SECURE WEB BASED VOTING SYSTEM FOR THE CASE OF ADDIS ABABA CITY

BY

AMHA BIRRU

A Project paper submitted to the School of Graduate Studies of Addis Ababa University in partial fulfillment of the requirements for the Degree of Masters of Science in Computer Science

March, 2007

Addis Ababa University

School of Graduate Studies

SECURE WEB BASED VOTING SYSTEM FOR THE CASE OF ADDIS ABABA CITY

BY

AMHA BIRRU

Department of Computer Science

Approved By,

Dr. Mesfin Belachew(Advisor):_____

Table of Contents

List of Figures

List of Tables

Abbreviations and Definitions

PIN: - Personal Identification Number

PSN:- Poll Station Number

CIN:-Citizen Identification Number

JDK:-Java Development Kit

SSL:-Secured Socket Layer

HTTPS:--Hyper Text Transfer Protocol over Secured Socket Layer

MD-5:-Message Digest Algorithm

DES: - Data Encryption Standard

SHA-1:- Secured Hash Algorithm

JAVA_HOME:- Installation folder of JDK

J2EE-Java 2 Enterprise Edition

JCA-Java Cryptography Architecture

Pass-Phrase: - String which is used as an input for generating encryption/decryption key

Hash: - A hash is one way function that is hard to get its inverse

Key: - Key is a combination of bits values which are used for encrypting/decrypting a plain text

GUI:-Graphical User Interface

JVM:-Java Virtual Machine

API:-Application Programming Interface

JSSE: - Java Secure Socket Extension

CA: - Certificate Authority

WTP: - Web Tools Platform

JSP:-Java Server Pages

JDBC: - Java Database Connectivity

TLS: - Transport Layer Security

Acknowledgement

This project work is done not only by my effort. It has got an input from different individuals. First of all, I present my thanks to my advisor, Dr. Mefin Belachew, for dedicating his time from the start to the end of this project; the department of Computer Science, on confirming the proposal of my project and facilitating conducive environment for the work; Ato Tesfaye Mengesha, from Ethiopia Election Board, helps me to get information about policies of Ethiopian Election rule; last, but not least, to all my friends who gave me comments on my work. Without the contribution of these people, my work would not be successful. I would say once again **Thank You** to all of you.

Abstract

The intension of this project is developing a supplemental voting system for Ethiopia, particularly to Addis Ababa City. The current mechanism for handling the vote management system of the country is limited on manual work. This has limitation on controlling the work securely, for declaring the result on time, and has high consumption on resources. Many countries have used different technologies to support their voting activity and have got successful results. Electronic voting is the most known technology for voting from the existed alternatives. This project proposes a web based electronic voting. The experience of other countries is used as an input for the system. The requirements for the system are collected from historical records and policies of the Ethiopian election. The system architecture, the security risks, and the implementation details of the system are also included in the document.

1 Introduction

Nowadays, the application of ICT is introduced at several domains of fields. Its' multidimensional benefits is becoming more visible from time to times. The economical benefit gained from the technology is the most significant one. Further more, it helps to increase the qualities of the work, reduces the complexities of tasks, keeps the security of data in most favorable condition, makes data transfer more easy, and others.

ICT role is wide, starting from low level systems to high level business and governmental applications. The business applications are used by business people to manage the business process; e-commerce can be taken as one example that shows the application of ICT to the business community. Similarly, ICT can play its role for governmental applications. Election is one of the tasks of the government that can be benefited from ICT. Electronic voting is common in several countries, but not known in Ethiopia till now.

This project initiated to start an initial work on e-voting for Ethiopia that can be extended in the future. The project does not have a plan to totally replacing the existed paper based voting methods. But rather, for supplementing the existed paper based vote casting with ICT. There are countries which are using both the paper based and electronic based vote casting system for one election process. For instance, Switzerland has managed its voting system both by electronic and with the manual method at one time [2].

One of the challenges for e-voting is identity identification issue. In the current voting system of Ethiopia, identity card is used for identifying the individuals and ink for separating voters who have given their vote. It is possible to use this traditional individuals' identification mechanism to e-voting as well. But the methodology has problems; it didn't address the problems very well that are raised related with

uniqueness identification. For example, it has lesser capability to protect voters from registering at more than one place. This system proposes alternative technology that can minimize uniqueness identification problems seen on the current voting system.

