An Exploratory and Feasibility Study of Implementing Online Based Voting System in Bangladesh

Mohammad Shabbir Hasan[1], Quazi Farhan[2] and Abdullah Al Mahmood[3]

Panacea Research Lab, Dhaka, Bangladesh
[1]shabbir_cse03@yahoo.com, [2]quazifarhan@gmail.com, [3]sajibcseofkuet@gmail.com

***Abstract*:** Modernization in voting system with various technologies has become an attention-grabbing issue in recent years. Currently, internet-based election systems are in the early stages of development and testing even in the developed countries and have been referred to as the ultimate challenge in network security and data encryption. Merging an information system with real-life problem has never been an easy task and to satisfy the zero-tolerance condition, the information systems implementation needs to handle lots of technical details. In Bangladesh, general elections are arranged on entirely paper based ballot system and manual voting procedures are employed. Here, electronic voting system is still in an experimental phase and the possibility of internet-based remote electronic voting in near future is not yet considered as tenable. But recent election problems in Bangladesh have sparked great interest in managing the election process through the use of internet to enhance the voters' scope for participating in the election as well as create scope for more error free rapid tallying of votes and distribution of seats and to enable the election commission to promptly announce the election results within a short time. In this paper, an online based voting system is proposed to eliminate the problems and bottlenecks of the existing voting systems in Bangladesh.

***Keywords*:** Online Voting System, Voting Systems in Bangladesh, Electronic Voting System.

1. Introduction

Election is the way through which people 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 [1]. Again, elections usually have high media coverage, especially if something goes wrong. Furthermore, voting system seems to have a unique combination of security requirements: voters need to be authenticated as well as results need to be verifiable. Voting systems are hard to make trustworthy because they have strong, conflicting security requirements: Integrity and confidentiality [2]. *Integrity* means election results must be guaranteed so that all voters are certain that votes are counted correctly and *confidentiality* means voters must be assured about the privacy of their votes, avoid selling of votes, and protect voters from coercion. In a word, voters need to be authenticated, results need to be verifiable, but it should not be possible to link a vote to a voter [3]. Although these conflicting requirements are very difficult to satisfy, the adaption of technology in upgrading voting system is practiced worldwide. The first use of computers to count votes — came with the introduction of the punch card system, first used in 1964. DREs (Direct Recording Electronic systems) are the first completely computerized voting systems. They were introduced in the 1970s [4]. Then some European countries started to introduce electronic voting systems. Hence, it can be said that Electronic voting is now a reality but along with many errors and vulnerabilities in commercial electronic voting systems [5, 6, 7, 8]. Many security experts have been skeptical about electronic voting [9, 10, 11, 12, 13], arguing that assurance in electronic voting systems is too hard to obtain and that their deployment creates unacceptable risks. More proofs of the vulnerability of an electronic voting system can be inferred from the fact that the use of similar paperless DREs has been discontinued in California [14], Florida [15], Ireland [16], The Netherlands [17], and Germany [18].

Recently, beside the conventional paper based voting system, Bangladesh Election Commission has also started experiments on electronic voting system by using electronic voting machines known as EVMs in some of the centers for Chittagong City Corporation Election 2010. As a process of building up *Digital Bangladesh,* it is highly likely that EVMs will be extensively used in the next National Election of Bangladesh. Even the possibility of remote electronic voting system, though not tenable in near future, is not out of question as there have been some research works conducted on SMS based secured electronic voting system [19] and internet based secured electronic voting system [20] also. This paper focuses on a comparative exploratory and feasibility study of online voting system with the existing voting system to upgrade a sensitive issue like national election, especially in a country like Bangladesh which is disreputably known for corruption and political mayhem.

The organization of the paper is as follows: section 2 briefly discusses about various voting systems previously implemented in various countries of the world. Section 3 describes the security concern about the existing voting systems in Bangladesh. Section 4 describes the proposed online voting system followed by the verification of the casted vote in Section 5. Features of the proposed system and a comparison between the present voting system in Bangladesh and the proposed system are mentioned in Section 6 and 7 respectively. Section 8 includes some recommendation and conclusion in section 9.

2. Various Types of Voting Systems

Over the years, many innovative changes have occurred to enhance election systems mainly in order to reduce various types of election frauds. According to Coleman and Fischer, currently, five different technologies are in use — paper ballots, lever machines, punch cards, optical scan, and electronic systems (direct recording electronic or DRE) [21]. Many states of USA even use more than one system to strengthen security. Online voting is a reality in many European countries. Multiple casts in online voting became popular by the Estonian's legal binding Local Government Council Election in autumn 2005 [22]. Here in Bangladesh, the scenario is not so advanced in terms of both security and technology. Paper ballot was the only system available in Bangladesh. However, recently the Election Commission started experimenting with EVM (Electronic Voting Machine).

