CHAPTER 8

PROPOSED VOTING PROTOCOL

8.1 INTRODUCTION

Traditional voting system (i.e., Paper based voting system) has many problems which is already discussed in the Introduction chapter. To overcome those problems, the researchers move towards the electronic voting system. Electronic voting is a type of vote which is done through electronic systems. The development of computer networks and the elaboration of the cryptographic techniques facilitate the implementation of electronic voting. Accordingly, the study of security mechanisms in electronic voting elections has received considerable attention in the last two decades.

There are several requirements for the secure e-voting system which is already discussed in Chapter 6. The several requirements can be satisfied partially by cryptographic techniques. Many cryptographers have proposed a secure e-voting system using cryptographic techniques. To achieve it, a lot of voting systems have been designed. While more and more protocols have been developed, the set of security properties that a protocol has to achieve has evolved. However, many cryptography researchers have been studying still to provide the perfect techniques for these requirements. Thus, researchers keep combining existing or created cryptographic primitives to construct efficient electronic voting schemes, with respect to these security requirements.
In the existing electronic voting systems such as Two agency, Blind signature and Sensus voting protocol, asymmetric key cryptosystem is used for achieving confidentiality and authentication. Asymmetric key cryptosystem is slower than the symmetric key cryptosystem which is discussed in chapter 7 [page no.92-99]. In Blind signature and Sensus protocol, the ballot is encrypted using public key of the voter and the signature is generated using secret key based on RSA signing for verification.

Moreover, the existing voting protocols (discussed in Chapter 6) are very difficult to implement and it will be very inconvenient for all the end users (particularly uneducated people). Because the voter should submit the private key value when it is decrypted by the tallier. So, it will be very difficult for the average people to remember the private key value and also to follow it. Because of the above reason, only this thesis proposes a new protocol for secure electronic voting system.

The proposed voting protocol is based on the hybrid cryptosystem which combines the convenience of a public-key cryptosystem with the efficiency of a symmetric-key cryptosystem.

8.2 PROPOSED VOTING PROTOCOL

This protocol consists of five phases is shown in Fig.8.1 and three parties are involved such as Voter, Validator and Tallier.
8.2.1 Setup

During this stage, voting parameters are initialized. They include candidates, voters and authorities’ eligibility criteria, voting procedures, ballot validity rules and counting rules. Eligible candidates register themselves, and the registration and tally authorities are selected in this stage. Afterward, the voting parameters, candidates and authorities are made public such that they can be publicly known and verified.

8.2.2 Registration

The process of voter registration is always done by the electoral officials before few days of the election. In this phase, each eligible voter will be identified by the electoral officials and issue the smart token (smart card) to the eligible voter. The smart card contains Unique ID (UID), Iris Pattern, name, age, sex, and address details. The Unique ID is a 14 digit number (IND/TN/99/0000078) and it will be generated automatically for each registered user. In this IND specifies the Country, TN specifies the State;
next two digit specifies (for example, 99) District and then the last 7 digit is the ID for the corresponding person.

It will be generated and issued by the electoral officials. Once all the above details are stored in the smart token, it will be verified and issued by the electoral officials. This step has to be started and completed before the process of election.

8.2.3 Authentication

In traditional voting, the voter is authenticated himself by showing their voting credentials. The proposed voting system cannot authenticate the person based on IP address or public key. The biometric characteristics that are used in authentication systems are unique for each person. In Electronic voting (online voting), the voter is at a remote location, we cannot be sure that the voter is who she avows to be, unless we use a biometric authentication protocol. Without biometrics, one can sell or be forced to sell her voting credentials to Eve without anybody realizing. It strengthens the security of e-voting and safeguards its transparency.

Biometrics are automated methods of recognizing a person based on a physiological or behavioral characteristics such as face, fingerprint, hand geometry, iris, retina, signature and voice. In the proposed voting protocol, Iris recognition is used for authentication. It is the most reliable biometric authentication method. Moreover iris is stable through the whole life (approximately from the age of one); the physical characteristics of the iris don't change with age. It also provides high accuracy than the other method.