Many countries have automated systems that can help to uniquely identify its citizens. For instance, USA uses Social Security Number (SSN) for this purpose. In Ethiopia, there is no such strong uniqueness identification system. This project considers the case by assuming that there is automated system that facilitates citizens' identification task, which is an external system that communicates with this system through the network. If this methodology is employed, it can minimize double voters registration problem, reduces age related problem for electors, protects those which are not eligible to cast a vote due to court related cases, identifies localities of individuals very well, etc.

The rest of the document is organized in such a way that, chapter-2 describes about the review work. In chapter -3 and chapter 4 the requirement analysis and the system design of the document respectively, chapter-5 describe about the implementation of the product, finally chapter 6 and chapter 7 describe; summary and conclusion of the document respectively.

1.1 Problem Statement

In most cases, computer programs are developed for handling daily routine tasks. But voting process is not an everyday task. In Ethiopia, it is conducted within every five year. However, the volume of the work is massive and wide. The current system used in Ethiopia for this purpose is manual starting from the registration process till the vote counting stage. It is complex and error prone task. The material cost required for managing the whole vote process is also high. The time for declaring the final result will also be beyond the schedules. Moreover, it seeks strong security system. By considering the complexity of the vote management system, many countries have been automating their voting process, and have gained successful result.

Therefore, implementing the state of art technology for Ethiopia that can reduce the major problems seen on the paper based vote casting system is necessary. The technology is tried in many countries and brings significant changes. And this project targets to do an initial work on the area that can be extended in the future.

1.2 Major Challenges of Web-based Voting System

- Protecting double vote casting
- Maintaining uniqueness of voters
- Establishing secured private network infrastructure that reaches to at each of the polling stations
- Identifying major security risks and addressing them
- Exhaustively testing the system to make sure its reliability

1.3 Objective

General Objective

The main objective of the project is producing an electronic voting system that can supplement the current paper based voting system of Ethiopia.

Specific Objectives

- Designing the system architecture of the system
- Designing back-end database to the system that can hold all the information
- Designing friendly user interface
- Implementing standard security algorithms that can keep the confidentiality of the data at rest as well as at communication lines
- Selecting the appropriate development tools for the system
- Integrating the whole system
- Testing the system
- Documenting the whole system

1.4 Scope

The scope of this project is developing e-voting system for Ethiopia, specifically to Addis Ababa City that can be extended in the future. There are different kinds of electronic voting system in the world, but this project targets to do web based e-voting system. The system contains modules that can handle voters' and candidates' registration system, including vote counting module.

1.5 Methodology

The following are some of the main procedures that are followed to work the project;

- Assessing the experience of other countries that have used electronic voting
- Studying the current voting system of Ethiopia to get the requirement of the system
- Study the security risks of e-voting
- Study the current security technologies so as to implement in the system
- Assessing the available network infrastructure that helps for data transfer

2 Related works review

To support the idea of this project, similar works on the area have been assessed in country as well as in foreign countries. There is one paper which is done for academic work at Addis Ababa University, Technology Faculty, in Electrical and Computer Engineering department, which tries to address problem of vote counting in a fixed audience. The objective of the work was automating the existed audience gathering system which is currently handled by counting raising hands in the Ethiopia parliament system [1]. The work is supported by hardware devices. However, the purpose, the application area, the technology used, and the requirements, are different from this project.

There are many countries that use electronic voting system effectively at various times. In October 2001, Australia has made parliamentary election for 16,559 voters to cast their vote electronically at four polling stations. Since 1999, Belgium has made general and municipal election. By 2000, and 2002 in Brazil, more than 400 thousand electronic machines are used at the nation wide. From November 5 to 10, 2003, Canada had made elections for 12 municipalities using Internet and phone with out using paper ballots. In October 2005, Estonia had made local elections using Internet as one means to cast vote and was declared a success by the Estonian election officials. In September 2000, Sweden, France and Germany tried an on-line election which was sponsored by European Commission to Cyber Vote project. In 2003, India had made all state elections held using electronic voting machines. In 2003, Norway had carried out pilots in three municipalities at local elections using voting machines in the polling stations using touch screens. In 2003, 2004, and in 2006, England had made voting pilots [2].

