Advances in Internet of Things, **2011, 1, 38-50**
doi:10.4236/ait.2011.12006 Published Online July 2011 (http://www.SciRP.org/journal/ait)

Secured Electronic Voting Protocol Using Biometric Authentication

Kalaichelvi Visvalingam[1], R. M. Chandrasekaran[2]
[1]*SRC-Sastra University, Kumbakonam, India*
[2]*Annamalai University, Annamalai Nagar, Pakistan*
E-mail: kalaichelvi2k@yahoo.com

Received June 16, 2011; *revised July* 5, 2011; *accepted July* 11, 2011

Abstract

This paper proposes a new secure e-voting protocol. This new scheme does not require a special voting channel and communication can occur entirely over the existing 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 as 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. Finally, the proposed protocol is compared with the existing protocols such as Simple, Two Agency, Blind Signatures and sensus protocols.

Keywords: Online Voting, Cryptology, Privacy, Security and Internet

1. Introduction

1.1. The Traditional Voting Process

Traditional voting process that can be divided into four phases.

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 lots 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.

1.2. 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.

1.3. Biometric Authentication

Biometrics are automated methods of identifying a person or verifying the identity of a person based on a physiological or behavioral characteristic. Examples of physiological characteristics include hand or finger images, facial characteristics, and iris recognition. Behavioral characteristics are traits that are learned or acquired. Dynamic signature verification, speaker verification, and keystroke dynamics are examples of behavioral characteristics.

Biometric authentication requires comparing a registered or enrolled biometric sample (biometric template or identifier) against a newly captured biometric sample (for example, a fingerprint captured during a login). During **Enrollment**, a sample of the biometric trait is captured, processed by a computer, and stored for later comparison.

Biometric recognition can be used in **Identification** mode, where the biometric system identifies a person from the entire *enrolled* population by searching a database for a match based solely on the biometric. For example, an entire database can be searched to verify a person has not applied for entitlement benefits under two different names. This is sometimes called "one-to-many" matching. A system can also be used in **Verification** mode, where the biometric system authenticates a person's claimed identity from their previously enrolled pattern. This is also called "one-to-one" matching. In most computer access or network access environments, verification mode would be used. A user enters an account, user name, or inserts a token such as a smart card, but instead of entering a password, a simple touch with a finger or a glance at a camera is enough to authenticate the user.

This recognition method uses the iris of the eye which is the colored area that surrounds the pupil. Iris patterns are thought unique and static one [1].

In electronic voting system, which is 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. In the Online Voting system the paper registration is supplemented by online registration. Manual Signature is replaced by digital signature and blind signature [2-6].

2. Existing Voting Protocols

The voting protocols define how communicating runs between the election authorities and the voter. To fulfill the constraints mentioned in the previous section, many protocols have been developed. It would be impossible to discuss all of them but most used protocols will be discussed in the following subsections.

2.1. Simple Protocol

This protocol is designed without employing any cryptographic techniques. In this voters would submit their vote along with a unique identification number to a validator who would then take their name off on a list of registered voters. Then the validator would then strip off the Unique Identification number and submit just the votes to the tallier who would count the votes.

Although this system has the advantages of being flexible, convenient and mobile, this system is far from secure. If the validator is compromised votes can be easily traced back to the voter or votes could be changed. Both privacy and accuracy lack with this protocol. There is no way to ensure the voter's privacy and the tallier accurately records the votes [7,8].

2.2. Two Agency Protocols

In this two agency protocols, the electronic validator distributes a secret identification tag to each voter just prior to the election. The validator then sends the tallier a list of all identification tags, with no record of the corresponding voters. Each voter sends the tallier his/her identification tag and an encrypted file contacting a copy of the tag and the voted ballot. At this point the tallier can make sure the identification tag is valid, but the program has no way of examining the contents of the ballot. The tallier publishes the encrypted file, and the voter responds by sending the tallier the key necessary to decrypt it. When the election is over, the tallier publishes a list of all voted ballots and the corresponding encrypted files. This protocol also has several problems. Most importantly it doesn't protect the voter's privacy if the tallier and validator collude [7,8].

2.3. Blind Signatures

Blind signatures allow a document to be signed without revealing its contents. The effect is similar to placing a document and a sheet of carbon paper inside of the envelope. If somebody signs the outside of the envelope, they also sign the document on the inside of the envelope. The signature remains attached to the document, even when it is removed from the envelope [2-6].

The voter prepares a voted ballot, encrypts it with a secret key, and blinds it. The voter then signs the ballot and sends it to the validator. The validator verifies that the signature belongs to registered voter who has not yet voted. If the ballot is valid, the validator signs the ballot and returns it to the voter. The voter removes the blinding encryption layer, revealing an encrypted ballot signed by the validator. The voter then sends the resultant encrypted ballot to the tallier. The tallier checks the signature on the encrypted ballot. If the ballot is valid, the tallier places it on a list that is published after all voters vote. After the list has been published, voters verify that their ballots are on the list and send the tallier the decryption keys necessary to open their ballots. The tallier uses these keys to decrypt the ballots and add the votes to the election tally.

2.4. Sensus Polling Protocol

One of the drawbacks of the Blind Signature protocol is the voter has to wait till the voting has ended before the voter can verify the casted vote was the correct one, which is not in line with the property of flexibility. Sensus system is closely based on the Blind Signature protocol. The major difference between the schemes emerges after the voter has submitted the encrypted ballot to the tallier. Instead of waiting till the voting ends the tallier sends a receipt to the voter when his/her ballot has been received. This receipt is no more than a confirmation the vote has been transferred to the tallier correctly. The voter may submit the decryption key immediately after receiving this receipt, completing the entire voting process in one session. The implemented Sensus system employs a pollster agent that performs all cryptographic functions and transactions with the election programs on the voter's behalf. Tests conducted with a prototype implementation of Sensus indicate that the entire voting process can be completed within a few minutes [9,10].

3. Proposed System

Before talking about the proposed electronic voting system (**Figure 1**)we need to define the biometric token (smart card) and the nature of that token and why we use it in our system, and how can it be useful for the voters in election. 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.