The voter authentication step is the first step in the process of voting. In this case, to increase the security biometric authentication protocol is used. First, the voter should insert the smart token into the Smart Card
Reader. Once the smart token is inserted, the voting software retrieves the 14-digit Unique ID information and checks whether he is already voted or not by checking the status bit. This status bit is used for achieving uniqueness by enabling this bit only when the voter cast his vote. If the status bit is set, the voter will be denied from accessing. If it is not, again the voting software retrieves the iris pattern information from the smart token and it will be compared with the live iris pattern. If it is matched, the voting software will provide the candidate details to cast the vote. Otherwise, the voter is denied. For Iris Comparison, this thesis exploits VeriEye SDK software.

8.2.4 Voting

This step will be started only after successful authentication. Cryptography plays an important role in this voting phase. The Voting software will generate a one-time symmetric key using PRNG process. It will be used for only one time. The Tallier will provide the corresponding candidate details to the Voter. Once the candidate is selected by the voter, it will be transferred in an encrypted form to the Tallier (Equation 8.1-8.2). ie., the ballot is encrypted using the proposed symmetric key cryptosystem (discussed in Chapter 7.4) with one-time secret key. Then, digital envelope is generated by encrypting the one-time secret key using Tallier’s public key (KUT).

\[ \text{[Encrypted Ballot || Digital Envelope || Unique ID]} \rightarrow \text{Tallier} \quad (8.1) \]

ie.,

\[ \text{[(E}_{K_s}(\text{Ballot})] || E_{KUT} [(K_s) || \text{Unique ID}]} \rightarrow \text{Tallier} \quad (8.2) \]
Where

\[ \text{KU}_T \] - Tallier’s Public Key \hspace{1cm} \text{KR}_T \] - Tallier’s Private Key
\[ \text{K}_S \] - Symmetric Secret key

Once the Tallier receives the above information, the Tallier only can decrypt the digital envelope using his private key (\text{KR}_T) to get \text{K}_S. Others cannot. Once he retrieves the key information \text{K}_S, using \text{K}_S the ballot will be decrypted (Shown in Figure 8.2 –Figure 8.5].

**Figure 8.2 Voter Send’s encrypted ballot to Tallier**

**Figure 8.3 Tallier Verifies the Ballot**
Once it is done, the Tallier will send just the confirmation message nothing other than that to the voter. At the same time, the Tallier will send confirmation to the authenticator to set the status bit. The voting count will be incremented for the corresponding candidate in the DB.

In the existing voting protocol, once the vote is casted, the Tallier has to wait until the decryption key is received from the voter. The existing voting protocol is very complex and it will be very difficult for the average user to follow it and it is time consuming process.

But, the proposed protocol uses Hybrid cryptosystem for achieving confidentiality and authentication and integrity. i.e., To encrypt the ballot it uses symmetric key cryptosystem using one-time symmetric key (Ks) and to encrypt the one-time symmetric key it uses public key cryptosystem using Tallier’s public key (KU_T).

8.2.5 Counting and Result Announcement

Once the election time is over, the result will be announced by the Electoral officials.

The following steps illustrate the Proposed Voting Protocol as shown in Figure 8.4.
Figure 8.4 (Continued)

Step 1:
Validator distributes Secret ID Tag (smart token) to the Voter

Validator distributes Secret ID Tag (smart token) to the Voter

Validator
Voters

Step 2:
Voter provides the Smart token

Validator
Voters

Step 3:
Validator checks voters off from the list of registered voters

Validator
Voters

Step 4:
Validator sends the authenticated message to the Tallier

Validator
Tallier

Figure 8.4 (Continued)
Step 5:

Tallier provides the candidate details

Step 6:

Voter sends the Encrypted ballot to the Tallier

Step 7:

