Ishtiaque Mahmud, Shamim Ahmed, A.K.M Nazmus Sakib, Quazi Emanual Alendey, Israt Jahan / International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622
www.ijera.com Vol. 2, Issue 3, May-Jun 2012, pp.2938-2943

# E-Voting Security Protocol: Analysis & Solution

**Ishtiaque Mahmud*, Shamim Ahmed**, A.K.M Nazmus Sakib***, Quazi Emanual Alendey****, Israt Jahan*****

*(Completed M.Sc. and B.Sc. in Computer Science and Engineering from Jahangirnagar University (JU), Dhaka, Bangladesh)

**(Completed B.Sc. in Computer Science and Engineering from Dhaka University of Engineering and Technology (DUET), Gazipur, Bangladesh)

***(Completed B.Sc. major in Computer Science and Engineering from Chittagong University of Engineering & Technology (CUET), Chittagong, Bangladesh)

****(Completed B.Sc. in Computer Science & Engineering from Jahangirnagar University, Dhaka, Bangladesh.)

*****(Completed her B.Sc. and M.Sc. in Electrical and Electronic Engineering from Bangladesh University of Engineering and Technology in 1997 and 2001 respectively. Later she achieved PhD degree from the Department of Computer Science and Engineering, Jahangirnagar University, Savar, Dhaka, Bangladesh in 2009. Now she is serving as an associate professor at the same department)

## ABSTRACT

**This paper describes an on-line e-voting system security implementation to reduce attacks. E-voting is gaining popularity in applications that require high security. E-voting is the electronically voting process via Internet. The system represents security analysis against large-scale attacks performed by rationally thinking attackers. Electronic Voting promises a lot of advantages: It is not only fast and very convenient to use, but it also features additional security properties that cannot be achieved with traditional voting, such as individual or universal verifiability. However, due to the sensitive and critical nature of voting protocols, it is crucial to formally guarantee their correctness with respect to certain intended security properties. We develop a model for describing the real life environment where voting takes place and analyze the behavior of rational adversaries. This paper tries to reduce these large-scale attacks that will help student as well as researchers to realize the e-voting and its security system. The system also eliminates the voting process of non-eligible voters. The security of our e-voting model is more developed than Secure Electronic Registration and Voting Experiment (SERVE) and the recent e-voting systems.**

*Keywords* - **Attacks Tree, Electronic voting, Large-Scale Attacks, Security, Secure Electronic Registration and Voting Experiment**.

## I. INTRODUCTION

Electronic commerce is a part of everyday life. The construction of electronic voting system is one of the most challenging security-critical tasks, because of the need for finding a trade-off between many seemingly contradictory security requirements like privacy vs. auditability. Thereby it is difficult to adopt ordinary mechanisms of e-commerce. For example, in e-commerce there is always a possibility to dispute about the content of transactions. Buyers get receipts to prove their participation in transaction. E-voters, in turn, must not get any receipts, because this would enable voters to sell their votes. In the United States of America, there were many attempts made to use electronic voting systems. The project named Voting over the Internet (VOI) was one of them. VOI was used in the general elections of 2000 in four states (Florida, South Carolina, Texas and Utah). VOI experiment was so small that it was not a likely target of attacks [1, 2, 3]. In January 2004, a group of American Security experts revealed the security report of Secure Electronic Registration and Voting Experiment (SERVE) [4, 5, 6, 7]. The SERVE system was panned for deployment in the 2004 primary and general electrons and allowed eligible voters to vote electronically via Internet [8, 9, 10, 11]. But the SERVE system and the recent e-voting systems have vulnerabilities in the system design, which makes possible to perform voting specific attacks [12, 13, 14, 15]. To solve this problem we developed e-voting model.

## II. CONCEPT OF E-VOTING

### 2.1. E-voting terms

The following terms are considered for e-voting system

- ***Electronic voting (e-voting)*:** E-voting is a voting method where the voter intention is expressed or collected by electronic means.
- ***Kiosk voting*:** Kiosk voting use of dedicate voting machines in polling stations or other controlled location. Voters mark their choice electronically rather than on paper ballot and voters are counted on individual machines, known as Direct Recording Electronic (DRE) machine.
- ***Remote electronic voting*:** Remote electronic voting is the preferred term for voting that takes place by electronic means from any location.
- ***.Internet voting (i-voting)*:** Internet voting is a specific case of remote electronic voting, whereby the vote takes place over the Internet such as via a web site or voting applet. Sometimes it also used synonymously with Remote Electronic voting.