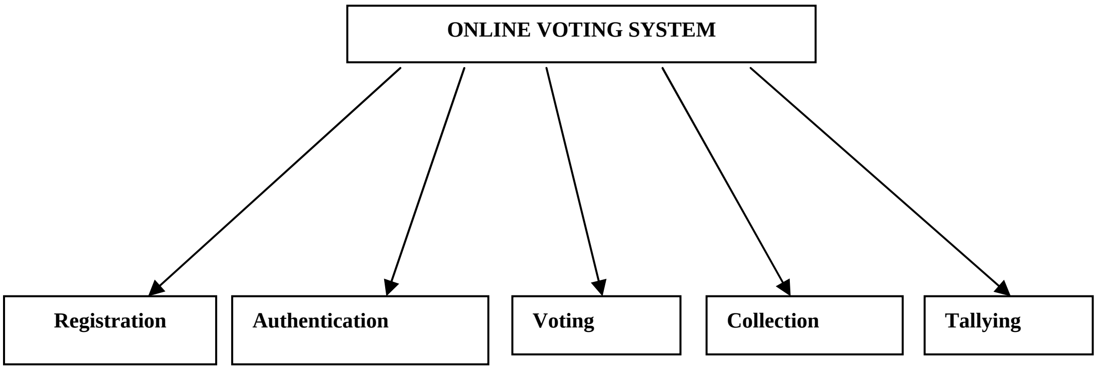
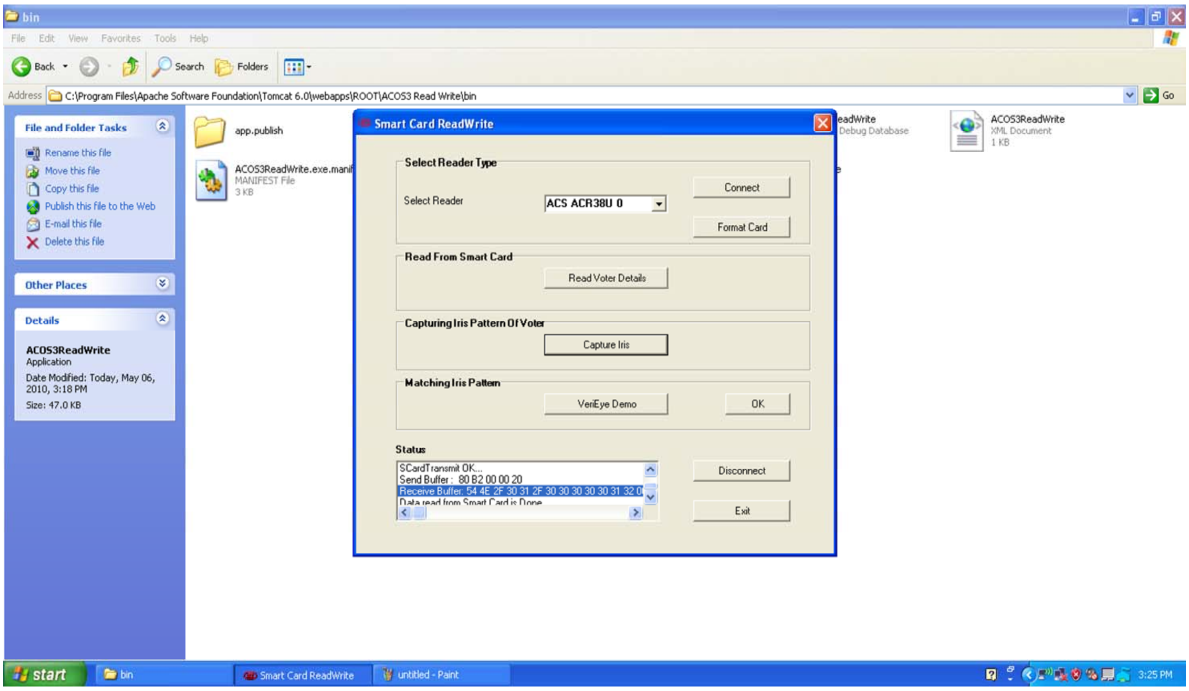


Figure 1. Tasks of Online Voting System.

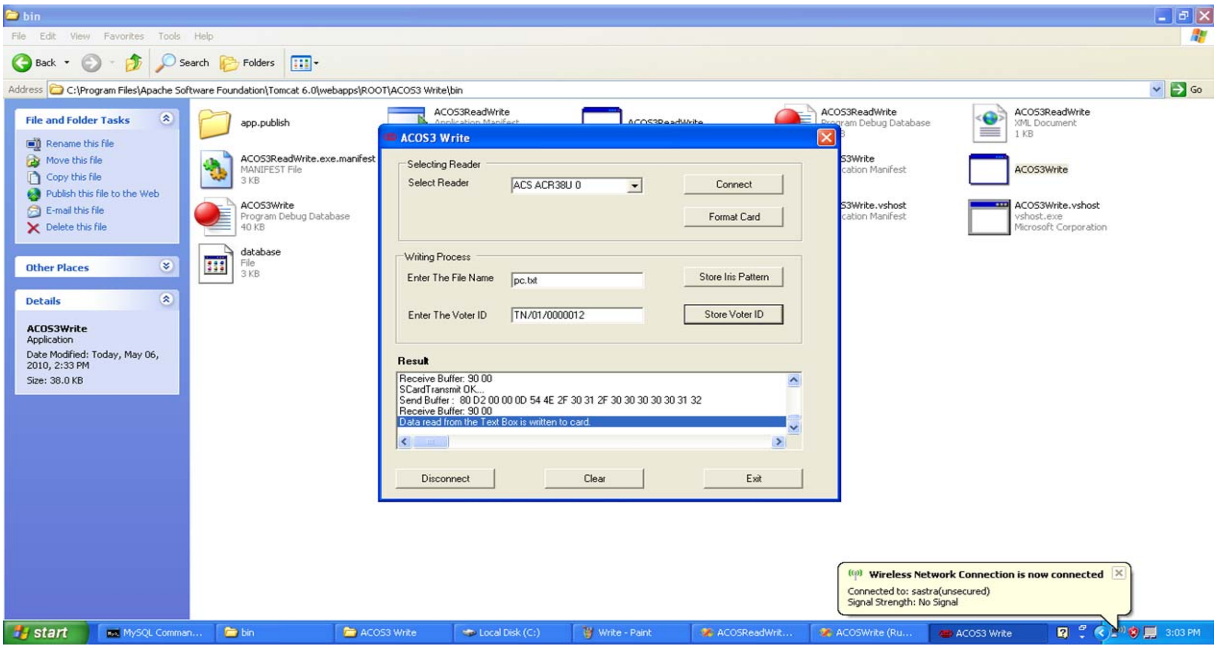


Select Reader: ACS ACR38U 0

Status

```
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
```

Figure 3.1. Smart Card – Reader Form.