A. Paper Ballots: This is the most common and classical method of voting. In this system, the candidate lists along with their respective parties are placed in a ballot paper. Voters mark their choices on the ballot. Each voter gets one paper. The vote counting system is totally manual. All voting technologies using document ballots use paper or cardstock, but the term paper ballot generally refers to those that are designed to be read by humans rather than machines [23].

B. Lever Machines: There is no document ballot in this technology. A voter enters the voting booth and chooses candidates listed on a posted ballot by pulling a lever for each candidate choice. The votes are recorded by advances in a counting mechanism that are made when the voter leaves the booth [24].

C. Punch Card: This is the first technological approach utilizing computers to count votes. This was first used in 1964. In this system, the voter records choices by punching holes in appropriate locations on a paper computer card that is later fed into a computer reader to record the vote. The computer card serves as the document ballot on which the votes are recorded [24]. Punch cards can be manually recounted and audited.

D. Optical Scan: This technology has been used for decades in scoring standardized tests. It first became available for use in voting in the 1980s. In this system, a voter fills in a box or oval or completes an arrow corresponding to each candidate choice using a paper form and an appropriate writing instrument. The completed ballot is then read by a computerized device that senses and records the marks [24].

E. Electronic Voting Machine: DREs (direct recording electronic systems) are the first completely computerized voting systems. They were introduced in the 1970s [4]. In this system, the voter chooses candidates from a posted ballot which may be printed and posted on the DRE or it may be displayed on a computer screen. Voters make their choices by pushing buttons, touching the screen, or using other devices depending on the equipment used.

DREs can be classified into three basic types. The oldest design mimics the interface of a lever machine. The entire posted ballot is visible at once. The voter pushes a button next to a candidate's name, or pushes on the name itself, triggering an underlying electronic micro switch and turning on a small light next to the choice [4]. In case of the second design, a ballot page is displayed on a computer screen, and the voter uses mechanical devices such as arrow keys and buttons to make choices on a page and to change ballot pages. The third type is similar to the second except that it has a touch screen display. Here, the voter makes a choice by touching the name of the candidate on the computer screen and casts the ballot by pressing a separate button after all choices have been made. In Bangladesh, the oldest type of DRE which is popularly known as EVM is under experiment at present.

Another form of electronic voting currently in development is Internet voting, in which voters make their choices online. This system is far more advanced in terms of technology but poses special challenges for ensuring authentication, secrecy, and security in the voting process.

3. Various Security Vulnerabilities of the Existing Voting Systems in Bangladesh

A. Security Concerns about Paper Based Voting System:

Paper ballot system is the conventional paradigm which is being used in Bangladesh from the beginning of voting. Paper ballots are readily understandable by the voter which is a great advantage as there are a huge number of uneducated voters here in Bangladesh. The security concerns are well understood by the authority as there are no chances of high-tech security breach in this system. The tampering of ballot paper is possible but this requires the involvement of corrupt officials. Ballot box hijacking and coercing the present officials to manipulate the result in a particular center are some other types of vulnerabilities in this system.

B. Security Concerns about EVMs:

Electronic Voting Machines, known as EVMs are widely used in Indian elections and now under experiment in Bangladesh. These EVMs are said to have less complex code than the previous electronic voting systems like DREs. In spite of this simplicity which makes them less susceptible to some of the threats faced by DREs, it also subjects them to a different set of highly dangerous attacks. An Indian research revealed two major types of possible attacks on Indian EVMs [25]. One of them is named as *Dishonest Display Attack* in which the real display board in the control unit of an EVM is replaced by a dishonest display board developed by the attacker. Another type of attack is called *Clip-on Memory Manipulator Attack* which uses new hardware to alter the internal state of the machine. In "Security Analysis of India's Electronic Voting Machines", the authors demanded that the Indian EVM manufacturers are exporting machines to Bangladesh [25] which is not correct as the EVMs which are currently being used in Bangladesh are developed by Information and Communication Technology (IICT) of Bangladesh University of Engineering and Technology (BUET) and a local manufacturer company named Pi Labs, Bangladesh. However, when asked about the similarities, the developers acknowledged that both share many similar characteristics and design patterns and Bangladeshi EVMs are also vulnerable to both *Dishonest Display Attack* and *Clip-on Memory Manipulator Attack* mentioned above. Bangladeshi EVMs are unique in the way that *Smart Cards* are used for configuring these EVMs. Smart Card is used to configure the Bangladeshi EVM which reduces the cumbersome work at the field level. This configuration procedure is done in two stages. In the first stage Symbols of the candidates and their allotted button number are written on the Smart card from a PC application. And then in the second stage at the field level, authorized person inserts the card to the control unit and presses the specified button and that finishes the configuration process. In contrast to the Indian EVM's configuration procedure the process described above might appear too much user friendly and less cumbersome but Indian EVM manufacturers may claim superior transparency in this aspect as it is done manually. The use of smart cards for configuring EVMs opens up another opportunity of susceptibility. If someone can have the chance of having access to any of the smart cards then he/she can configure it as desired. This *Smart Card Attack* also needs physical access like the previously mentioned two types of attacks. Another major concerning issue of these EVMs is that they do not use any kind of encryption for signal transferring.

