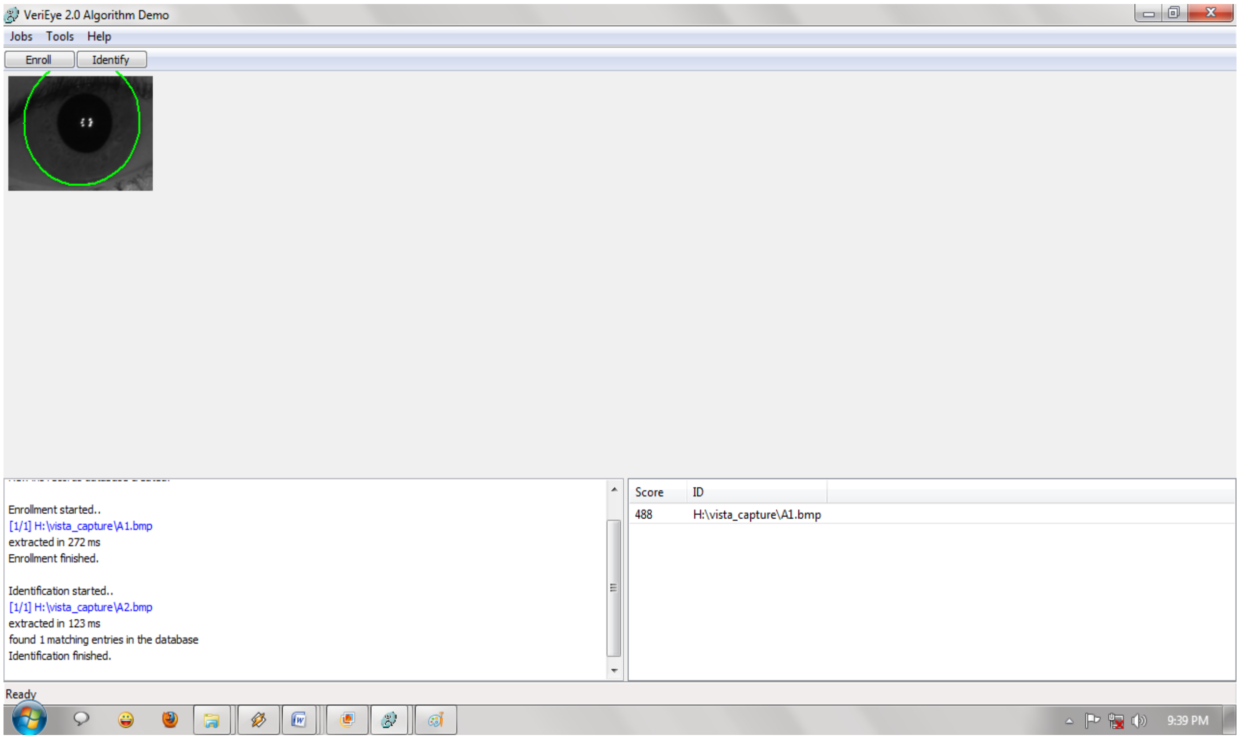
VeriEye – Enrollment



```
failed to load iris records database
New iris records database created.

Enrollment started..
[1/1] H:\vista_capture\A1.bmp
extracted in 272 ms
Enrollment finished.
```