Select Reader: ACS ACR38U 0

Enter The File Name: pc.txt

Enter The Voter ID: TN/01/0000012

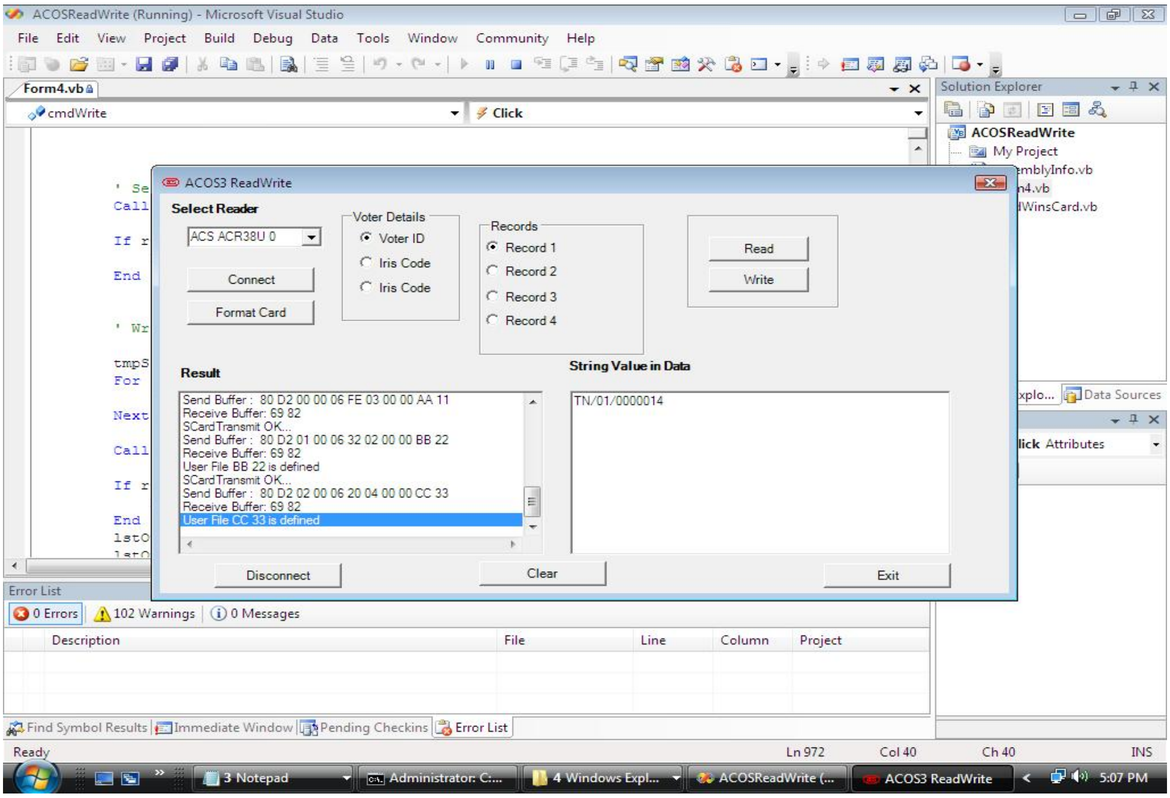
Result

```
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.
```

Figure 3.2. Smart card—Writer Form.

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). Because it is a temporary storage 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



Select Reader: ACS ACR38U 0

Voter Details: ● Voter ID ○ Iris Code ○ Iris Code

Records: ● Record 1 ○ Record 2 ○ Record 3 ○ Record 4

Result

```
Send Buffer :  80 D2 00 00 06 FE 03 00 00 AA 11
Receive Buffer: 69 82
SCardTransmit OK...
Send Buffer :  80 D2 01 00 06 32 02 00 00 BB 22
Receive Buffer: 69 82
User File BB 22 is defined
SCardTransmit OK...
Send Buffer :  80 D2 02 00 06 20 04 00 00 CC 33
Receive Buffer: 69 82
User File CC 33 is defined
```

String Value in Data: TN/01/0000014

0 Errors | 102 Warnings | 0 Messages

	Description	File	Line	Column	Project

Ln 972 Col 40 Ch 40 INS

Figure 3.3. Smart Card Data Storage.

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.

To store data into the smart card the following code is used: (Figures 3.2 and 3.3)

```
' Select User File
        Call SelectFile(HiAddr, LoAddr)
        If retcode <> ModWinsCard.SCARD_S_SUCCESS Then
            Exit Sub
        End If
  ' Write data from text box to card
        tmpStr = txtData.Text
        For indx = 0 To Len(tmpStr) − 1
            tmpArray(indx) = Asc(Mid(tmpStr, indx + 1, 1))
        Next indx
        Call writeRecord(1, rec, dataLen, Len(tmpStr), tmpArray)
        If retcode <> ModWinsCard.SCARD_S_SUCCESS Then
            Exit Sub
        End If
        lstOutput.Items.Add("Data read from Text Box is written to card.")
        lstOutput.SelectedIndex = lstOutput.Items.Count − 1
    End Sub
```

To read data from the smart card the following code is used: (Figure 3.1)

```
' Select User File
        Call SelectFile(HiAddr, LoAddr)
        If retcode <> ModWinsCard.SCARD_S_SUCCESS Then
            Exit Sub
        End If
' Read First Record of User File selected
        Call readRecord(rec, dataLen)
        If retcode <> ModWinsCard.SCARD_S_SUCCESS Then
            Exit Sub
        End If
' Display data read from card to textbox
        tmpStr = ""
        indx = 0
```

```
            While (RecvBuff(indx) <> &H0)
                If indx < txtData.MaxLength Then
                    tmpStr = tmpStr & Chr(RecvBuff
(indx))
                End If
                indx = indx + 1
             End While
```

3.1. Registration

The process of voter registration is always done by Administrator before few days of the election process as follows: 1) Registration phase begins by storing the Voter information such as Unique Voter 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), Name, Age, Sex, Address and District in the database. 2) Obtaining the **Iris pattern** (**Figure 4.8**)of the voter and storing it in the **Smart card**. 3) Testing and issuing of the Smart card to the voter.

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

In this phase, the corresponding public key and private key will be generated automatically using RSA algorithm for each voter. The Key information (**Figure 3.4**) will be maintained by the Administrator securely.

3.2. Authentication

The voter identification (Authentication) is the first step in the process of voting according to this system as follows: 1) Obtaining the iris pattern of voter using an **iris recognition** device on the polling booths. 2) Obtaining the approved iris pattern of the voter from the **smart card** provide through smart card reader. 3) Comparing (**Figure 4.9**) the two patterns to know whether they match or not. (To match the iris patterns, VeriEye technique is used) 4) On matching the voter identification is confirmed and further steps are taken. 5) On mismatch the voter is notified regarding the mismatch and proper enquiry and alternate solutions is done.

Once the voter is authenticated, tallier checks the validity against the database whether the voter can cast vote or not. It extracts the Voter ID (unique id) from the smartcard, using that it compares the status of the voter whether it is 0 or 1. If status = 1, the voter can't cast vote. If status = 0, the voter is allowed to cast vote.

3.3. Voting

Once the voter is authenticated then, the Validator sends the confirmation message to the Tallier to conduct the vote. After this voter is provided with the graphical user interface to cast his/her vote. The various steps involved