### 2.2. Properties of E-voting System

Elections allow the populace to choose their representatives and express their preferences for how they will be governed. Naturally, the integrity of the election process is fundamental to the integrity of democracy itself. The election system must be sufficiently robust to withstand a variety of fraudulent behaviors and must be sufficiently transparent and comprehensible that voters and candidates can accept the results of an election. Unsurprisingly, history is littered with examples of elections being manipulated in order to influence their outcome. The design of a "good" voting system, whether electronic or using traditional paper ballots or mechanical devices must satisfy a number of following criteria.

- Eligible voters are capable to cast ballot that participate in the final tally.
- Non-eligible voters are disfranchised.
- Eligible voters are not capable to cast two ballots that both participate in the computation of the final tally.
- Votes are secret.
- It is possible for auditors to check whether all correct cast ballots participated in the computation of final tally.
- The result of an election must be secret until the end of the election.
- All valid voters are counted correctly and the system outputs the finally tally.
- It must be possible to repeat the computation of the final tally.

### 2.3. Description of E-Voting System

- ***The voters' managing:*** Is a phase in which votes are managed, stored and prepared for counting.
- ***The voters' registration:*** Is the phase to defined voters for the e-voting system and gives them authentication data to log into the e-voting system.
- ***The authentication:*** Is a phase to verify that the voters have access rights and franchise.
- ***The voting and vote's saving:*** Is a phase where eligible voters cast votes and e-voting system saves the received votes from voters.
- ***The voters' managing:*** Is a phase in which votes are managed, stored and prepared for counting.
- ***The voters' counting***: Is the phase to decrypt and count the votes and output the final tally.
- ***The auditing:*** Is a phase to check that eligible voters were capable to vote and their votes participate in the computation of final tally.

It is possible to divide the e- voting system into three main components of infrastructure.

- ***Voter application*:** Voter application is a web application or an application in voter's personal computers for casting votes. It connects to network server. Usually, encryption and authentication methods secure the communication between these components.
- ***Network server*:** Network server is an online server that provides voters a necessary interface for casting votes. It connects to Back-office server and transfers the received votes.
- ***Back-office* server:** Back-office is consists of server to save and maintain votes and count a final tally.

### 2.4. E-voting attacks and security analysis

There are following e-voting specific attacks.

- *Large-scale vote: Theft* the aim of the attack is to change votes or give more votes for favorite candidates. Another threat is that voters are able to cast more than one vote, so that all votes are accepted final tally.

*Security properties*:

- Non-eligible voters are disfranchised.
- Eligible voters are not able to cast two ballots that both participate in the computation of the final tally.
- *Large-scale disfranchisement votes:* It means that a large number of correctly encrypted ballots from eligible voters never reach Back-office. Attacks could also selectively disfranchise eligible votes. The aim of disfranchisement of votes is to eliminate undesirable votes.

*Security properties:*

- Eligible voters are able to cast ballots that participate in the computation of the final tally.
- *Large-scale votes' buying and selling:* It means that a large number of votes are sold. The aim of this attack is to increase the amount of votes for certain supported candidates.

*Security properties:*

- Voters are secret
- *Large-scale privacy violation:* One of the main rights is voter's privacy. The aim of the attacks is to reveal how voters have voted.