4. Proposed Online Based Voting System

The proposed system comprises of several steps. The system is accessible from two sides: (a). Election Commission who is the administrator and (b). The voter. There are some steps which are automated i.e. not accessible from any side. Figure 1 shows the possible input output scenario of the proposed system and total system architecture is presented in detail in Figure 2. Steps of the proposed system are described in the following section.

A. Adding Voter Information

In this proposed system, information of each voter is added according to their National Identity Number. This National Identity Number is unique for each voter and this number is also used to identify the constituency of the voter. After adding information, an auto generated e-mail is sent to the e-mail address of the voter notifying him/her about the information and this e-mail also contains a computer generated password which can be used by the voter for login as well as for changing password and setting verification keys. Here verification keys are used to protect "*Vote Purchase*" and to ensure security. On screen keyboard is used to take the new password from user. The system will not take the password typed in any keyboard other than the onscreen keyboard. Purpose of using on screen keyboard is to prevent capturing password through any software if the voter changes password from any cyber café or in any public computer. Discussion about the use of verification keys is presented later.

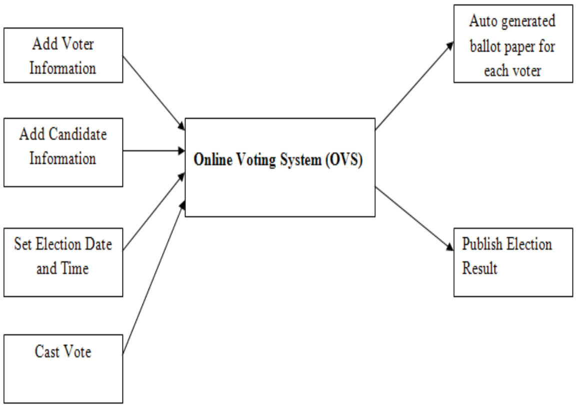

Add Voter Information
Add Candidate Information
Set Election Date and Time
Cast Vote
Online Voting System (OVS)
Auto generated ballot paper for each voter
Publish Election Result

Figure 1. Possible Input-Output scenario of the proposed Online Voting System

B. Adding Candidate Information

Candidate information is added according to the constituency. Here each candidate is assigned an auto generated code to identify uniquely. Party symbol and candidate profile image are also added with other information in this phase.

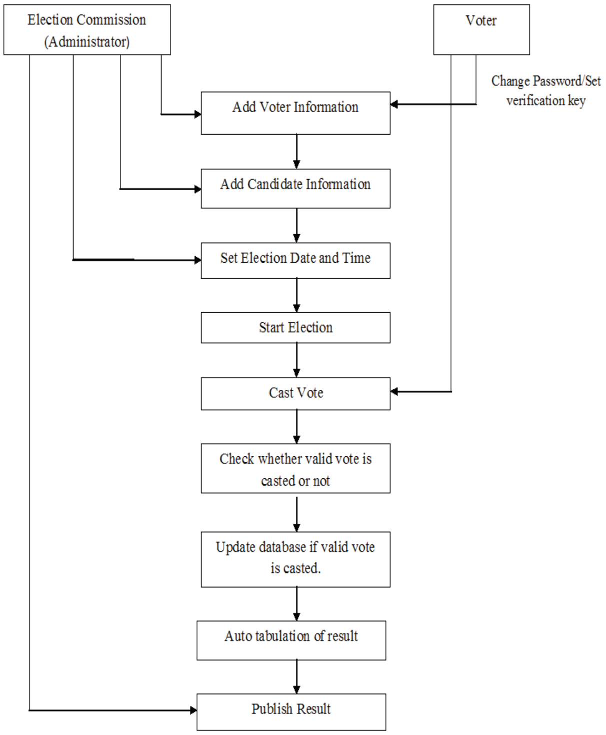

Election Commission (Administrator)
Voter
Change Password/Set verification key
Add Voter Information
Add Candidate Information
Set Election Date and Time
Start Election
Cast Vote
Check whether valid vote is casted or not
Update database if valid vote is casted.
Auto tabulation of result
Publish Result

Figure 2. Details architecture of the proposed system.

