Chapter 1

Introduction

1.1 Motivation

The emerging Information Society has enabled people in the developed countries to perform several of their activities in a direct, electronically automated and efficient way. To keep up with the need to provide citizens with the ability to benefit from services over networks, as well as to reduce the cost and bureaucracy of public administration, governments are striving to transfer an increasing number of their activities to the new medium.

E-voting can be an efficient and cost effective way for conducting a voting procedure and for attracting specific groups of people (e.g. young or disabled electors) to participate [1]. The term e-voting (electronic voting) is used hereby to denote a voting process, which enables voters to cast a secure and secret ballot over a network. In this paper, e-voting refers to general elections and/or referenda, at state and/or local level, with binding effects.

Many public authorities are, in general, concerned with the compliance of electronic voting systems with the existing legal (i.e. constitutional) framework. The first aim of the paper is to discuss whether an e-voting scheme could meet the legal requirements, as these are laid down in the modern information societies. The paper discusses how an e-vote process should be designed and implemented, in order to comply with the democratic election principles and rights, as well as to the other human rights, which constitute the cornerstone of the international legal civilization. Along these lines, the requirements of an electronic voting system are considered as the design principles, which are essential to comply with, in order to conform to the legislation framework, which is governing general elections [2]. Although technology moves at a pace faster than the legal system does, technological evolution should be pursued as a means to improve human life, as opposed to an end by itself. In this respect, the technological developments — and in particular those affecting fundamental principles — should be carefully reviewed with an eye towards ensuring their contribution to the improvement of the quality of the citizen life.

The second aim of this paper is to discuss confidence upon technology. Information system developers face e-vote systems with an eye towards ensuring their adequate level of security [3-7]. In recent literature, a distinction is often made between different types of e-voting systems requirements [8]. In literature, requirements are usually identified as legal, technical and user-oriented — the latter in the form of conditions the system should meet (e.g. “the system shall allow online-voting from home”). Other authors select a specific election procedure (e.g. the paper absentee ballot process [9]), deriving requirements for electronic voting systems based solely on this procedure. Although such approaches may produce acceptable e-voting systems in given contexts, they have not yet led to the specification of a complete system.

This paper focuses on the elicitation of the legal and functional requirements of an e-voting system, through a User Requirements Specification suitable for providing information system designers with the essential information for designing a valid and complete system. A milestone, towards this end, is the development of a generic e-voting model by depicting the principles and practices to be followed during an election procedure.

The present report attempts to provide better chances for secure electronic voting by reducing the problems and irregularities of the existing voting schemes. One possible solution could be the biometric voter authentication, vote casting and counting presented in this thesis.

1.2 Main Issues of E-Voting

A fundamental challenge of electronic democracy is to improve and develop representative democracy and strengthen processes aiming at the empowerment of citizens [10]. The new civilization, brought about by the Information Society, should comply with the principles and values of democracy. The introduction of an e-voting system should conform to this rule, since voting is one of the functions "e-citizens" may wish to see performed online. In this respect, a phenomenon, which should be taken under consideration, is the digital divide. Affordable access to the Internet is a key to fight the digital divide between the "info -rich" and the "info-poor" in an Information Society. Specific policies should be adopted towards this end. The European Union, for example, has adopted three key actions: a) to adapt the existing regulatory framework to communication industry needs in the Internet, b) to boost competition in local access networks, so as to encourage widespread Internet take-up and high-speed Internet access in Europe, and c) to ensure a high standard of user rights and privacy protection.

An election system may, by itself enforce unequal access of an individual to the electoral process [11]. It is a matter of democracy, equality, and equity to guarantee that the traditional and the e-voting technologies are equivalent, with respect to ease and opportunity of access. Parliamentary elections have to be free, equal and secret. At the same time, the election procedure has to be transparent and subject to public scrutiny.

The constitutions of many countries require that general elections should respect Generality, Freedom, Equality, Secrecy, and Directness. Adding to them the fundamental requirement of Democracy, the set of generic constitutional voting requirements stems with. This set reflects, in turn, to the set of the essential voting design principles (shown in Table 1.1).

Table 1.1: Constitutional requirements and design principles.