*Security properties:*

- Voters are secret

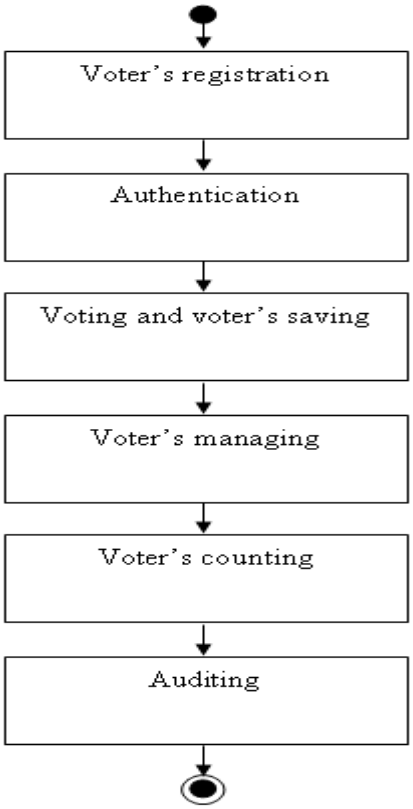


**Fig.1:** Phases of e-voting system

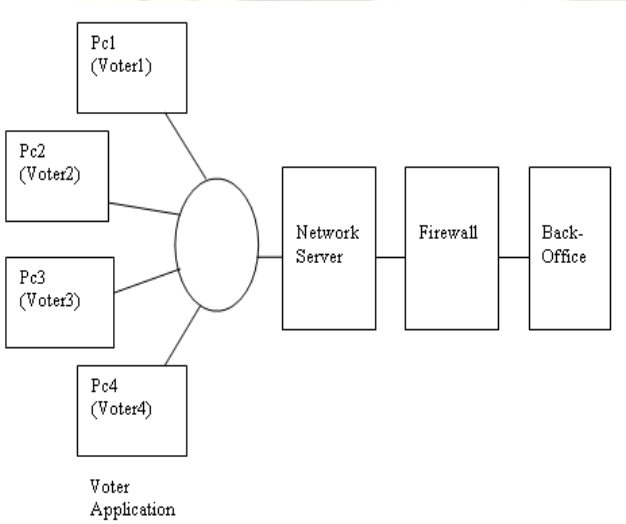


**Fig.2:** Components of e-voting system

We analyze adversarial behavior by using attack tree method. Attacks tress provides a formal method of describing the security of systems, based on varying attacks. Fig. 3 depicts the example of attack tree. Basically attack tress represents attacks against a system structure. The root node represented the goal of attack and sub node represents different ways how to achieve the goal. Nodes are divided into child nodes and parent nodes. There are two types of conditions: AND and OR. They represent logical operations. To satisfy the condition of an OR node, it is sufficient to satisfy at least one of his child nodes. The node of the AND condition is true if every child node is satisfied. When the condition root node is satisfied, the attack is complete.

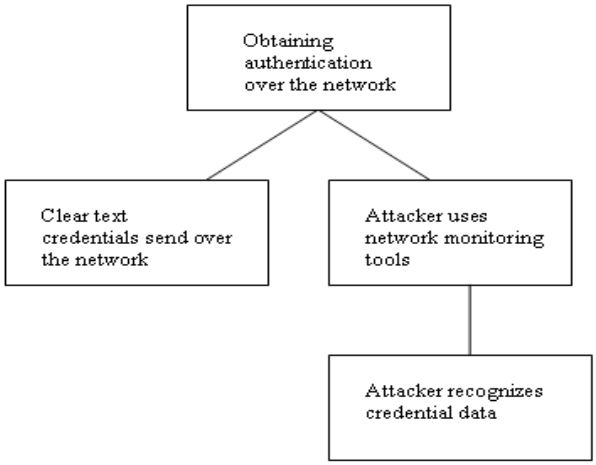


**Fig.3:** Attack tree

## III. DESCRIPTION OF PROPOSED MODEL

For constructing the models of our system we focus on five components:

- Voters Application.
- Network Server.

- Voting Storing Server
- Voting Counting Server
- Back-office Server

Voters Applications of our proposed system send a request to Network Server for establishing a secure connection. Voter Application receives the certificate of network server, if he is an eligible voter. Voters enter the name and password decides whether to verify the signature on the server message component. The certificate is signed with the private key of Back-office.Then the signature is verified by the voter application with the help of public key of Back-office. In our system the Voter Application creates a vote and encrypts the ballot by using the public key of Back-office. Finally, our system accepts the received ballots then Voters Application receives a confirmation response, which confirms that voter's vote reached to Voting Storing Server. Then the vote is counted with the help of time stamping by the Votes Counting Server.