C. Setting Election Date and Time

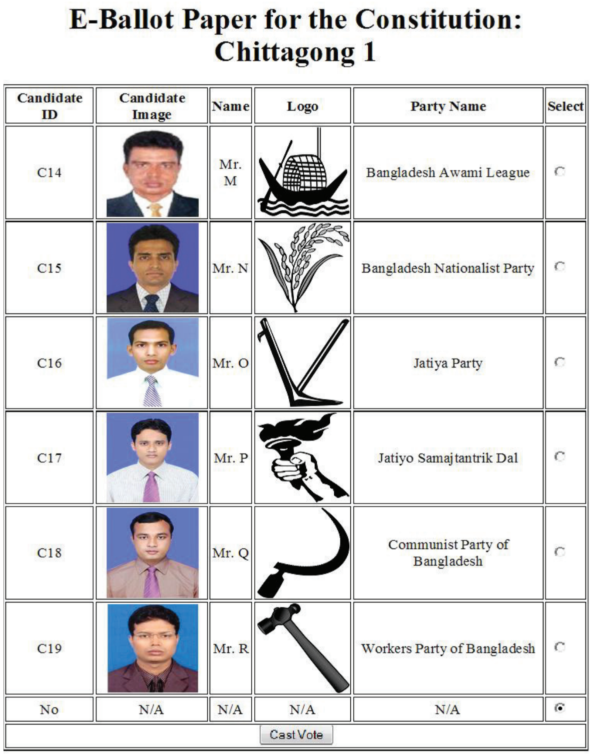
In this phase, starting time and ending time of election along with election date are set by the election administrator. Bangladesh is in the "Dhaka" time zone which has +6.00 offset from GMT. The voting server is configured according to this time zone. Voters who reside outside of Bangladesh can cast their vote according to the local time in Bangladesh during Election Day.

D. Start Election

This is an automated phase. During the stipulated date and time, election is started. Voter can cast their vote within this time period. If anyone wants to cast vote before or after the specific time period, an error message is shown.

E. Cast Vote

In this phase, voter has to login first. After logging in with the national id and password, the constituency of the voter is determined from the information stored in the voter database. An E-Ballot paper is created automatically for that constituency from information stored in candidate database. This ballot paper contains the candidate name along with their profile picture, party name with party logo and a radio button to select the candidate for casting vote. There is also a "No" option if the voter is not interested to cast vote to any of the available candidates. Figure 3 shows a sample ballot paper for a constituency.



E-Ballot Paper for the Constitution: Chittagong 1

Candidate ID	Candidate Image	Name	Logo	Party Name	Select
C14		Mr. M		Bangladesh Awami League	○
C15		Mr. N		Bangladesh Nationalist Party	○
C16		Mr. O		Jatiya Party	○
C17		Mr. P		Jatiyo Samajtantrik Dal	○
C18		Mr. Q		Communist Party of Bangladesh	○
C19		Mr. R		Workers Party of Bangladesh	○
No	N/A	N/A	N/A	N/A	●

Figure 3. A sample E-Ballot paper for a constituency.

Voter selects radio button of the corresponding candidate and finally press the "Cast Vote" button. A security checking is done to verify whether the vote is casted actually by the voter himself. A discussion about the security checking is presented in the next section.

F. Security Checking

When a voter presses the "Cast Vote" button in the e-ballot paper after selecting the suitable candidate, a security checking is done internally. This security checking is one of the most striking points of this proposed system as it is required to protect "*Vote Purchase*" by any candidate. Figure 4 shows the steps of the security checking process.