Constitutional requirements	Voting systems design principles
Generality	▪ Isomorphic to the traditional ▪ Eligibility
Freedom	▪ Uncoercibility ▪ No propaganda in the e-voting site ▪ Non-valid voting capability
Equality	▪ Equality of candidates ▪ Equality of voters ▪ One voter - one vote
Secrecy	▪ Secrecy ▪ Balance security vs. transparency
Directness	▪ Unmonitored ballot recording and counting
Democracy	▪ Trust and transparency ▪ Verifiability and accountability ▪ Reliability and security ▪ Simplicity

1.3 Voting Systems Design Principles

1.3.1 Generality

Universal suffrage is a generic principle for democratic elections, requesting that every eligible voter can participate in the election process, and nobody can be excluded or discriminated. The consequences deriving from this principle are the following:

- Every voter has the right to participate in an election process.
- The ability to participate in an election process (eligibility) must be founded on and be controllable by the law.
- Voting possibilities and technologies should be accessible by every voter.
- E-voting should be considered as an alternative way of exercising one's voting rights.
- The democratic principle (i.e. every eligible voter should be included in the election process) leads to publicly available appropriate infrastructure (e.g. public internet kiosks, internet voting in state offices, etc.), in order to allow citizens to exercise their rights.

E-voting improves the generality of election procedures by providing an additional option of participation to the electoral process [11]. An issue arising is whether participation in the election through e-voting should be subject to the proof of special conditions, as is the case

with postal voting. In most countries where postal voting has been established, only specific categories of individuals are allowed to exercise this option.

Adopting an e-vote capability as an exception to the rule (i.e. on the ground of the proof of a special condition, which prevents the eligible voter from physically casting her vote) is generally considered acceptable. On the other hand, the evolution towards the Information Society has a significant impact on the ability of a citizen to exercise her rights. In the light of the political decision to improve e-government and e-participation, the introduction of an e-voting capability should be viewed as an isomorphism of the traditional voting system.

Eligibility can be ensured through the registration of eligible voters and their identification at the moment of registration. Registration and authentication are procedures, which are essential to ensure that the principle of universal suffrage is being respected and that elections cannot be rigged. The purpose of keeping a voters' register is to guarantee that only people eligible by law to vote can do so, and that no one can vote more than once.

Another issue is whether there is a need for registration in the case of e-voting. E-voting is, in some way, analogous to postal voting. Where an e-voting system is introduced, registration and authorization procedures are usually required. These procedures do not conflict with the principle of general elections for the following reasons: a) supposing that there is no national online voter register, a pre-registration for e-voting is necessary, to avoid vote fraud and support the integrity of elections. On the other hand, an Internet-based voter registration system could be vulnerable to large-scale fraud [12], and b) in case e-voting is an alternative to the traditional procedure, registration or declaration that the voter wishes to use the e-voting option should not lead to exclusion or discrimination. Moreover, it should be ensured that it is easy for e-voters to register, identify and authenticate themselves, because complicated procedures could be a burden to them [13].

1.3.2 Freedom

The principle of free election requires that the election process take place without any violence, coercion, pressure, manipulative interference, or any other influence, exercised either by the state or by one or more individuals. Regarding postal voting, the voter may be asked to sign a declaration on the vote-by-mail certificate, promising that she has filled out the ballot personally. Providing such a signature is not trivial in e-voting [14]. E-voting procedures pose new threats to the freedom and integrity of a voter decision, beyond those that postal voting does. For example, in the case of the workplace, even if the employer, the supervisor or a colleague are not standing over the shoulder of the e-voting employee, system administrators can monitor or record the activity at each workstation and obtain a copy of the ballot [15].

Uncoercibility and prevention of vote buying and extortion can be ensured by an e-voting system designed so that no voter can prove that she voted in a particular way (intractability on the part of the voter) [16]. Since the employment relationship is not power-balanced, it is

suggested to avoid e-voting from the workplace. In any case, coercion can hardly be prevented by technology alone. One solution to this is to develop a publicly accessible infrastructure, allowing voters to exercise their rights free of the coercion of any third party.

The freedom of decision may be violated if a propaganda message is blended on the computer screen while the voter is casting her electronic ballot. In current election schemes it is not allowed to advertise in (the vicinity of) the polling place. The e-voting procedure should also make the advertisement of political entities on the e-voting website technically infeasible.

The free expression of the preferences of the voter should be ensured [17]. Therefore, the possibility for casting a consciously invalid (or "white" paper) ballot should be ensured.

1.3.3 Equality

The requirement of equality, in the context of general elections, is a reflection of the generic principle of equality and constitutes one of the cornerstones of modern democracies. Under the principle of equal suffrage, two major requirements are identified: a) equality regarding the participating political parties and candidates and b) equality regarding the voting rights of each voter.