**Table 1:** The function of the proposed model.

| Authentication | process for authentication |
|---|---|
| Enc | function for encryption |
| Dec | function for decrypting ballot |
| Sign | function for digitally signing encrypted ballots |
| Cast | process to cast a vote |
| PK | the public key of e-voting system |
| SK | the secret key of the e-voting system |
| Count | function for counting the final tally |

From Table 1 we can get different functuion of proposed model.

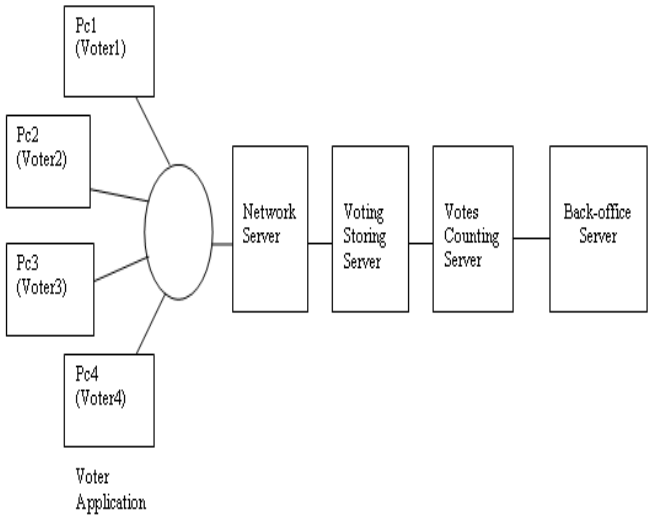


**Fig.4:** E-voting components of proposed model.

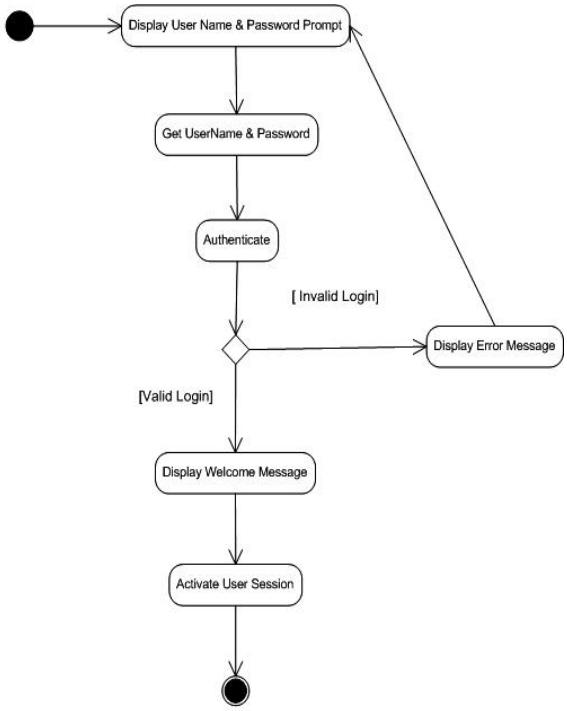


**Fig.5:** The process of log in Voter Application of proposed model

## IV. SECURITY ANALYSIS OF PROPOSED MODEL

The attacker considers with the probability p to succeed the attack and to get gains from the attack. After the attack, it is possible that the attacker will be detected and will be caught. Hence, the rational attacker estimates this probability and penalties so that an outcome ratio will be – Costs + Gains – Penalties.

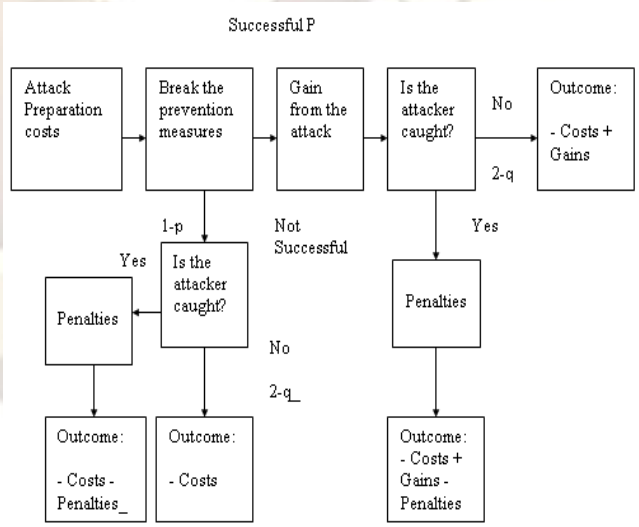


**Fig.6:** Diagram of the attacks

Considering all these parameters, attacker calculates the excepted outcome of the attack. To overcome the attack we can derive an equation which reduces the attack.

