Ishtiaque Mahmud, A.K.M. Nazmus Sakib, Shamim Ahmed, Sajeeb Saha, Md. Habibullah Belali, Nafiz – Al – Naharul Islam, Samiur Rahman / International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com
Vol. 2, Issue 5, September- October 2012, pp.425-429

A Realistic Secure On-line E-Voting System

Ishtiaque Mahmud*, A.K.M. Nazmus Sakib, Shamim Ahmed***, Sajeeb Saha****, Md. Habibullah Belali*****, Nafiz – Al – Naharul Islam******, Samiur Rahman*******

*(Completed M.Sc. and B.Sc. in Computer Science and Engineering from Jahangirnagar University (JU), Dhaka, 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 and Engineering from Dhaka University of Engineering and Technology (DUET), Gazipur, Bangladesh.)
**** (Completed M.Sc. and B.Sc. in Computer Science and Engineering from University of Dhaka (DU), Dhaka, Bangladesh,)
***** (Completed B.Sc. in Computer Science and Engineering from University of Dhaka (DU), Dhaka, Bangladesh,)
****** (Completed M.Sc. and B.Sc. in Computer Science & Engineering from Jahangirnagar University (JU), Dhaka, Bangladesh.)
BSc in Computer Science and Engineering from Chittagong University of Engineering and Technology.

ABSTRACT

This paper describes an on-line e-voting system security implementation to reduce attacks with the help of time stamping and hash function. E-voting is electronically voting process via Internet, it gaining popularity in applications that require high security. 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. The system also eliminates the voting process of non-eligible voters. The security of our e-voting model is more developed than recent e-voting systems.

Keywords - Electronic voting, large-scale attacks, Security, Time stamping, Hash function.

I. INTRODUCTION

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. 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 [2, 3]. In January 2004, a group of American Security experts revealed the security report of Secure Electronic Registration and Voting Experiment [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]. At the same time, Estonia continued to develop an e-voting system and implemented it according to the plans. The Estonian security experts published their security analysis at the end of 2003 [12, 13, 14].But the American both systems (SERVE and Estonian e-voting system) and the recent Bangladeshi e-voting system have vulnerabilities in the system design, which makes possible to perform voting specific attacks [15, 16, 17]. To solve this problem we developed e-voting model.

II. CONCEPT OF E-VOTING

2.1. Properties of E-Voting System

E-voting is a voting method where the voter intention is expressed or collected by electronic means. Remote electronic voting is the preferred term for voting that takes place by electronic means from any location. This could include the use of Internet, text message, interactive digital TV or touch tone telephone. Design of a better voting system, whether

electronic or using traditional paper ballots or mechanical devices must satisfy a number of following criteria [1].

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

2.2. Phases of E-Voting System

There are six main phases of e-voting system [1].

- **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.

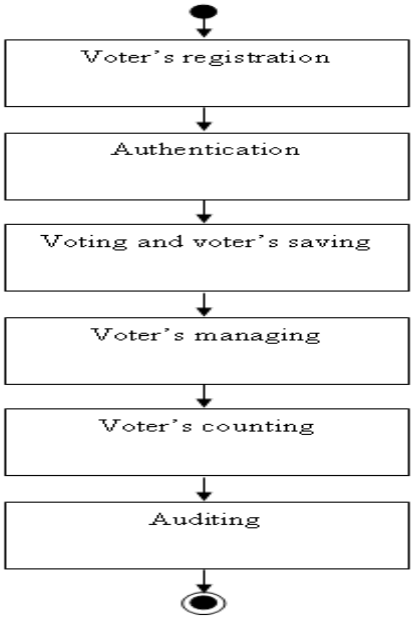

Fig.1: Phases of e-voting system

2.3. Components of E-Voting System

It is possible to divide the e- voting system into three main components of infrastructure [1].

- **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.