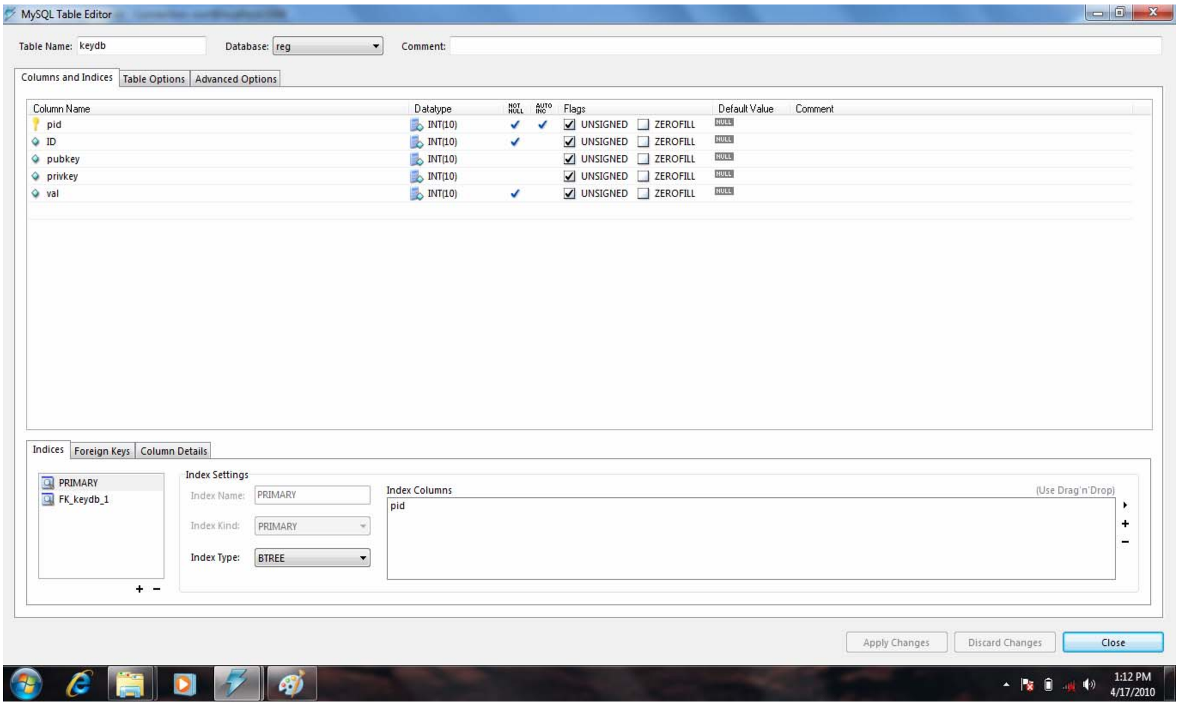


Table Name: keydb
Database: reg
Comment:

Column Name	Datatype	NOT NULL	AUTO INC	Flags	Default Value	Comment
pid	INT(10)	✓	✓	☑ UNSIGNED ☐ ZEROFILL	NULL	
ID	INT(10)	✓		☑ UNSIGNED ☐ ZEROFILL	NULL	
pubkey	INT(10)			☑ UNSIGNED ☐ ZEROFILL	NULL	
privkey	INT(10)			☑ UNSIGNED ☐ ZEROFILL	NULL	
val	INT(10)	✓		☑ UNSIGNED ☐ ZEROFILL	NULL	

PRIMARY
FK_keydb_1

Index Settings
Index Name: PRIMARY
Index Kind: PRIMARY
Index Type: BTREE
Index Columns (Use Drag'n'Drop)
pid

Figure 3.4. Key Generation Database.

are done by Validator as follows,

- Selection of the candidate by the user.
- Asked for confirmation of selection in the form of message box.
- On confirmation the vote is updated to the local database.
- On non confirmation the voter is taken back to the candidates list screen to get the voters selection.

The selection and confirmation of the vote is the user part in this module the connectivity and the updating of the local database which stores the votes are programmed to work in the background of the software.

- If the status is 0 then Tallier provides the voting page to voter to give vote.
- 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 is 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 votes that are casted are stored in the local database of each booth 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.

Cryptography for security:

This protocol adopted with the existing Public key RSA algorithm. 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.

4. Use Case Diagrams

The following diagram depicts the use case specification of different modules (**Figures 4.1-4.5**).

5. 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

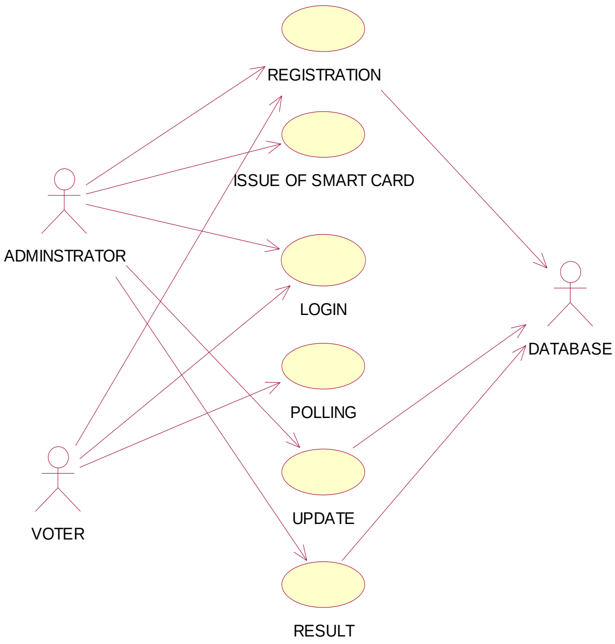


Figure 4.1. Main Use Case Diagram.

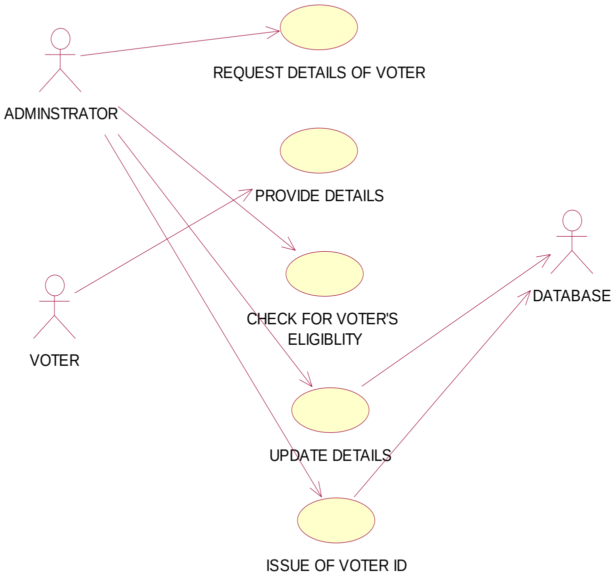


Figure 4.2. Registration Use Case Diagram.

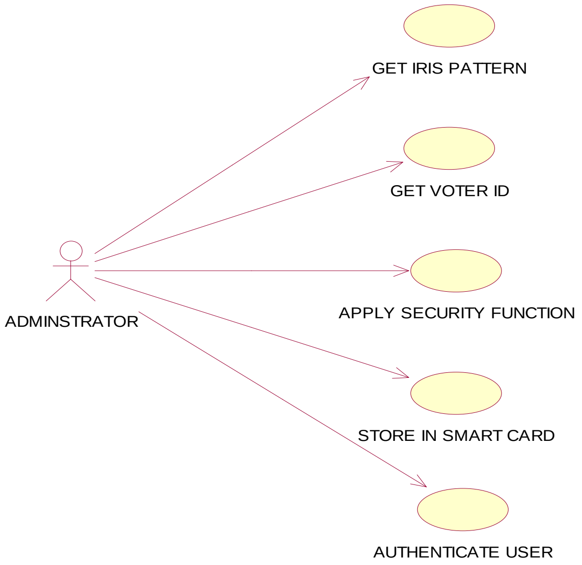


Figure 4.3. Smart Card Use Case Diagram.

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.

6. Comparison of the Existing Voting Protocols and the Proposed Protocol

The Comparison of the existing voting Protocols and the proposed protocol is given in **Figure 6.1**.