The parameters are:

Gains-The gains of the attacker, when the attack succeeds;

Costs- The cost of the attack;

p- The success probability of the attack;

q- The probability of getting caught (if the attack was successful);

q_-The probability of getting caught (if the attack was not successful);

Penalties-The penalties when the attacker are caught (if the attack was not successful);

The value of cost does not affect attacker's final decision to attack an e-voting system or not. Therefore, we may even assume Costs=0. If an e-voting system is secure when Costs=0 or Costs>0. Costs do not affect the attacker's final decision. In our security analysis we may consider attacks is not possible if Outcome=1 and the attacker the attack is successful if Outcome>1.

We can justify the security of our proposed model. Then we calculate the value of outcome.

Outcome = -Costs + Gains. (p. (2-q)- (1-p). q_) (1)

If voters vote more than once, in the case when 10 voters among 100 eligible voters vote twice the probability to succeed voting is $p=0.99^{10}$ .The probability of getting caught is $q=q\_=1-0.99^{10} = 0.096$.

Here, $p=0.99^{10}$

$q=0.9$

$q\_=0.096$

Putting the value in equation (1) the outcome is following:

Outcome = -Costs + Gains. (p. (2-q)- (1-p). q_)

= -Costs + Gains. ($0.99^{10}$ . (2-0.9)- (1-$0.99^{10}$) . 0.096)

= - Costs + Gains . (0.995-0.009)

= - Costs + Gains . (0.99)

= 0.99

≈ 1

In our proposed model attack is not be successful because outcome equal to 1 (Outcome=1). If Outcome>1 may happen multi-parameter attack, like Man in the Middle Attack for logging voters encrypted ballot. If an adversary knows secret in voters ballots, then he able to create all possible encrypted ballots per vote and deduced how voter voted. To reduce this attack we develop an algorithm.

## V. Result of Proposed Model

Algorithm for our proposed model is following:

### 5.1. Algorithm

Step1. Initialize number of ballot paper.

Step2. Find any attack then calculate time stamping.

Step3. If current attack is occur when the time of voter 1st vote is grater or equal 2nd vote (1st vote time≥2nd vote time) then go to step 4, else go to step 5.

Step4. If the time of voter 1st vote is less than 2nd vote (1st vote time<2nd vote time) then attack is reduce. Otherwise go to step 2.

Step5. If all attacks are reduced (Outcome=1) then exit; else go to step *4.*

Fig. 7 shows the result of the proposed model, outcome is equal to 1 (Outcome=1).

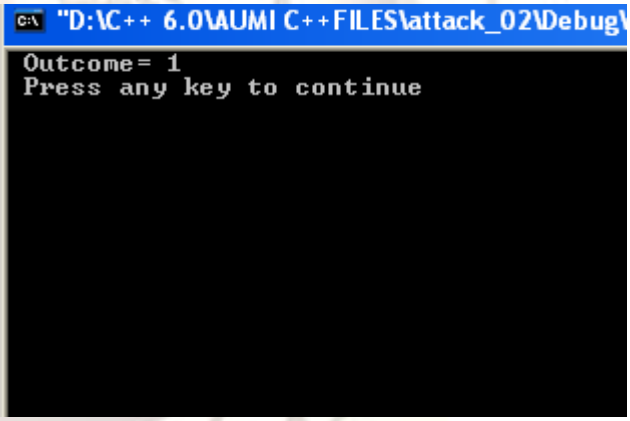


**Fig.7:** Result of the proposed model

From the above results it may conclude that when Outcome>1, then attacks are occurring and if Outcome=1, then attacks are reducing. So, in our proposed model attack is not possible because the outcome of the security model is equal to 1 (Outcome=1).