Tallier sends confirmation message to the voter & Encrypted ballot stored in DB

Figure 8.4 Steps involved in the Proposed Protocol
<table>
<thead>
<tr>
<th>Voter</th>
<th>Validator</th>
<th>Tallier</th>
<th>DB1</th>
<th>DB2</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Issue Smart Card</td>
<td>2. Voter Details</td>
<td></td>
<td>Registration</td>
<td></td>
</tr>
<tr>
<td>UID,K&lt;sub&gt;U&lt;/sub&gt;, Iris Pattern</td>
<td>UID</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1. Insert Smart card</td>
<td>2. Check Status</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3. If status updated, Deny from access (i.e., Exit)</td>
<td>3. If status not updated, Compare stored iris pattern with Live iris Pattern</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4. Send Authenticated Message to the Voter</td>
<td>4. Send Authenticated Message to the Tallier</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1. View Candidate Details</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2. EK&lt;sub&gt;S&lt;/sub&gt;[Ballot]</td>
<td></td>
<td>EK&lt;sub&gt;U&lt;/sub&gt;[K&lt;sub&gt;s&lt;/sub&gt;]</td>
<td></td>
<td>UID]</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3. Send Confirmation Message to the Voter</td>
<td></td>
<td></td>
<td>Voting</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4. Ballot is decrypted twice by the Tallier</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5. Send Message to update the status</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1. Update Counting DB</td>
<td></td>
<td></td>
<td>Result</td>
<td>Announcement</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2. Result Announcement</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Figure 8.5 Steps involved in the Proposed Protocol
8.3 USE CASE DIAGRAMS

In this section, the generic constitutional requirements will be facilitated as a basis for eliciting the functional user requirements. This elicitation will be based on the Rational Unified Process. The Rational Unified Process is the synthesis of various software development processes. One of its most important characteristics is that it is use-case driven. Each use case refers to system functional requirements (shown in Figure 8.6-Figure 8.11).

- REGISTRATION
- ISSUE OF SMART CARD
- LOGIN
- POLLING
- UPDATE
- RESULT

Figure 8.6 Use cases for Proposed Voting Model
Figure 8.7 Use case for Registration

Figure 8.8 Use case for Smart Card
Figure 8.9 Sequence Diagram for Smart Card

Figure 8.10 Sequence Diagram for Authentication
8.4 EXPERIMENTAL RESULTS

The outputs of few screens are shown in Figure 8.12-Figure 8.20.
Figure 8.12 Registration Panel  Figure 8.13 Candidate List Panel

Figure 8.14 Voter Home Panel
Figure 8.15 VeriEye Enrollment

Figure 8.16 VeriEye Identification
Figure 8.17 Voting Panel
Figure 8.18 Voter Casting Candidate List Panel
Figure 8.19 Voter Help_Panel
8.5 ANALYSIS AND DISCUSSIONS

8.5.1 Analysis of the Properties of the Proposed Protocol

This section discusses about how the proposed protocol satisfies all the voting requirements such as accuracy, uniqueness, efficiency, security, privacy, authentication, eligibility, fairness, verifiability, anonymity and uncoercibility.

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, others cannot.
**Security Issues:** It is very difficult for the hacker to find out the symmetric key (secret key) to decrypt the encrypted vote during the time of transferring the vote from the voter to Tallier. The digital envelope can be decrypted only by the Tallier because he is only having the corresponding private key (KR_T). Others cannot open that message.

To get the secret key value, the digital envelope should be opened first. This can be done only by tallier, others cannot. Then only the ballot can be decrypted using that secret key.

**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.

Moreover, this proposed protocol is based on the hybrid cryptosystem. That is, it uses the new high speed symmetric key cryptosystem to encrypt the ballot and it also uses asymmetric key cryptosystem only for sharing the secret key value.

But, the existing protocols are based on the asymmetric key cryptosystem. These protocols are very complex and slower in speed. It will be very difficult for the average people to follow it.

**Fairness Issues:** In our scheme, no one can acquire any information about the tally result before the voting deadline. Because the counting DB will be maintained only by the Tallier. Therefore no one can learn or predict the outcome of each vote before the tally announcement.
**Uniqueness Issues:** No voter is able to vote more than once, by maintaining the status bit information; it prevents the double voting. Whenever vote is casted by the voter, the status bit will be updated for the corresponding person.

**Privacy and Fairness:** This scheme achieves privacy and fairness issues because no one can acquire any information about the tally result before the voting deadline. Because the tally DB will be maintained securely by tallier (electoral officials). Therefore no one can learn or predict the outcome of each vote before the tally announcement.

**Anonymity Issues:** In the existing protocol, to guarantee verifiability, the voter’s encrypted vote will be sent to the voter with the key value to decrypt that vote. By decrypting that vote, the voter can verify that the voter’s vote has been counted correctly. If it is verified by the voter, it violates the anonymity and Uncoercibility property.

So, this protocol advocate those voters not be allowed to verify their votes by themselves. It is not necessary to allow voter to verify (or show to bribers) their votes in the announcement phase.