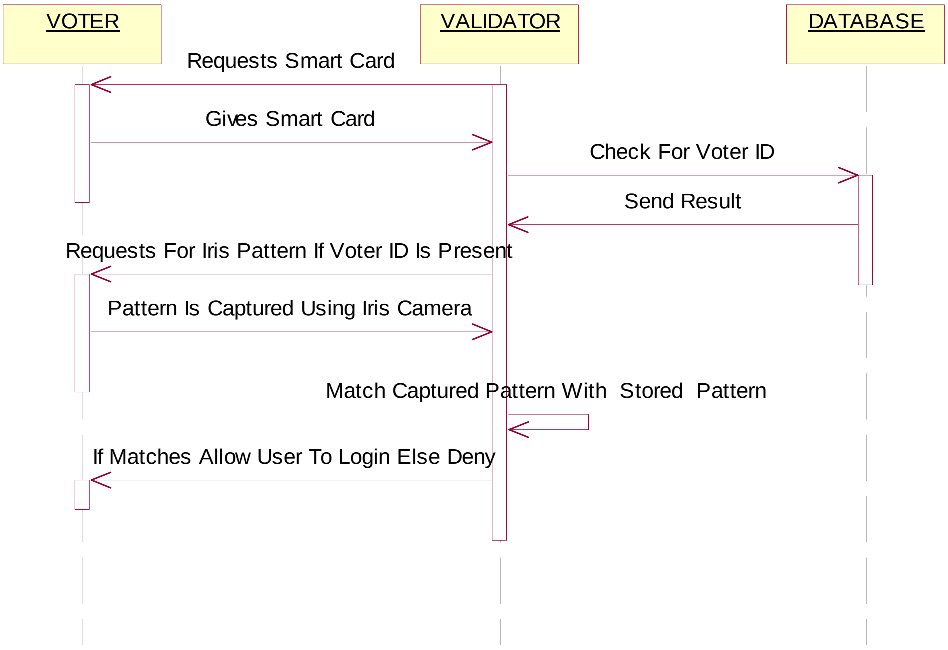

VOTER
VALIDATOR
DATABASE
Requests Smart Card
Gives Smart Card
Check For Voter ID
Send Result
Requests For Iris Pattern If Voter ID Is Present
Pattern Is Captured Using Iris Camera
Match Captured Pattern With Stored Pattern
If Matches Allow User To Login Else Deny

Figure 4.4. Authentication Sequence Diagram.

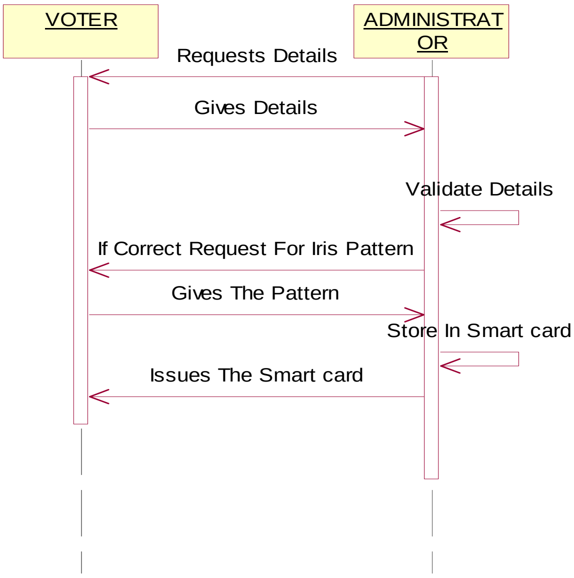


Figure 4.5. Smart Card Sequence Diagrame.

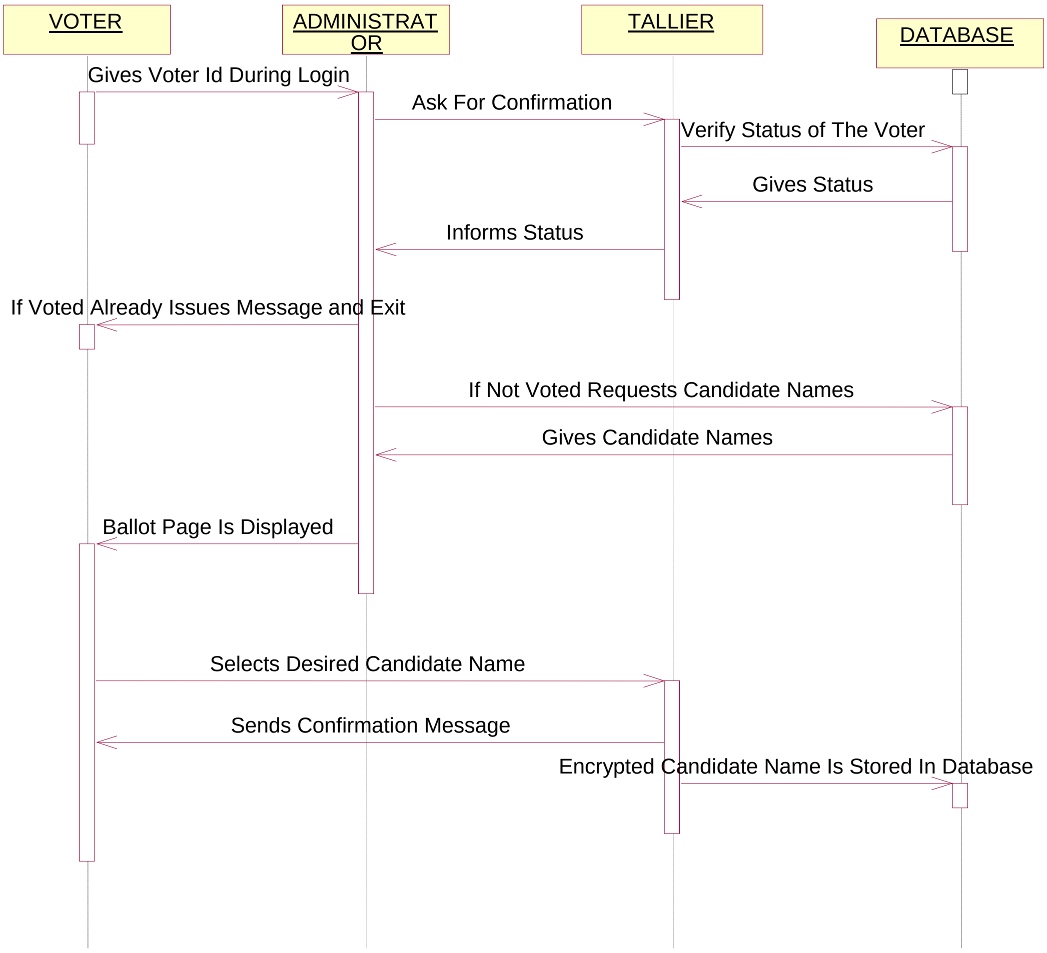
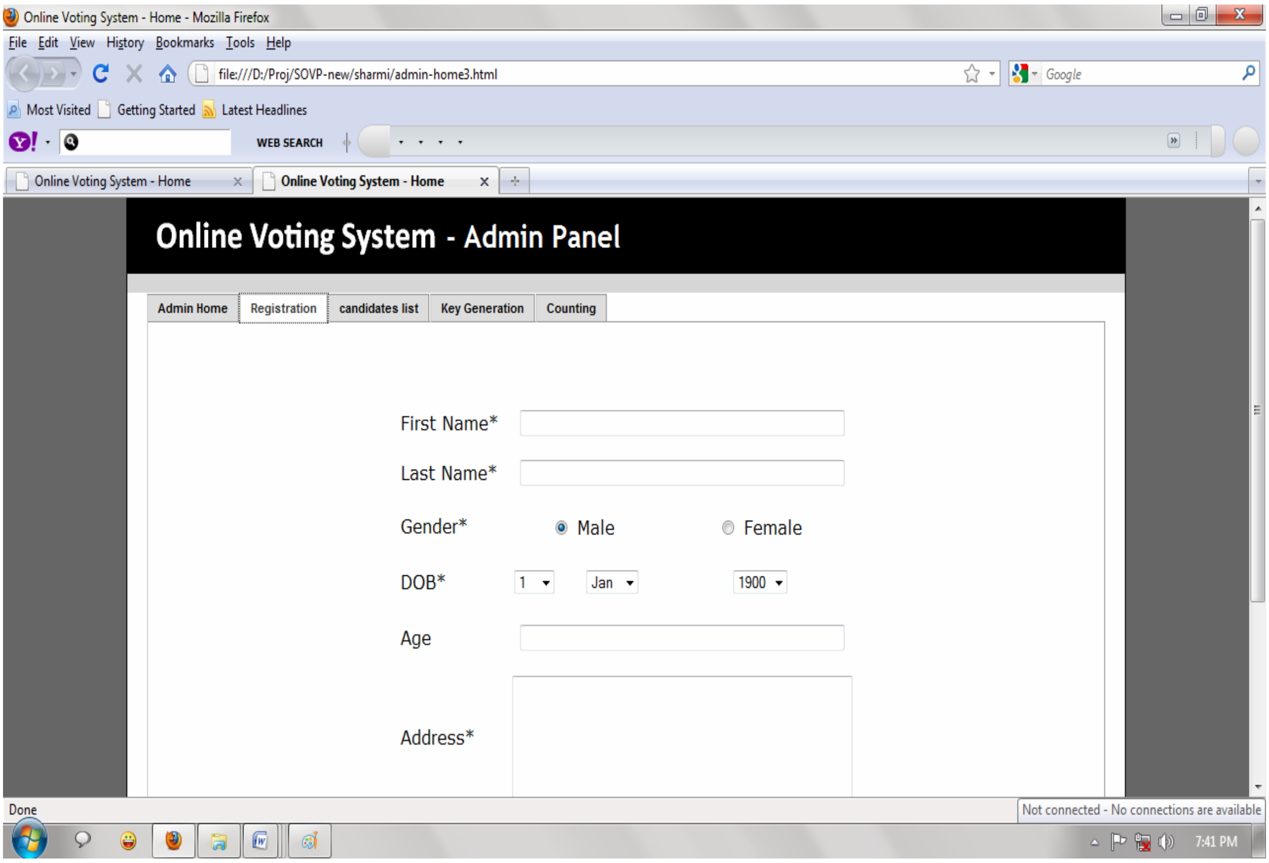