VeriEye – Identification

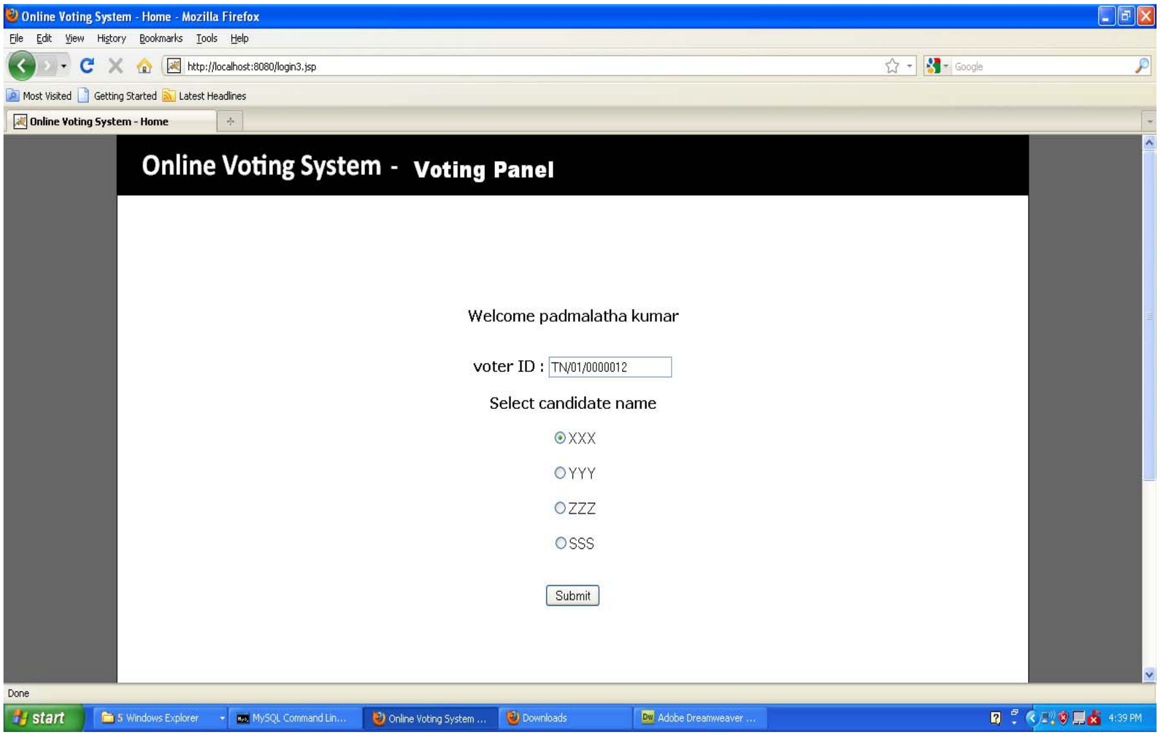


```
Enrollment started..
[1/1] H:\vista_capture\A1.bmp
extracted in 272 ms
Enrollment finished.

Identification started..
[1/1] H:\vista_capture\A2.bmp
extracted in 123 ms
found 1 matching entries in the database
Identification finished.
```

Score	ID
488	H:\vista_capture\A1.bmp

Candidate List Panel


Online Voting System - Home - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://localhost:8080/login3.jsp
Google
Most Visited Getting Started Latest Headlines
Online Voting System - Home
Submit
Done
start
5 Windows Explorer
MySQL Command Lin...
Online Voting System ...
Downloads
Adobe Dreamweaver ...
4:39 PM

Online Voting System - Voting Panel

Welcome padmalatha kumar

voter ID : TN/01/0000012

Select candidate name

● XXX

○ YYY

○ ZZZ

○ SSS

4.0. Analysis of the Properties of the Proposed Protocol

In this section, we will verify that the protocol previously proposed satisfies the main indispensable requirements to any electronic vote scheme.

Security Issues: The protocol provides security taking the key size 512 bits. As the key size increased, it is very difficult for the hacker to find out the key to decrypt the encrypted vote during the time of transferring the vote from the voter to tallier. The time to guess the key will be more and the whole process will be over by the time the key is guessed.

Single Transaction/ Efficiency The Transactions in the existing protocol are multiple, as the tallier has to send the receipt to the voter to get the decryption key to decrypt the encrypted votes. In the proposed protocol these functions are carried out in a single transaction, as the tallier does not have to wait for the decryption key from the voter. The advantages of the proposed single transaction voting protocol over the existing protocols are less complexity in implementation and consumption of very less time in the voting process.