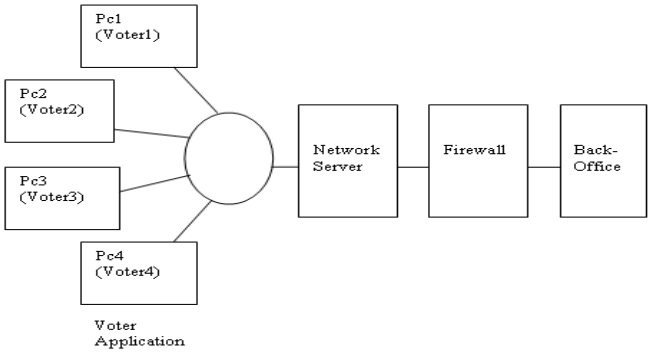

Fig.2: Components of e-voting system

2.4. E-Voting Attacks and Security Analysis

There are following e-voting specific attacks [1].

- **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

III. DESCRIPTION OF PROPOSED MODEL

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

3.1. Internal Components:

- Voter Application.
- Network Server.
- Voting Storing Server
- Votes Counting Server
- Back-office Server

Voter application: Voter application is a web application or an application in voter's personal computers for casting votes. It connects to network server.

Network server: Network server is an online server that provides voters a necessary interface for casting votes. It connects to voting storing server and transfers the received votes.

Voting Server: The voting server is responsible for the second stage of the election process. The voting server manages the vote casting stage. It receives the voters' anonymous ID validated from the network server, and use it to authenticate the legality of voter, but not the voter identity, which mean the voting server can only check if the voter have the rights to cast a vote or not, but it will be never able to figure the real identity of the voter who cast the vote in the time of the voting or after the end of the voting session. The voting server also keeps tracking the voting process to ensure that each eligible voter will vote only once.

Votes Counting Server: The counting server is responsible for the last and final stage of the election process which is votes counting also known as election post, the counting server collects the vote's ballots, counts the votes, and finally professes the election result.

Back-office Server: Back-office is consists of server to save and maintain votes and count a final tally with help of time stamping process and hash function.

3.2. External Components:

- E-token
- Certificate Authority

E-Token: Is a national public key infrastructure based on smart card and USB technologies. E-token includes a full suite of security and authentication methods. Voters will use e-token for authentication purpose in the voter application stage and also to store their election certificate, and to execute other security and cryptology computing required by the e-voting system. The use of e-token in our scheme provides a high level of security, and introduces a new feature which is the mobility of the scheme, which allows voters to cast their vote from any place and on any computer.

Certificate Authority: Is responsible to confirm the person identification data received by the network server in the voter application and identification stage and to provides personal information about the voter where the network server can use this information to take a decision about the state of the voter if he/she is eligible or not.

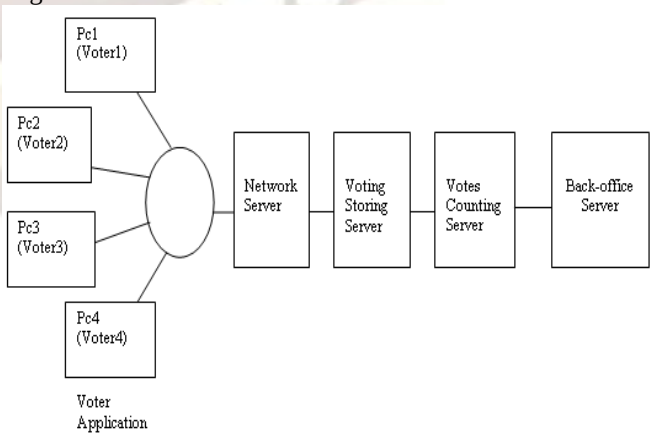

Fig.3: E-voting components of proposed model.

IV. VOTE COUNTING PROCESS OF PROPOSED MODEL

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 (Vote Count=1) and the attacker the attack is successful if (Vote Count=2).We can justify the security of our proposed model. Then we calculate the Votes. 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);