VOTER
ADMINISTRATOR
TALLIER
DATABASE
Gives Voter Id During Login
Ask For Confirmation
Verify Status of The Voter
Gives Status
Informs Status
If Voted Already Issues Message and Exit
If Not Voted Requests Candidate Names
Gives Candidate Names
Ballot Page Is Displayed
Selects Desired Candidate Name
Sends Confirmation Message
Encrypted Candidate Name Is Stored In Database

Figure 4.6. Polling Sequence Diagram.


Online Voting System - Home - Mozilla Firefox
File Edit View History Bookmarks Tools Help
file:///D:/Proj/SOVP-new/sharmi/admin-home3.html
Google
Most Visited Getting Started Latest Headlines
WEB SEARCH
Online Voting System - Home
Online Voting System - Home
Admin Home
Registration
candidates list
Key Generation
Counting
Done
Not connected - No connections are available
7:41 PM

Online Voting System - Admin Panel

First Name*

Last Name*

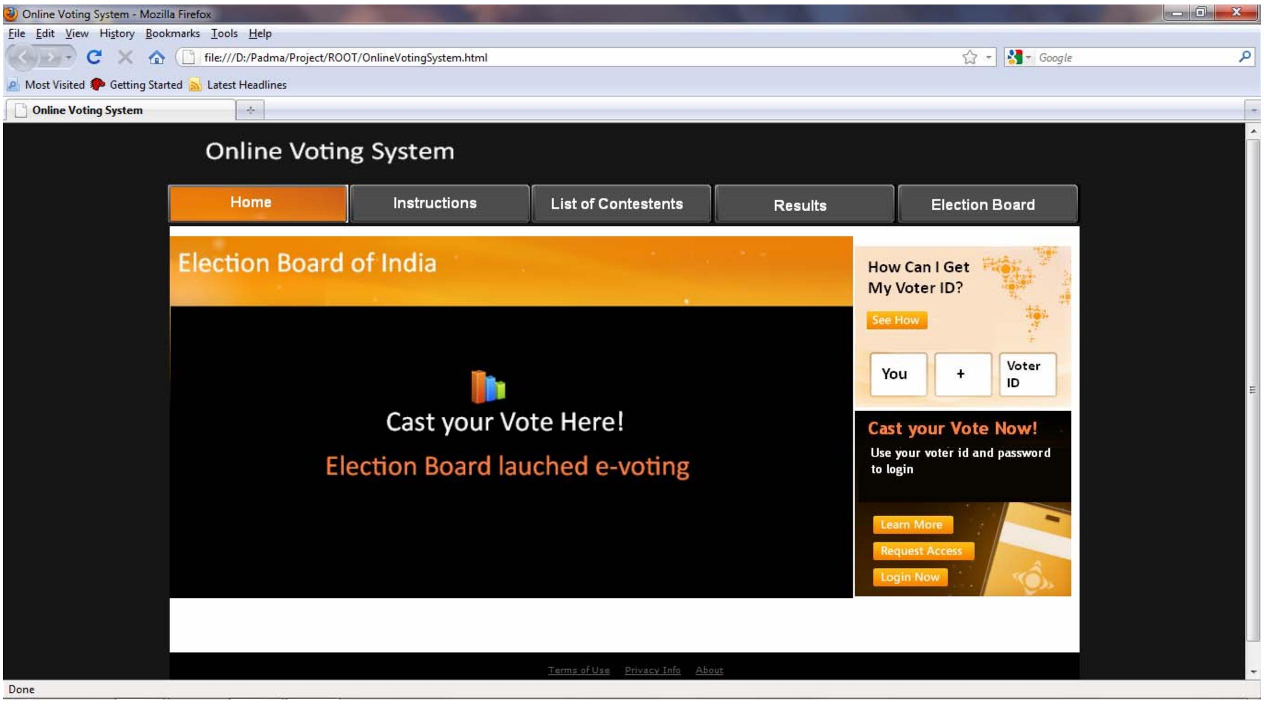
Gender* ● Male ○ Female

DOB* 1 Jan 1900

Age

Address*

Figure 4.7. Admin Panel.


Online Voting System - Mozilla Firefox
File Edit View History Bookmarks Tools Help
file:///D:/Padma/Project/ROOT/OnlineVotingSystem.html
Google
Most Visited Getting Started Latest Headlines
Online Voting System
Home
Instructions
List of Contestents
Results
Election Board
See How
You
+
Voter ID
Learn More
Request Access
Login Now
Terms of Use
Privacy Info
About
Done

Online Voting System

Election Board of India

Cast your Vote Here!