The next section summarizes the technical experience of two countries which have very near similarity to this project. The first one is the case of one of the states of UK, Stratford-upon-Avon district, for May 2003 of local government election to electorate of 100,000 voters; and the second is the case of Dutch government for 2002/2003 election.

2.1 Case of Stratford-upon-Avon District [7]

Overview of the work

Stratford-upon-Avon is one district in UK. In the district, Postal voting is an alternative to the expatriates to cast their vote for the local government election of the district. Since the postal voting was becoming insecure to cast a vote, the local government was looking for better technology that replaces postal voting. After looking the experience of other countries, they planned to replace postal voting with Internet voting. Because, it was thought that, Internet voting will bring better advantage compared to postal voting with regard to security and manageability of the whole process. i.e., the vote cannot be observed in transit or in storage before it is counted and the counting process can also be processed automatically.

The local government of Stratford-upon-Avon was committed for the change, and one online voting application is developed. Before using the application the local election commission made an amendment on the electoral policy so as to permit vote casting via electronically. Then, training is provided to the eligible voters and the application was getting into operation for handling the vote casting by replacing postal voting method.

The application has a friendly graphical and interactive user interface. The online voting system has more than one ballot built into it. When the voter accesses the system and logs in, the system offers the right ballots based on the electoral enrollment of the voter. The software that runs the actual election is very small; it is just a simple pair of programs, i.e. the server and the client side browser.

The application generates the required reports at the close of the polls. Then the election office publishes the report of the election over the Internet to voters. This is done by

replacing the content on the voting website. In this way, voters can check back the result shortly after the close of polls to get an instant result.

Security Technique

The user interface protects the voters from action that is prohibited by the electoral rule. If more candidates or few candidates are chosen, which is against the Electoral law; the user interface displays an alert message. This helps the user to correctly cast a vote.

The other security tool used in the application is cryptography. Cryptographic keys have been used to lock the votes submitted in the ballots (data storage server). The votes will not be unlocked before the counting process finished. This is done by using public key cryptography technique. One or more election officials and observers contribute pass-phrase which together combines to give access to the created keys. The public key is sent to the voter to encrypt the ballot, and the other key is kept by the election officials to decrypt the votes.

Voter identification is done with three attributes, i.e. the Registration Number (RN), the Ballot Number (BN), and the PIN. These attributes are modified when submitted to the ballot for the sake of keeping their security. They are used to authenticate the voters .The election office of the district allocated these numbers to the voters at the registration date.

Result

The author of the report states that the result was successful. One of the reasons for the success can be that the citizens of the district has access to modern technology and 60% of the citizens have web access ,and the network infrastructure used to execute the application was private network, which is accessed only by specified target group and has great contribution to the security of the system.

2.2 Case of Dutch Government Election [8]

Overview of the work

The kiezen Op Afstand(KOA) system was a remote voting system developed for the Dutch government in 2003/2004. The introduction of such a system was not a radical development for the country, because Electronic Voting Machines (EVM) was already introduced in the Netherlands around 1998.

However, due to the increasing insecurity and unreliability of the existed EVM, the Dutch parliament seeks a better technology for voting. The need of electronic voting is coming from the government parliament. It was seeking for better technology for development of Dutch voting system. After seeing all the technology used in the world, remote voting through an Internet selected as the preferable choice to handle the voting process of Netherlands.

The application was tested as a pilot project for the expatriates to vote in the election to the European parliament via the Internet. It was executed by replacing the oldest postal voting process. Dutch national election law was explicit to how votes may be cast. In order to conduct an experiment on voting over the Internet, some amendments to electoral law of Dutch was necessary, and the amendment is done very soon. This formed the legal foundation for the project, then election to the European parliament of June 2004 allowed remote voting via the Internet. The application was used by expatriates who were required to explicitly register beforehand. It was thought that such a small scale use (thousands of voters) would provide a useful real world test for the technology. The application was tested on a small scale (thousands) voters, this can be used to execute the application in wider scale.

Security Technique

When a voter registered to cast his/her vote, PIN is given to the voter for authentication. The registered voter can login to the system with the help of the PIN code. Then, the system shows the check box, names and party symbol of the candidates. The voter checked the check box corresponding to each candidate and submits his/her vote to the system.