A requirement deriving from the principle of equality is that electronic ballots should be edited and displayed in a way analogous to that used for the paper ballots. Electoral equality requires that there are no meaningful deviation between the printed ballot and its electronic equivalent look. Furthermore, the placement of electronic ballots in the voting site (i.e. on a computer screen) should ensure equal accessibility. Thus, the "look and feel" of the e-voting website and ballots should not favor or discriminate against any of the participating parties. Another element of equality among the participating parties is that the ballot of the voter is transmitted and counted without any changes or/and interferences. A valid cast vote must not be altered or removed in the course of the voting process.

Transparency should also be supported. All parties should have the opportunity for equal access to the elements of the voting procedure, in order to be able to establish its proper functioning.

The principle of equality requires that each vote, either physical or online, be equally weighted towards the election outcome. In an e-voting situation, certain voters have an access advantage to the enabling technology and, therefore, to e-voting capability. Some argue that remote voting could be used to manipulate election outcomes by managing the access in a way favoring those who are the most network connected [18].

Because of the emerging characteristics of the technology, the right to equal accessibility to the voting process should become the right of equal accessibility to election technology [19]. As a result, a non-discriminating procedure should be offered to the voters, allowing them to

efficiently exercise their voting rights with no obstructions. Equal accessibility means, also, that the system should be user-friendly and independent of a voter education, age, and physical condition (to accommodate physically disabled voters).

An e-voting system should ensure that the one voter - one vote principle is respected, that is only eligible voters can vote, only once, either online or off-line. Therefore, an e-voting system should be designed in such a way as to prevent the: a) Duplicability of the vote (either by the voter herself or by someone else), b) reusability of the vote (either by voting online more than once or by voting both online and offline), and c) modification of the cast vote (after a voter has dispatched her vote).

Another issue is the duration of the e-voting period. The California Internet Voting Task Force suggests that Internet voting does not continue throughout the election day, i.e. that there should be a time in advance of the election day, fixed by law, when e-voting is cut off. On the other hand, and in order to facilitate e-voting, others suggest that the voting period be extended for more than one day. This possibility may result in two suggestions: a) In most European Union member States the general elections take place on one day only, therefore the relevant legal provisions should be amended, and b) the principle of equality is put in question, especially if e-voters could make use of this possibility for more than one day.

1.3.4 Secrecy

Secrecy and freedom are strictly related principles. Secrecy is the condition of the voter free political decision. In democratic elections the link between the vote and the voter should be irreversible to ensure that votes are cast freely. In traditional voting systems secrecy is physically protected, but e-voting may make e-voting vulnerable to violations of secrecy. As a result of the above, the following requirements are derived: a) The secrecy of the vote should be guaranteed during casting, transfer, reception, collection and tabulation of votes, b) none of the actors involved in the voting process (organizers, election officials, trusted third parties, voters, etc.) should be able to link a vote with an identifiable voter, c) there should be a clear separation of registration and authentication procedures, on one hand, and casting-transfer of the vote, on the other, d) no voter should be able to prove that she voted in a particular way.

The electoral provisions which are applicable to postal voting and to the protection of communication secrecy could also serve as a basis for solving the problem of political privacy. However, there can be no guarantee of freedom from external influence by third parties during the casting of votes. This is an inherent risk of any form of remote or e-voting. To face this risk, measures should be taken on the legal and regulatory level, in order to impose adequate measures against coercion and to sanction illicit behavior.

Secrecy has to be in harmony with the democratic principles for general elections. Ballot secrecy should be reconciled with transparency and audit ability of the entire voting process. The election system should allow the verification of the authenticity of the ballot before the

votes are viewed or counted. In order to protect secrecy, the voted ballots should be decrypted and counted only after the authentication information is reviewed and removed. The e-voting system should make vote control and recount technically feasible, while ensuring the non-identifiability of the voters [20, 21].

1.3.5 Directness

The principle of direct election requires that there can be no intermediaries in the process of voting decision. This principle may be also adapted to fit with an e-voting procedure. The relevant requirement is that each and every online ballot is directly recorded and counted.

A problem may arise in case the voting period differs from the voting procedure (on-line or off-line) used to cast the vote. Online voting results may influence the outcome of the entire election process and limit the integrity and legitimacy of the whole process. To avoid this, a system can be developed allowing the recording and maintaining of the cast vote, while prohibiting any counting before the end of the (off-line) voting period.