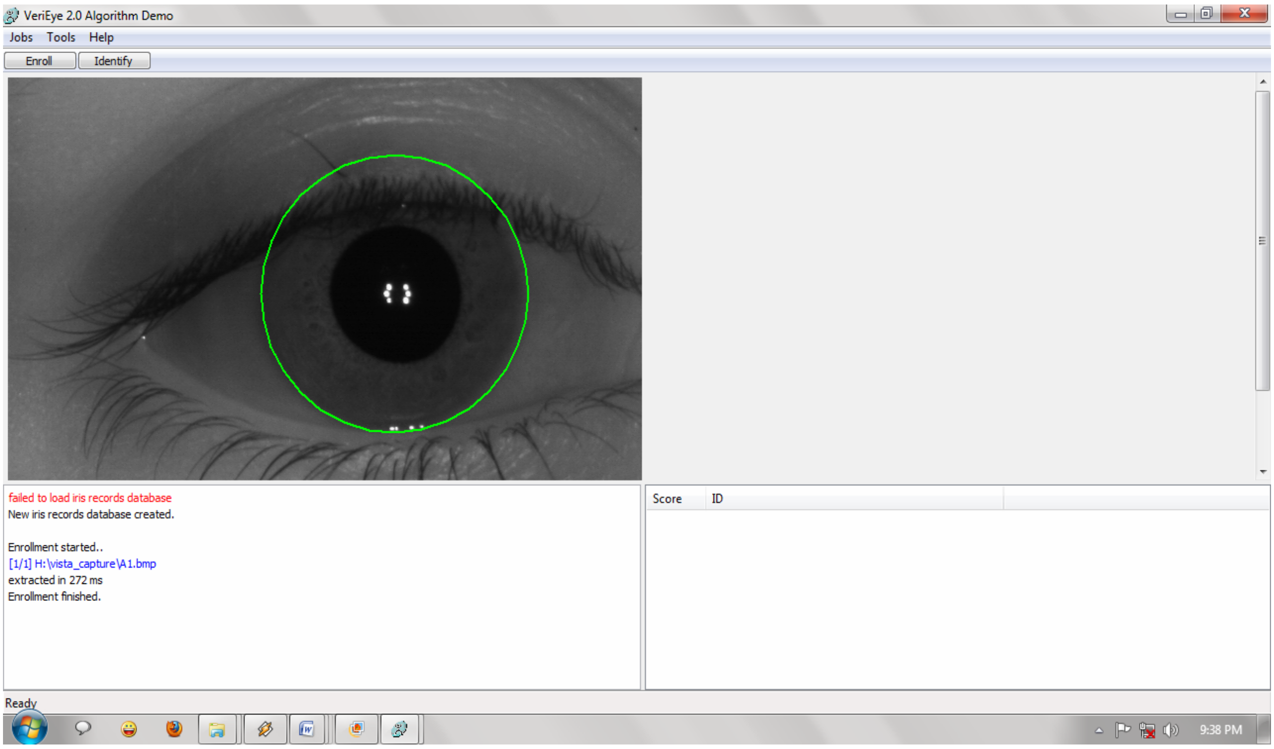
Election Board lauched e-voting

How Can I Get My Voter ID?

Cast your Vote Now!

Use your voter id and password to login

Figure 4.8. Voter Home Panel.

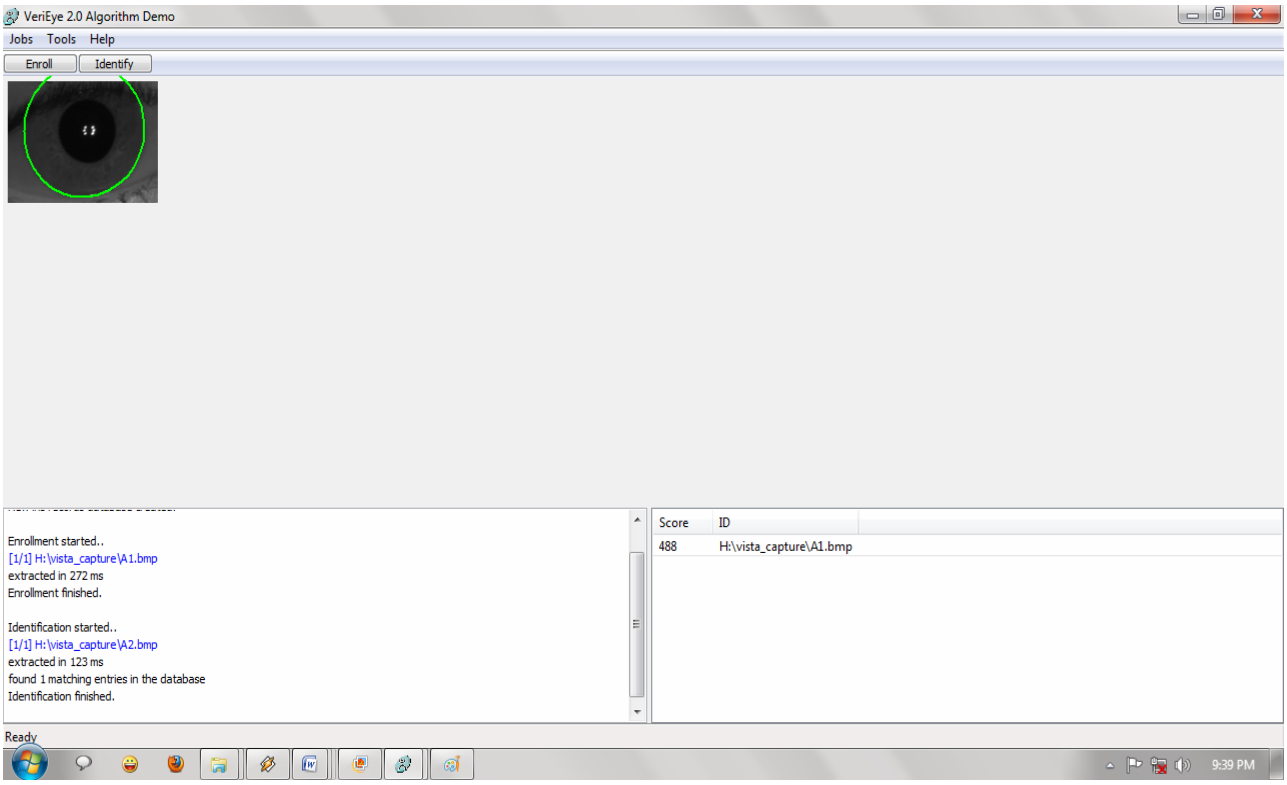


```
failed to load iris records database
New iris records database created.

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

Score	ID

Figure 4.9. VeriEye Enrollment.

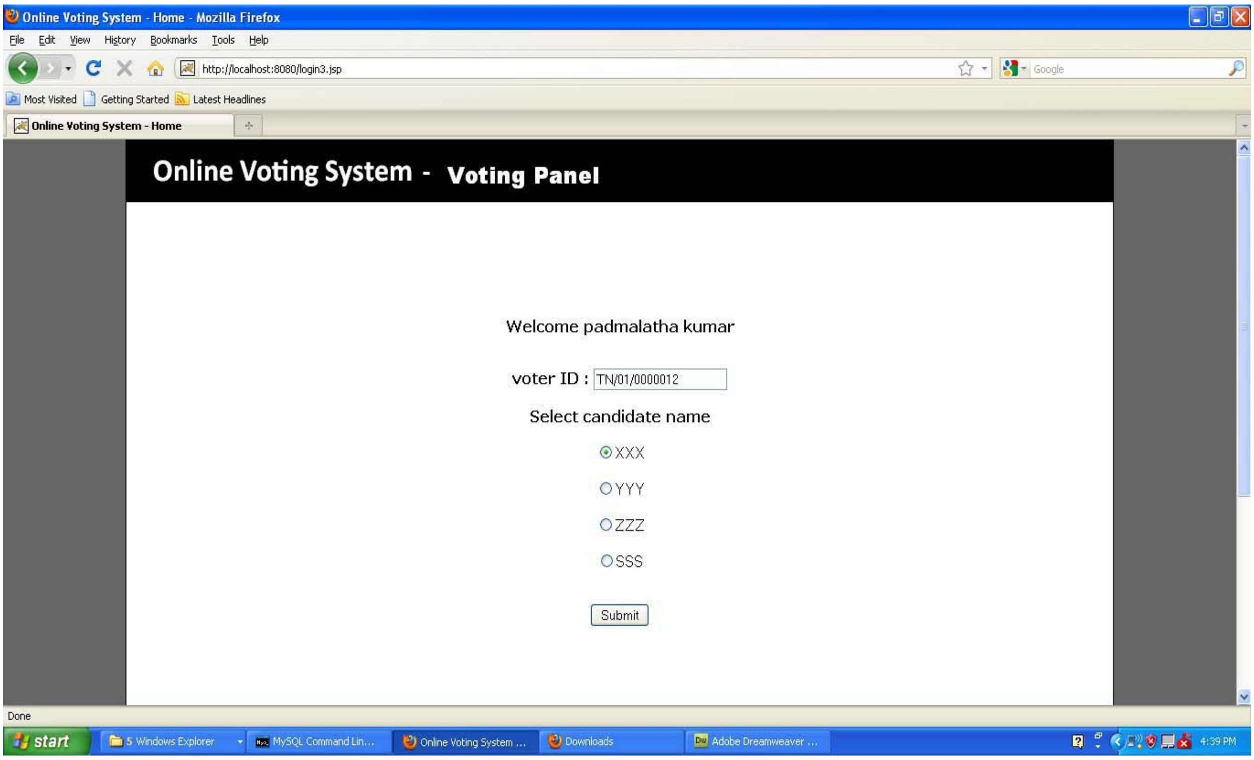