Communication between the browser and the web server is secured with Secured Session Layer (SSL). All votes are stored in a double-encrypted fashion, i.e., each vote is encrypted by a symmetric key stored in the system, i.e., SSL and again by the public key of the voting authority.

The power to change the state of the system and to decrypt the votes is restricted to a small number of polling station officials. These officials hold the private key for the system and each has PIN code to use this private key. In order to decrypt the votes all the officials must enter their PIN code.

Result

Since the application has problems on the area of security, it was not executed to handle the real elections of Dutch government. The major problem was security. The communication line was insecure, and denial of service was one of the major problems. The network infrastructure that was used for the data transfer was public network. This has contribution for the unreliability of the system. The security of the system is tested by expertise and fails to satisfy the security requirement of the system as expected. Finally, the system is taken to laboratories for further study.

2.3 Lessons Learned

Many countries have used electronic voting system for state level elections and some for the whole nation. This will give us confidence to test it for our country. The two countries experience mentioned in section 2.1 and section 2.2 have contributed good input for this project. The technical details like security, business process, and user interface construction are the major ones.

Many countries have made an amendment to their election policy. This is done just for the purpose of executing election by electronic means. It is also an issue for Ethiopia; and will be left for the policy makers for consideration.

There are countries that have tested electronic voting as a pilot project in small size, i.e., state level election. This has a great contribution to strengthen the idea of this project. The scope of this project is specified only for one region, Addis Ababa City, which has an equivalent meaning to the word state in other countries.

Before doing an electronic voting, there are some countries who have studied the culture of their society, the distribution of the technology, the access of the society to the technology, and other studies have been done. This helped them to predict the viability of the application as well as for their project plan. This also needs to be considered for Ethiopia in future works.

3 Requirement Analysis

The requirement analysis is divided into three sections; the first section highlights the general requirements of online voting applications. The second section details the specific requirements of the system, i.e., the functional and non functional requirement.

3.1 General Requirement

A Web based voting application created for elections requires to offer ballots, collect votes, warn the voter of incorrectly filled ballots, issue a confirmation message and encrypt the vote. It is important to note that there is no easy way by which to easily decrypt voters' votes. The strength of the encryption is derived from the strength of standard security algorithms that the system implements [1]. The electronic vote in polling stations, with votes' transmission through an electronic infrastructure has to guarantee the confidentiality, integrity and availability of the system [9] [5].

The transmission of personal data through a network that connects online polling stations does not provide enough guarantees, unless the transmission is done in a secure private network. Internet based approaches have been criticized for reasonable and sometimes proven security concerns due to the fact that an open network is always vulnerable to hackers attack[7][4]. Solutions based on private networks should be enforced with strong security layers pose as more viable approaches to implement reliable and strong secure e-voting systems.
The integrated computer and communication systems performing all functions from collecting the voters' choice and transmitting and counting process should be done securely.

In addition, the database which holds the voter and candidate details should also be protected by a firewall, housed on separate servers, with their identity hidden from all.

Some of the more sensitive information held on these databases, such as ballots and voter identification data should be additionally encrypted to protect both the integrity of the ballot and the privacy rights of the voter. It is in this way that a ballot can be cast by a voter with the confidence that even a security breaches occurs on the database server, they and their vote would be kept anonymous.

3.2 Specific Requirement

The inputs for the specific requirement of the voting systems are based historical information, organizational policies (see Appendix-1) and constraints. This section will list down the functional and the non- functional requirements of the application. Then, the interaction between users of the voting application and the system is depicted using case diagrams (see Fig.1).

3.2.1 Functional Requirements

The following points list down the functional requirements of the system.

- **Maintain Policies:** The election officer has to set the maximum number of votes given for parliament and regional candidates based on the policies of the election rule.
- **Create Pass phrase**: The election officer has to create the pass phase in the system. The encryption/decryption key is generated from the pass phrase created in the system.

- **Create Polling Stations**: The election officer has to create the codes of the selected polling stations before the vote casting process begins.

- **Check eligibility to cast a vote**: When the voter registers to cast a vote, the system will check whether the user is eligible to cast a vote or not.

- **Create Candidates**: Before the vote casting process begins, the registrar needs to create the candidates

- **Create Registrars**: Before the registration process begins, the election officer has to create the username and password of the registrars.