Voter can enter verification key before election by logging in his/her account as we mentioned in section A. Number of verification keys to be used are selected by the voter, but among them, only one key is used as "*Real Key*" and rest of them are treated as "*Fake Key*". Among these keys voter will select which one will be used as "*Real Key*". In case of any attempt to "*Purchase Vote*" by any candidate, the voter has the option to hide "*Real Key*" and supply only "*Fake Keys*" to the candidate. If vote is casted by using fake keys, notification will be shown as if vote is casted successfully, but there will be no update in database. So if the voter wants to cast his/her vote, he/she can cast vote using the real key in any time within the voting period. This process will reduce the tendency of purchasing vote by any candidate and hence make the election process fair.

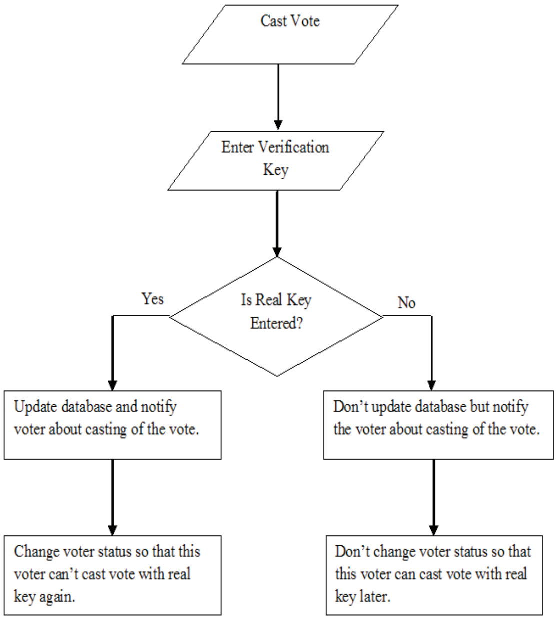

Cast Vote
Enter Verification Key
Is Real Key Entered?
Yes
No
Update database and notify voter about casting of the vote.
Don't update database but notify the voter about casting of the vote.
Change voter status so that this voter can't cast vote with real key again.
Don't change voter status so that this voter can cast vote with real key later.

Figure 4. Flow Diagram of the Security Checking Process.

G.Auto Tabulation and Publication of Result

During the election period, result is tabulated automatically and after the election period is over, winner in each constituency is declared automatically. In this proposed system, results can be published immediately which leads to a huge saving of time than the existing methods.

4.1 Security Measurement of the Proposed System

A basic assumption of online voting system is that it does not disregard the underpinning principles of an electoral system. In traditional system voters attend at designated polling centers and nominate their candidate using ballot papers. This way the voter can be assured that his/her confidentiality has been preserved and vote has been casted correctly. But using online system, when voters are casting their vote digitally from their household they cannot be sure that their vote is indeed counted. On the other hand if voters are provided with the opportunity of verifying their vote after casting, this can be used for coercion or vote selling. These contradictory issues are the first hurdle of online voting.

Beside this, there is also a chance of wire tapping or any other means through which voter's identity and vote can be exposed to sniffers. It can be interrupted in the way or may get lost due to bad transmission. To enhance security, in this proposed system, vote is encrypted after casting.

In this proposed system the dilemma between voter integrity and confidentiality is solved using the key that the voter used previously to cast vote. This verification technique is described in detail in the next section.

5. Verification of the Casted Vote

To validate the correctness of the voting, to assure the voter that the vote has been casted exactly the manner he/she intends; multiple, independent communication is required, as employed by the Moguls in India some 500 years ago in the context of combating corruption [26] or mathematically described by Claude Shannon some 50 years ago in the context of combating noise when he introduced his Information Theory [27], a well-known general theory of communication processes.

The problem with the solution is maintaining two parallel schemes is no small feat. The cost, manpower, complexity and newly arisen security holes nullify the advantages of online voting. Worse yet is even with such exaggerated method we cannot rectify an error. Let us consider two ballot of a voter shows two opinions. Online submission chooses one candidate and offline/printed copy supports another. With no way to deduce which was the original choice of the voter, the approach can only ensure that the online version might be wrong but not with certainty, since the offline ballot might tampered with, too.

Now, here comes the most crucial contradiction of using an online system: conflict of integrity and confidentiality. While integrity requires all voters' votes must be counted and voters must be assured that their votes are casted and counted properly. But confidentiality complies that there is no way a voter's ballot and voter's id can be connected, even if a court order comes in or supervisors in charge of election collude. This dilemma can be solved using the key that was used previously by the voter to cast vote. Voter can verify whether the vote has been casted as well as counted correctly by inputting the key that he/she provided during casting his/her vote. In database, information regarding the casted vote and the corresponding key is stored. So voter can retrieve his/her vote information by providing the key. Even if vote is casted using one of the fake keys, it also returns the candidate name that was selected by the unauthorized person during casting vote by using fake keys though this vote has no effect in counting the total vote. As only candidate name with the corresponding key is stored in the table, i.e., no voter information is stored so only voter can check whether vote is correctly casted or not. So it preserves the confidentiality. Again as the system allows voter to become assured of the casted vote, it also ensures integrity of the voter. This verification system is presented in Figure 5.