```
Enrollment started..
[1/1] H:\vista_capture\A1.bmp
extracted in 272 ms
Enrollment finished.

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

Figure 4.10. VeriEye Identification.


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
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

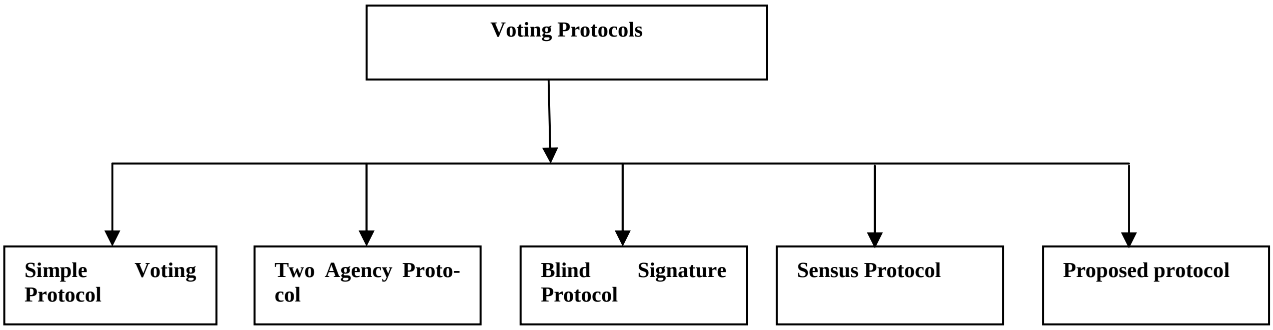
○ YYY

○ ZZZ

○ SSS

Submit

Figure 4.11. Voting Panel.



Disadvantages
Voter’s Privacy is not secured.
The improper update of voting DB is less

Advantages
The improper update of voting DB is less
Tallier can’t cast vote for all voters.
Disadvantages
Voter’s Privacy is not secured
The voting process time is more.

Advantages:
Accuracy property is satisfied
Voter’s Privacy is ensured.
Disadvantages:
The verification process has to wait until the election over.

Advantages:
Accuracy property is satisfied.
Voter’s Privacy is ensured.
The voting process time is less.
Disadvantages:
The verification process has to wait until the election over.

Advantages:
The improper update of voting DB is very less.
Voter’s Privacy is ensured.
The voting and verification processes are completed in a single transaction in very less time.

Figure 6.1. Comparison among different protocols.

7. Conclusions

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

8. Acknowledgement

I am grateful to **SASTRA** University, Thanjavur, Tamilnadu-India for providing the necessary facilities to carry out this work reported in this paper. I sincerely thank the Management for the generous financial support under Innovation Fund.

9. References

[1] Biometric Consortium web site: http://www.biometrics.org

[2] B. Kharchineh and M. Ettelaee, "A New Electronic Voting Protocol Using a New Blind Signature Scheme," 2nd *International Conference on Future Networks*, Darab, 22-24 January 2010, pp. 190-194. doi:10.1109/ICFN.2010.40

[3] S. Mohanty and B. Majhi, "A Secure Multi Authority Electronic Voting Protocol Based on Blind Signature," 2010 *International Conference on Advances in Computer Engineering IEEE*, Bangalore, 20-21 June 2009, pp. 271-273. doi:10.1109/ACE.2010.82

[4] O. Cetinkaya and M. L. Koc "Practical Aspects of DynaVote e-Voting Protocol," *Electronic Journal of e-Government*, Vol. 7, No. 4, 2009, pp. 327-338.

[5] V. M. Patil, "Secure EVS by Using Blind Signature and Cryptography for Voter's Privacy & Authentication," *Journal of Signal and Image Processing*, Vol. 1, No. 1, 2010, pp. 01-06.

[6] F. Baiardi, A. Falleni, R. Granchi, F. Martinelli, M. Petrocchi and A. Vaccarelli, "SEAS, a Secure e-Voting Protocol: Design and Implementation," *Computers & Security*, Vol. 2, No. 8, 2005, pp. 642-652. doi:10.1016/j.cose.2005.07.008

[7] I. Ray and N. Narasimhamurthi, "An Anonymous Electronic Voting Protocol for Voting over the Internet," 3*rd International Workshop on Advanced Issues of E-Commerce and Web-Based Information Systems* (*WECWIS*'01) San Juan, 21-22 June 2002.

[8] M. Pitka, "Electronic Voting Protocol and Their Security," University of Biaystok, Biaystok, 27 May 2009.

[9] L. F. Cranor and R. K. Cytron, "Sensus: A Security-Conscious Electronic Polling System for the Internet," *Proceedins of the Hawaii International Conference on System Sciences*, Hawaii, 7-10 January 1997.

[10] J.-S. Chou, Y. L. Chen and J.-C. Huang, "A Novel Secure Electronic Voting Protocol Based on Bilinear Pairings," 2006.