- **Register Voter**: After the eligible registrars are created, the registrar will register the voters.

- **Login***:* The registrar, the voter, and the election officers have their own credentials stored in the database. The system will check the keyed values against the values stored in the database.

- **Cast Vote:** When the voter keys the correct PIN and poll station code to the system, the system will extract the eligible candidates on that polling station, then, the voters casts the vote by keeping the rules.

- **Generates Report:** At the end of the election, the election officer will generate the reports based on the polling stations code.

3.2.2 Non functional Requirements

The non-functional requirement describes constrains for implementing the project. Some of them are; the central server have to be provided at secured area, the system must be maintainable and expandable, the network infrastructure have to be private network, client machines at each of the polling stations must be installed. In each of the polling stations there should be technically supporting people. The voter should have also basic computer skills and training should be provided to the voters on the demo version of the voting application. The input value which is used to generate the encryption key must be provided from the election officials, and needs to be kept securely, and others.

3.2.3 Use case Model

The vote application is accessed by four actors; i.e., the registrar, the voter, the election officer and the external system. Their interaction with the system is shown in Fig.1.

The Election officer accesses the system for different purposes; i.e., for maintaining the polices that can be enforced in the system , for creating the pass-phrase which is used to generate the encryption/decryption key, for creating polling stations, registrars and also for generating final reports.

The registrar role is limited on registering the eligible voters at each of the polling stations. The user name and password for each of the registrars is created by the Election Officer. After the registrar logins to the system successfully, he/she registers the eligible voters coming to that particular polling station. Then the voters' information will be sent to the central server.

The other user is the voter; the only interaction permitted for the voter with the system is vote casting. The system proposes CIN for uniquely identify voters. It can be used as the PIN number to the voter, and PSN together with the PIN helps to login to the

system. Based on the PSN keyed by the voter, the list of candidates registered at that particular polling station will be retrieved from the database and displayed at the desktop screen. The Check boxes will appear along with the candidate's name and party symbol. Then, the voter can check the checkbox of his/her choice of candidate and submits it to the system.

The system will also interact with an external system. The external system is database system that holds information about citizens besides to the CIN. Our system will interact with the citizens' database to confirm that whether the voter can register to cast a vote or not.