1.3.6 Democracy

A democratic e-voting system should at least meet the requirements of a traditional election system. However, additional requirements should be also met, particularly due to the remote nature of e-voting. These requirements pertain to the preservation of attributes and properties such as transparency, accountability, security, accuracy and legitimacy of the system. E-voters should be able to understand how the elections are conducted. The traditional voting procedures operate in a way that is transparent to both, the voters and the other election actors. On the contrary, e-voting procedures are not transparent because the average voter does not have the knowledge necessary to understand how the system works. Therefore, in e-voting much more trust in the technology used and the persons involved (election officials, technology providers, etc.) is be required by the voters.

Verifiability conflicts with transparency. An e-voting system should allow its verification by voters (individual verifiability) or by election officials, parties and independent observers (institutional verifiability). However, verifiability is orthogonal to secrecy (confidentiality), in the sense that individual verifiability (i.e. the possibility of a voter to verify his vote and receive confirmation about casting and counting of the vote) is conflicting with the requirement of secrecy (as a condition of free choice).

Accountability is an additional requirement of an e-voting system, which is meant as the logging and monitoring of all operations related to e-voting.

Reliability and security requirements are derived by the democratic need, to ensure that the outcome of the election reflects correctly the voter will. A reliable system should ensure that the outcome of the voting process corresponds to the votes cast. The ballot that is transmitted

to the voting counting equipment should be an accurate and not modifiable copy of the voter choice (integrity). Moreover, it should be infeasible both to exclude a valid vote from the tabulation and to validate a no valid one.

Security is a multidimensional notion in the context of e-voting. Security refers mainly to the technically guaranteed respect of confidentiality (secrecy), integrity and availability, but it also refers to a whole range of functions and election components, such as registration, eligibility and authentication. The e-voting system should be protected against accidental or intentional denials of service and be available for use whenever it is expected to be operational. Unavailability of the system (or of one of its components) may result to loss of the capability of a voter to exercise her fundamental political rights.

E-voting systems are inevitably complicated. Furthermore, they usually involve more actors than a traditional system. From the point of view of the voters, the system should be easy to use and should require no particular skills. Therefore, an e-voting system should be developed in such a way as to facilitate its usability and to preserve its controllability.

Simplicity and accessibility of a system are not merely technical issues. Proper training and election processes re-engineering (e.g. help desks, e-election officials, etc.) are required to fulfill these requirements.

Based on the above principles, the following requirements are derived: a) there should exist trusted certification procedures for hardware and software, b) the entire infrastructure, as well as any system functionality, must be logged (e.g. all non -interface software should be open source), c) all operations (authentication, vote recording, etc.) should be monitored, while secrecy is preserved, d) the infrastructure should be open to inspection by authorized bodies, e) voters, parties and candidates should be ensured that there has been no malpractice, f) adequate system security must be ensured, g) the system must be simple and user-friendly.

1.4 Project Objectives

The basis of this project is to create an electronic voting machine that will help to eradicate defrauding of the manual voting systems and prior versions of electronic voting. This e-voting system provides a voting service that allows people to vote from booth using authenticate finger through the fingerprint sensor. The primary goal of the project is to make a system that requests the voter to give his fingerprint through the fingerprint sensor. The biometric voting system reads the fingerprint's data and compares it with the data previously stored. If the data is matched, the voting system will enable the voter to enter into the voting system and give his vote. If the data of the finger did not matched with the stored data, then the system will instantly on the buzzer and display shows the invalid notification and the authorities will come to take an action. Some objectives of the project are:

- To ensure overall accuracy.
- To ensure voter privacy.
- To ensure vote verifiability.
- To ensure receipt-freeness to some extent.
- To stop fake voting.
- To make sure that every voter can give his/her vote to their favourite candidate.
- To reduce the sufferings of the people who are in duty of a vote center.
- To reduce the time of overall voting process.

1.5 Report Structure

There are 6 chapter of the dissertation. The structure of this report is as follows:

- Chapter 1 introduced the idea of "Biometric Voter Authentication, Vote Casting and Counting & Ensuring Vote Verifiability" in Electronic Voting System.
- Chapter 2 describes the Existing Voting System.
- Chapter 3 describes the Importance of EVM in the Context of Bangladesh.
- Chapter 4 describes the Methodology of our proposed EVM.
- Chapter 5 illustrates the Results.
- Chapter 6 describes conclusion and future plan.