Another layer of security is client software. Instead of implementing this as a web interface, a java applet or custom software is prepared, which is available to download at the voting site just prior the voting commences and the server always monitors the applet/client for any kind of modification or tampering. In this way we can ensure another layer of security even on the client end.

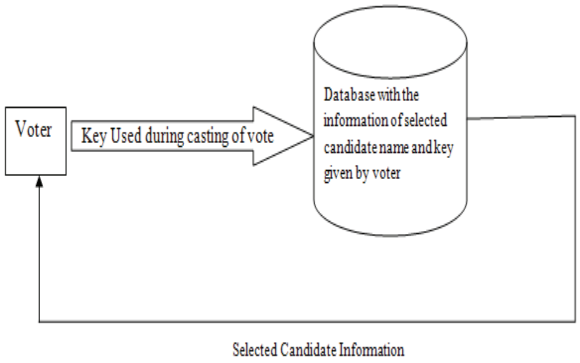

Voter
Key Used during casting of vote
Database with the information of selected candidate name and key given by voter
Selected Candidate Information

Figure 5. Verification by the voter whether vote is casted and counted correctly.

6. Features of the Proposed System

The features of the proposed system are:

a. No need to stay in the queue for a long time to cast vote, anyone can cast his/her vote from anywhere through internet.

b. Increased voter turnout.

c. The cost for arranging election will be reduced as there is no need to prepare any voting center or no need to manage huge manpower.

d. Impervious security checking to verify whether vote is casted by the voter himself.

e. Verifiability by the voter of the casted vote.

f. Coercion resistant voting system.

g. Result can be published within a very short time as the system automatically tabulate the results and declare winners.

h. Overall, the election will be fair enough and transparent.

7. A Comparative Study between the Proposed System and the Existing System

As paper ballot based voting system is being used in most of the voting centers in Bangladesh, here we compare the proposed system with the paper based voting system. To compare with the existing system, the proposed system was implemented in the trade union election of Technocrats BD on February 2010. The election system was totally online based and the previous elections were paper ballot based like other traditional elections. Comparative statistics between these two election methods are shown in Table 1.

Table 1 shows that the proposed system increases voter turnout than the previous method as online voting system is very much convenient than the traditional voting system. In this proposed system voter cast their vote from any place through internet rather waiting in a queue for long time and this is the main reason for making the voting system interesting which leads to the increase in voter turnout.

From Table 1 it is also clear that there is no way of invalid vote in the proposed system which is a case in the traditional one. As the e-ballot paper contains radio button for each candidate, voter can select only one candidate at a time for the same post. If the voter doesn't select corresponding radio button of any candidate, "NO" vote is casted which means the casted vote doesn't correspond to any candidate. So there is no way of either casting multiple votes in the same ballot paper at a time or cast vote without selecting any radio button. That's the reason of 100% valid vote in the proposed system.

Table 1. Comparative statistics between two election methods.

Criteria	Paper Based Election on January 2006	Online Based Election System on February 2010
Total Voter	1054	1173
Turnout	797 (75.6%)	1053 (89.8%)
Valid Votes	753 (94.47%)	1053 (100%)
Total Cost (in Bangladeshi Taka)	84,320	82,110

Another striking point of the proposed system is the reduction of cost to arrange an election. Lots of manpower and funds are required to arrange the election in the traditional manner. But in this online voting system, there is no need of setup cost for any voting center as voters can cast vote from their personal computer and hence no manpower is required to maintain any voting center. Few people are enough to manage the complete process of the proposed system as many steps are fully automated. Huge reduction of cost is clear from Table 1. In the traditional system, 80 Bangladeshi Taka is required for each voter where as only 70 Bangladeshi Taka is required in the proposed system. With the increase in total number of voters, total cost to arrange election in the proposed system decreases rapidly than the traditional system which is shown in Figure 6.

Finally, after this comparative study, it can be said that better turnout and strong security system with low setup cost have made the proposed voting system better than the traditional system.