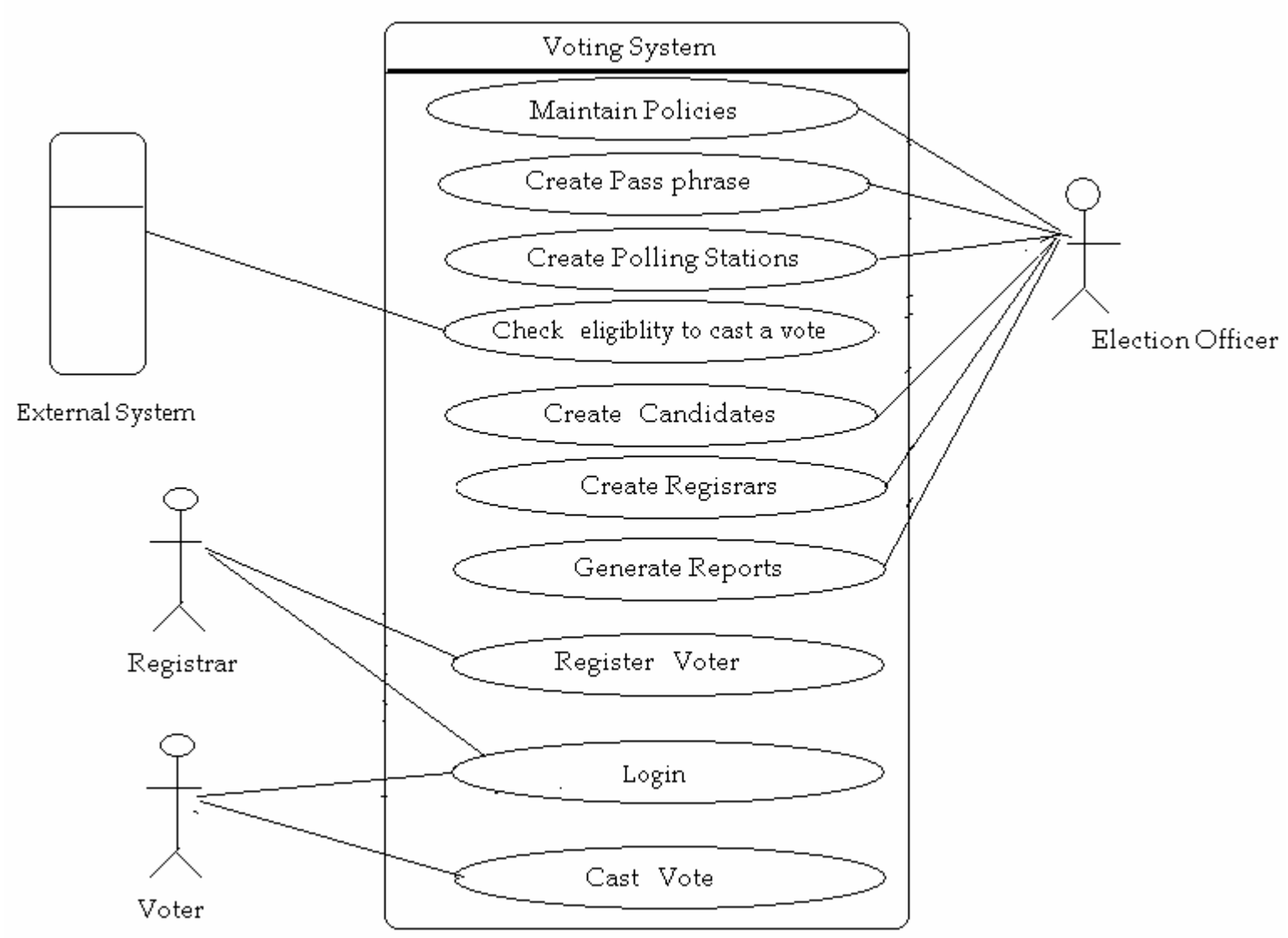

Fig.1 Use case Diagram

4 System Design

This section describes about system architecture, the database design, the targeted network infrastructure and the security risks of the system

4.1 Architecture of the System

The architecture chosen for the system is three tier. The first layer runs on the client side, the second layer at the middle layer and the third layer will be the database system. The system will run using web technology. This architecture provides greater application scalability, high flexibility, high efficiency, lower maintenance, and reusability of components. Since each tier runs on a separate machine, it improves systems performance.

The system uses dynamic web technology, i.e., adding and retrieving data to and from the data store whenever requested is possible. It requires a client side program which is accessed by the Election officer, by the registrar, by the voter and also an interface that communicate with the external system. It needs server side functions that implement the functional requirements and the database system that stores data.