**Uncoercibility Issues:** No voter will be coerced to casting for particular candidate. Because there is no receipt, no one can know which candidate voter vote to, so there is no coerce.

Since the voter is at a remote location, we cannot be sure that the voter is who she avows to be, unless we use a biometric authentication protocol. Even with the use of biometrics to authenticate, both eligible person and Eve (political person) sit in front of the same system (reserved for election) doing the authentication and Eve voting or monitoring the votes, as he wants. If voter wants to sell her vote, and Eve is not present, she can take a
picture of his voting and give it to Eve as proof. In any case, the remoteness of the voter makes the abolition of the sale of votes impossible to fulfill for online voting. Because of this reason, this proposed protocol partially achieves uncoercibility property.

**Receipt-freeness:** Ensures that the voter can be convinced that his/her ballot is counted without getting a receipt. That is, it just sends the confirmation message to the voter nothing other than that during the voting phase. This electronic method minimizes the possibility of bribes and is environmentally friendly by making a paperless process. Because of this reason, the proposed protocol partially achieves verifiability property.

### 8.5.2 Types of possible attacks

All Computer based systems have to be protected from external threats that attack the normal functioning of the system. The threats selected are Masquerade, Denial of Service (DoS) and Viruses.

**Masquerade:** Even with the use of biometrics to authenticate, both eligible person and Eve (eavesdropper) sit in front of the same system (reserved for election) doing the authentication and Eve voting or monitoring the votes, as he wants. So, the eavesdropper can act like a original user here.

If the voter wants to sell her vote, and Eve is not present, she can take a visual rendering of his voting and give it to Eve as evidence. In any case, the remoteness of the voter makes the eradication of the sale of votes impossible to fulfill for online voting.

**Denial of Service (DoS):** When DoS is executed the communication between the client and server is interrupted by flooding the target with more requests that it can handle. In the case of remote electronic voting the availability of
the internet service is vital, and reactivation of the tune-up can take hours once it has been congested.

**Viruses:** Viruses are the computer codes that recursively replicates a possibly evolved copy of itself causing malicious effects in the machines when they are activated. They are downloaded without the knowledge of the end user, during a program download from websites. Once the virus has been downloaded it can infect a host file or system area or simply modify reference to objects to take control and then multiply to form new generations of the virus.

### 8.6 COMPARISON

In the proposed voting protocol, one time secret key is generated using PRNG process using the seed value. It will be used for only one time. The ballot is encrypted using proposed symmetric key cryptosystem (discussed in Chapter 7.4) using this one time secret key. Then, digital envelope is generated by encrypting the one time secret key using Tallier’s public key ($KU_T$). So, the Tallier only can decrypt the digital envelope using his private key others cannot. In this way, the proposed voting protocol achieves authentication. Once the one time secret key is retrieved from the digital envelope, the ballot is decrypted immediately by the Tallier using that key without getting decryption key from the voter and then the counting DB is updated for the corresponding candidates.

It uses asymmetric key cryptosystem (RSA algorithm) for sharing the key value alone. It achieves confidentiality using the proposed high-speed symmetric key cryptosystem and this algorithm is compared with the existing symmetric key algorithm (discussed in chapter 7.5).
The Table 8.1 presents the comparison of the various protocols and Figure 8.21 presents the performance comparison of various protocols.

**Table 8.1 Comparison of the Various Protocols**

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Eligibility</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Accuracy</td>
<td>No</td>
<td>Medium</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Fairness</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Efficiency</td>
<td>No</td>
<td>No</td>
<td>Medium</td>
<td>Yes</td>
<td>High</td>
</tr>
<tr>
<td>Privacy</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Security</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Uniqueness</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Authentication</td>
<td>No</td>
<td>Medium</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Verifiability</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Medium</td>
</tr>
<tr>
<td>Anonymity</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Uncoercibility</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Low</td>
</tr>
</tbody>
</table>

The existing voting protocols were compared with the proposed protocol. From the results, it is easy to understand that the proposed protocol achieves better performance.
This chapter discussed about the Proposed Voting protocol in detail. It also discussed about how the proposed protocol achieves the various voting requirements/properties in detail. Finally, the proposed protocol is compared with the existing voting protocols. It also depicts the use case specification of each functional requirement.