8. Recommendation

Before adopting any new voting system there should be at least two official technical evaluations and reviews of those technical evaluations should be made public so that general people can have more faith in new system. These technical evaluations must be performed by an expert committee which should have profound prior knowledge on computer security. One of the technical evaluations for Indian EVMs was conducted by an "expert committee" comprised of C. Rao Kasarbada, P.V. Indiresan, and S. Sampath [28], none of whom appear to have had prior computer security expertise [25]. Unfortunately, Bangladesh also has many previous examples of forming an expert committee without any expert members of the related issue. So, it is to be noted very carefully that a real expert committee must be formed for an official technical evaluation for such a sensitive matter like National Election. Moreover, this step will ensure that people have a reason to put their faith in this system.

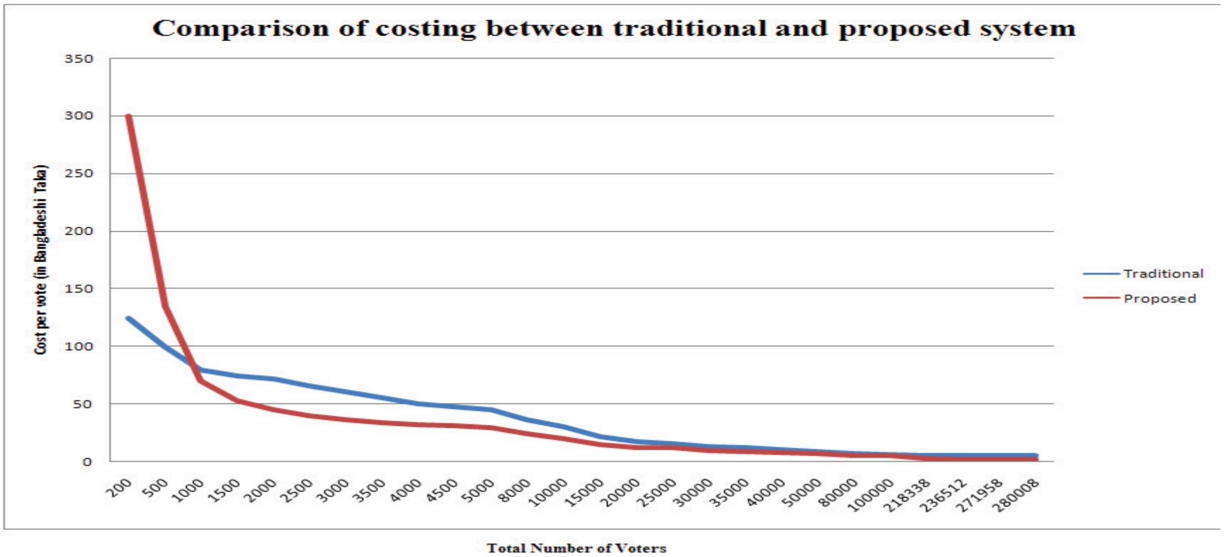


Figure 6. Comparison of costing between traditional and proposed voting system.

9. Conclusion

This paper discusses about various security issues of the existing voting systems in Bangladesh and also describes the design, implementation and evaluation of an online based efficient voting system. To our knowledge, this has not been done before in Bangladesh. Deriving from the previously-known voting scheme, the proposed system is coercion resistant and ensures security and efficiency through technical advances. Experimental results show that cost, tabulation time and security can be practical for real-world elections.

When a system like voting needs to be upgraded from a classical human dependant to a technologically advanced computer dependant system, it is certain that the system authority will have to face difficulty with security as well as lots of adversary of technical, social and also bureaucratic. But perhaps the most important contribution of this work is evidence that secure online voting system could be made possible and we are optimistic about the future of the proposed system which abides by the principals of electoral system.

References

[1] Tadayoshi Kohno, Adam Stubblefield, Aviel D. Rubin, Dan S. Wallach, "Analysis of an Electronic Voting System", Johns Hopkins University Information Security Institute Technical Report TR-2003-19, July 23, 2003.

[2] Michael R. Clarkson Stephen Chong Andrew C. Myers, "Civitas: Toward a Secure Voting System", Computing and Information Science Technical Report TR 2007-2081, May 2007.

[3] Bart Jacobs, Wolter Pieters, "Electronic Voting in the Netherlands: from early Adoption to early Abolishment", "Foundations of Security Analysis and Design", V: FOSAD 2007/2008/2009 Tutorial Lectures, Springer LNCS 5705, 2009, pp. 121-144.