## VI. Differences Between Proposed Model and Other Systems

**Table 2:** Points out briefly the main difference between our proposed model and SERVE e-voting system.

| | Characteristics | Proposed model | SERVE system | Recent e-voting System |
|---|---|---|---|---|
| 1 | The period of e-voting | In the election day | Before the election day and on the election day | In the election day |
| 2 | Time Stamping | Yes | No | No |
| 3 | National public key infrastructure | Yes | No | Yes |
| 4 | A voter signs the encrypted ballot | Yes | No | Yes |
| 5 | The state of votes in Voting Server | Encrypted ballot | No encrypted ballot | Encrypted ballot |
| 6 | The state of Votes Counting Server | Offline | Online | Online |

From Table 2 we can get difference between our proposed model and SERVE e-voting system.

Proposed Model which is more secured than other e-voting systems, because in Proposed Model:

1. Voter Application creates a vote and encrypts the ballot by using the public key.
2. Encrypted ballots used in voting storing server.
3. Ballots are signed by voters.

4 Votes counting server is off-line contains, so the system can check the correctness of the process of e-voting and count the votes with the help of time stamping.

## VII. CONCLUSIONS AND FUTURE WORKS

Our proposed e-voting model is secure against the large-scale voting-specific attacks and the security properties of this e-voting model are justified. The Traditional paper based voting system is not secure enough. We develop a model with a view to analyze the practical security of the e-voting system and to compare objectively of its security level. For a developing country like Bangladesh where traditional paper based voting system is maintained with its drawbacks, our proposed e-voting system is more secure as it has the properties of elimination of the non-eligible specific voters. But regardless of being cost effective and time consuming system, the implementation of e-voting system in the voting procedure will ensure voting privacy, upgraded security level and thus the selection of a fair candidate. An interesting topic for future research would be to prove other security properties for Civitas using type-based verification. For instance, one could develop a linear type system for verifying freshness properties such as non-reusability. As future work, one could devise a more comprehensive model that includes e.g., multiple registration tellers and compromised participants.

## REFERENCES

[1] Johansen, B. (2007) *Get There Early: Sensing the Future to Compete in the Present*, San Francisco: Berrett-Koehler. Department of Defense Washington Headquarters Services Federal Voting assistance Program, Voting Over the Internet Pilot Project Assessment Report, 2001.

[2] Department of Defense Washington Headquarters Services Federal Voting assistance Program, Voting Over the Internet Pilot Project Assessment Report, 2001.

[3] Gritzalis D. (Ed.), *Secure Electronic Voting*, Kluwer Academic Publishers, USA, October 2002.

[4] VoteHere Inc., *Network Voting Systems Standards*, Public Draft 2, USA, April 2002.

[5] Jefferson D., Rubin A.D., Simons B., Wager. A., Security Analysis of the Secure Electronic Registration and Voting Experiment (SERVE), 2004.

[6] Ansper A., Buldas A., Oruaas M., Piirsalu J., Veldre A., Willemson J., Kivinurm, K.. The security of Conception of E-voting: Analysis and Measures, 2007.

[7] Martens T., Organizational and Technical Concept of the E-voting, 2003.

[8] Research Center Faktum & Ariko. The e-voting and diminishing alienation: The summary of the result of the public poll, 2004.

[9] The election' atlas of the United State of America. http:// www. Uselectionatlas.org/, 21.01.2007.

[10] Konho, T., Stubblefield A., Rubin A.D., Wallach D., Analysis of an Electronic Voting System, 2004.

[11] Local Government Association, The Implementation of Electronic Voting in the UK research summary, 2002.

[12] Newkirk, M.G., US Public Opinion towards Voting Technologies, InfoSENTRY Servies, 2004.

[13] Schneier B., Attack Trees, Dr. Doob's Journal December 2006, hppt://www.schneier.com/paper-attacktrees-ddj-ft.html.

[14] Buldas A., Laud P., Piirsalu J., Saarepera M., Willemson, J., Rational Choice of Security Measures via Multi-Parameter Attacks Trees, in Critical Information Infrastructured Security First International Workshop- CRITIS , LNCS 4347, pp. 235-248, 2006.

[15] Geer D., K. Soo Hoo K., Jaquith A., Information Security: Why the Future Belongs to the Quants. IEEE Security and Privacy, 2007.

[16] Evaluation report. Experiment with Internet and telephone voting for voters abroad, 2009.