Vote Count = -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 and q_=0.096

Putting the value in equation (1) the Vote Count is

Vote Count = -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 . (1)
= 1

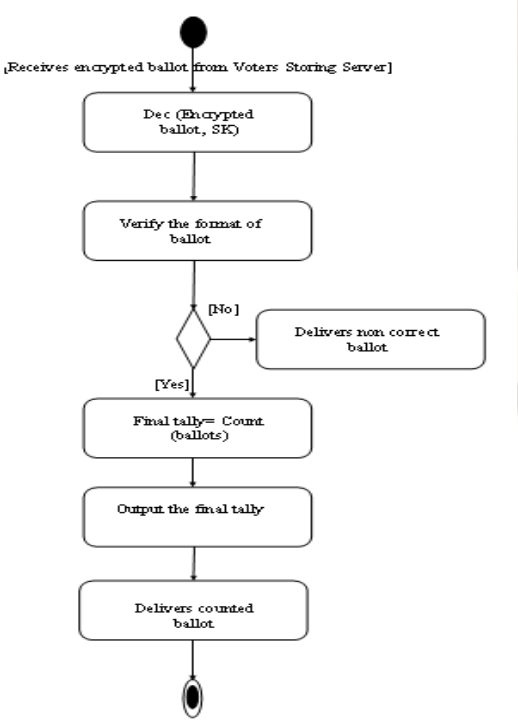

Fig.4: The votes counting process of proposed model

In our proposed model attack is not be successful because Vote Count equal to 1 (Vote Count=1). If (Vote Count=2) 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. ALGORITHM AND 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 and compare hash function.
Step3. If the time of voter 1st vote is grater or equal 2nd vote (1st vote time≥2nd vote time) and hash function (H1=H2) 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) and hash function (H1≠H2) then attack is reduce. Otherwise go to step 2.
Step5. If all attacks are reduced (Vote Count=1) then exit; else go to step 4.

5.2. Result

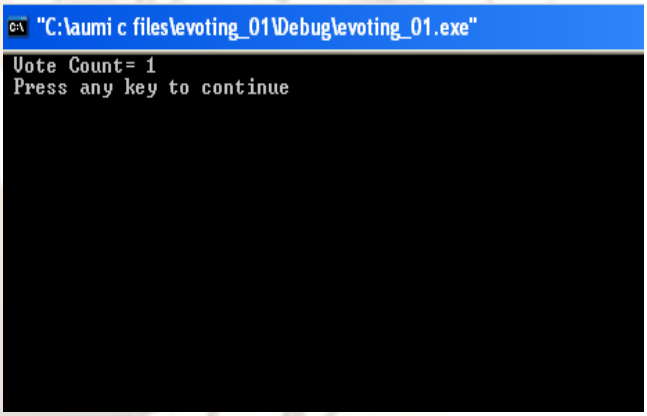

Fig. 5: Result of the proposed model

Fig.5 shows the result of the proposed model, Vote Count is equal to 1 (Vote Count=1).From the above results it may conclude that when Vote Count=2, then attacks are occurring and if Vote Count=1, then attacks are reducing. So, in our proposed model attack is not possible because the Vote Count of the security model is equal to 1 (Vote Count=1).

VI. DIFFERENCES BETWEEN PROPOSED MODEL AND OTHER SYSTEMS

Table 1: Points out briefly the main difference between our proposed model and other e-voting system.

	Characteristics	Proposed model	Bangladeshi e-voting system	American (SERVE & Estonian) e-voting system
1	The period of e-voting	In the election day	In the election day	Before the election day and on the election day
2	Time stamping & hash function	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 1 we can get difference between our proposed model and other e-voting system. The main difference of our system use time stamping process and the state of votes counting server is offline. But other e-voting system can not use time stamping process and the state of votes counting server is online.

VII. ADVANTAGES OF PROPOSED MODEL

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

1. Voter application creates a vote and encrypts the ballot by using the public key.
2. Encrypted ballots used in voting storing server and ballots are signed by voters.
3. otes counting server is off-line contains, so the system can check the correctness of the process of e-voting with the help of time stamping and hash function.

VIII. CONCLUSIONS AND FUTURE WORKS

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. 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 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. As future work, one could devise a more comprehensive model that includes e.g., multiple registration tellers and compromised participants.

REFERENCES

[1] Mahmud I, Ahmed S, Sakib N, Alendey Q.E, Jahan I, E-voting Security Protocol: Analysis & Solution, IJERA,2012.

[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, Info SENTRY Servies, 2004.

[13] Estonian National Electoral Committee. Data Structures of the E-voting System.

[14] Estonian National Electoral Committee. Essential Use Cases of the E-voting System

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

[16] 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.

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