[4] Eric A. Fischer, "Election Reform and Electronic Voting Systems (DREs): Analysis of Security Issues", "CRS Report for Congress", November 4, 2003.

[5] Jonathan Bannet, David W. Price, Algis Rudys, Justin Singer, Dan S. Wallach, "Hack-a-vote: Security issues with electronic voting systems", IEEE Security & Privacy, 2(1):32–37, Jan. 2004.

[6] Brennan Center for Justice, “The machinery of democracy: Voting system security, accessibility, usability and cost”, New York University, Oct. 2006.

[7] Tadayoshi Kohno, Adam Stubblefield, Aviel D. Rubin, Dan S. Wallach, “Analysis of an electronic voting system”, In Proc. of IEEE Symposium on Security and Privacy, pages 27–42, May 2004.

[8] David Wagner, Matthew Bishop, “Voting systems top-to-bottomreview”,http://www.sos.ca.gov/elections/elections_vsr.htm, 2007.

[9] David L. Dill, Bruce Schneier, Barbara Simons, “Voting and technology: Who gets to count your vote?”, Communications of the ACM, 46(8):29–31, Aug. 2003.

[10] David Evans, Nathanael Paul, “Election security: Perception and reality”, IEEE Security & Privacy, 2(1):24–31, Jan. 2004.

[11] David Jefferson, Aviel D. Rubin, Barbara Simons, David Wagner, “A security analysis of the secure electronic registration and voting experiment (SERVE)”, http://www.servesecurityreport.org/paper.pdf, Jan. 2004.

[12] Rebecca Mercuri, “Statement on electronic voting”, http://www.notablesoftware.com/RMstatement.html, 2007.

[13] Aviel D. Rubin, “Security considerations for remote electronic voting”, Communications of the ACM, 45(12):39–44, Dec. 2002.

[14] D. Bowen et al, “Top-to-Bottom Review of voting machines certified for use in California”, Technical report, California Secretary of State, 2007.

[15] A. Goodnough, C. Drew, “Florida to shift voting system with paper trail”, The New York Times, Feb. 2007.

[16] Minister Gormley announces Government decision to end electronic voting and counting project, http://www.environ.ie/en/LocalGovernment/Voting/News/MainBody,20056,en.htm, Apr. 2009.

[17] A. U. de Haes, “Dutch government bans electronic voting”, IDG News Service, May 2008.

[18] Bundesverfassungsgericht, German Constitutional Court. Judgment 2 BvC 3/07, 2 BvC 4/07, official English translation.
http://www.bverfg.de/entscheidungen/rs200903032bvc000307en.html, Mar. 2009.

[19] Chowdhury M. Rahman, Md. Adnan Khan, “Study of SMS Security as part of an Electronic Voting System”, Unpublished Thesis report, BRAC University, Bangladesh, 2006.

[20] Mohammad Shabbir Hasan, Abdullah Al Mahmood, Quazi Farhan, “A Roadmap towards the Implementation of an Efficient Online Voting System in Bangladesh”, To be appeared in “International Conference on Computational Intelligence and Software Engineering”, 2010, China.

[21] Kevin J. Coleman, Eric A. Fischer, “Elections Reform: Overview and Issues”, “CRS Report for Congress”, October 30, 2003.

[22] Melanie Volkamer, Rüdiger Grimm, “Multiple Casts in Online Voting: Analyzing Chances”, “2nd International Workshop Co-organized by Council of Europe, ESF TED, IFIP WG 8.5 and E-Voting.CC”, August 2006.

[23] S.J. Ackerman, “The Vote that Failed”, “Smithsonian Magazine”, November 1998.

[24] Eric A. Fischer, “Voting Technologies in the United States: Overview and Issues for Congress”, “CRS Report for Congress”, March 21, 2001.

[25] Hari K. Prasad, J. Alex Halderman, Rop Gonggrijp, Scott Wolchok, Eric Wustrow, Arun Kankipati, Sai Krishna Sakhamuri, Vasavya Yagati, “Security Analysis of India’s Electronic Voting Machines”, http://indiaevm.org/, April 29, 2010.

[26] Ed Gerck, in an interview by Eva Waskell, “California Internet Voting.”The Bell, Vol. 1, No.6, ISSN 1530-048X, October 2000.

[27] Shannon, C., “A Mathematical Theory of Communication.” Bell Syst. Tech. J., vol. 27, pp. 379-423, July 1948.

[28] C. R. Kasarbada, P. V. Indiresan, S. Sampath, “Report of the expert committee for technical evaluation of the electronic voting machine”, Apr. 1990.