Fairness Issues: In our scheme, no one can acquire any information about the tally result before the voting deadline. Before announcing the election outcome, each ballot will be in an encrypted form. Therefore no one can learn or predict the outcome of each vote before the tally announcement.

Eligibility Issues: No one can vote without going through the correct procedure for registration to get the smart card from the electoral officer. Only the smart card holder can eligible to vote.

Uniqueness Issues: No voter is able to vote more than once, by maintaining the status bit information; it prevents the double voting.

Uncoercibility Issues: No voter will be coerced to casting for particular candidate. The only way to coerce voters is to know the content of the ballot sheet, and because there is no receipt, no one can know which candidate voter vote to, so there is no coerce.

Receipt-freeness: Ensures that the voter can be convinced that his/her ballot is counted without getting a receipt. This electronic method minimizes the possibility of bribes and is environmentally friendly by making a paperless process.

5.0. Conclusion

According to the concepts mentioned above, our scheme solves the fairness, eligibility, uniqueness, uncoercibility, efficieny security and privacy issues, and is very suitable for implementation on the internet. Our scheme is more suitable for meeting the voting demands of the future.

References

[1] Postnote: Online Voting. UK Parliamentary Office of Science and Technology, May 2001,Number 155, pp. 1–4. Online:www.parliament.uk/post/pn155.pdf.

[2] Atsushi Fujioka, Tatsuaki Okamoto, and Kazuo Ohta. A practical secret voting scheme for large scale elections. In Advances in Cryptology |AUSCRYPT '92, pp. 244-251, 1992.

[3] W. Juang and C. Lei, "A secure and practical electronic voting scheme for real world environment," IEICE Trans. On Fundamentals, E80-A(1), January 1997.

[4] Kazue Sako. Electronic voting schemes allowing open objection to the tally. In Transactions of IEICE, vol. E77-A No.1, Jan. 1994.

[5] Tatsuaki Okamoto. Receipt-free electronic voting schemes for large scale elections. In Proc. Of Workshop on Security Protocols '97, vol. 1361 of LNCS, pp. 25-35.Springer-Verlag, 1997.

[6] Josh Cohen Benaloh and Dwight Tuinstra. Receipt-free secret-ballot elections (extended abstract). In Proc. 26th ACM Symposium on the Theory of Computing (STOC), pp. 544-553.ACM, 1994.

[7] Ronald Cramer, Matthew K. Franklin, Berry Schoenmakers, and Moti Yung. Multi-authority Secret-ballot elections with linear work. In Advances in Cryptology | EUROCRYPT '96, v ol. 1070 of LNCS, pp.72-83.Springer-Verlag, May 1996.

[8] Ronald Cramer, Rosario Gennaro, and Berry S choenmakers. A secure and optimally efficient multi-authority election scheme. European Transactions on Telecommunications, 8:481-489, 1997. Preliminary version in Advances in Cryptology | EUROCRYPT '97.

[9] Kazue Sako and Joe Kilian. Secure voting using partially compatible homomorphisms. In Advances in Cryptology | CRYPTO '94, vol. 839 of LNCS,pp.411-424. Springer-Verlag, 1994.

[10] Kazue Sako and Joe Kilian. Receipt-free mixtype voting scheme A practical solution to the implementation of a voting booth. In Advances in Cryptology | EUROCRYPT '95, vol. 921 of LNCS, pp. 393{403. Springer-Verlag, 1995.

[11] Markus Jakobsson. A Practical Mix. In Advances in Cryptology | EU-ROCRYPT '98, vol. 1403 of LNCS,pp. 448-461, Springer-Verlag, 1998.

[12] Masayuki Abe. Mix-networks on permutation networks In Advances in Cryptology |ASIACRYPT '99, vol. 1716 of LNCS, pp. 25-273. Springer-Verlag, 1999.