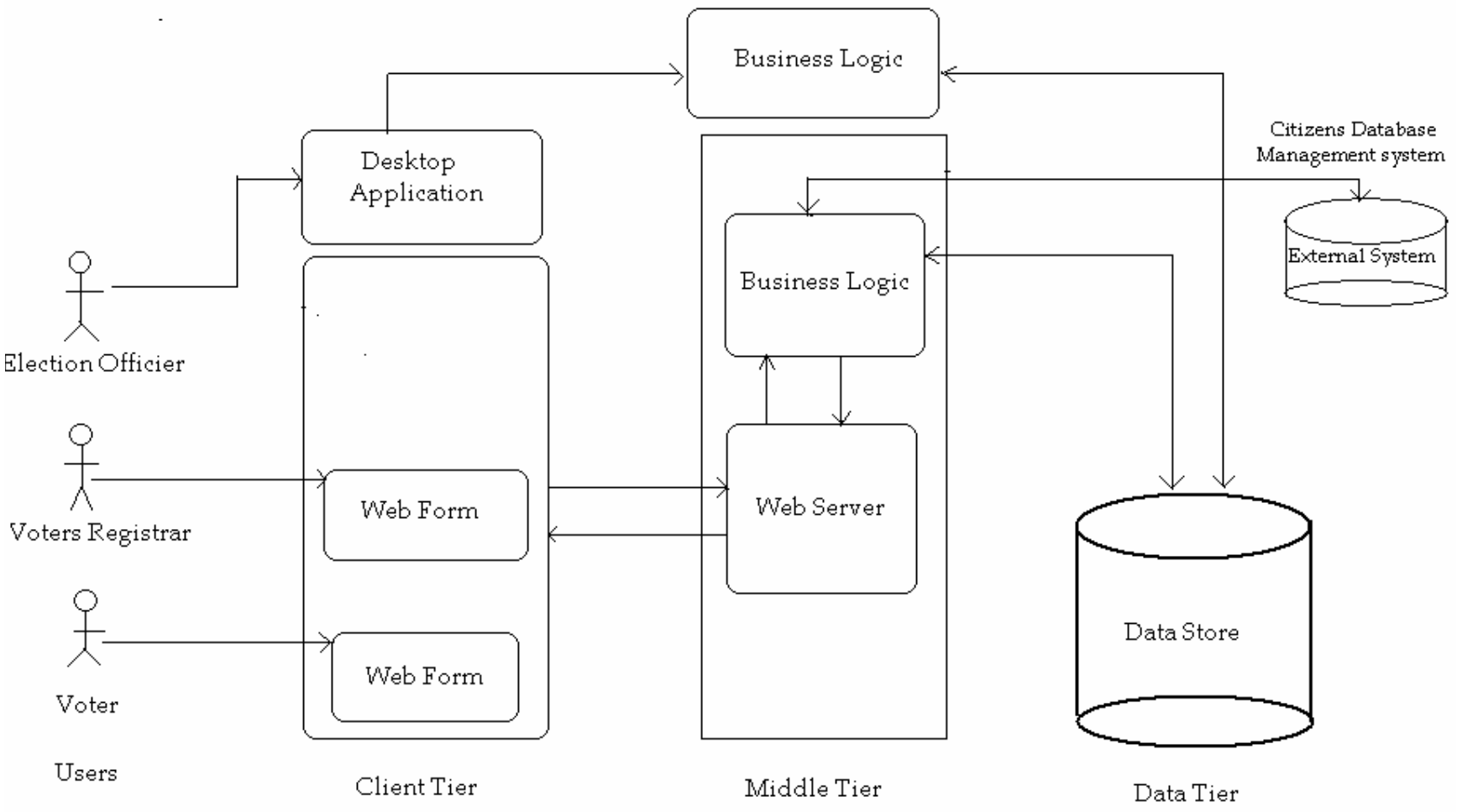

Fig.2. System Architecture

Client Tier

As shown in Fig. 4, at the client side there are three kinds of users. The first user is the Election Officer. This person is responsible for adding critical data to the system, the type of data is like candidates' credentials, registrars' username and password, election rules and pass-phrase that help to generate encryption/decryption key. The final report is also generated by this person. The type of application used by the Election Officer is also different. The application has to be standalone application that will not be accessed by the web browser due to security reasons. The desktop application has its own business logic, which is isolated from the web application. The reason is, the two applications are executed on their own timeline, i.e., the desktop application is running first for initializing the database with preliminary data like pass-phrase text, and at the end of the election for generating reports; where as the web application is used to handle the voters registration and the vote casting process. But, both the desktop application and the web application share the same database.

The second user of the system is the registrar. The role of this person is registering the eligible voters. The privilege to access the system is given by the Election Officer. The interface accessed by the registrar is web form. The reason is because; registration is expected to be processed at each of the polling stations. The polling stations are found at different geographical location, far away from the central database.

The third user is the voter; the role of this voter is casting votes. The interface used by the voter is web form. As vote casting is processed at the polling stations, which are distant from the database server.

Middle Tier

The middle tier will contain the core parts of the vote application, i.e., the web server and business logic. The web server will handle all requests coming from the client machines. The requests are different with its type, for example; request for data insertion, request for report generation and others. It is also the web server which manages the responses that is forwarded to the client machines.

The business logic part will hold the process and core functions that will be implemented in the system. All the list of function stated in the functional requirement (section 3.2.1), will be coded in this section. When the data is submitted from the client machines, first it will be handled by the functions of the web server and then transferred to the business logic for processing. Again, the business logic processes the data and sends it either to the database or back to the web server, this is determined by the type of service required.

Data Tier

The system uses two databases. The first database is the one which stores information about citizens. This database is not part of the system; it is referred from an external system. It stores citizens' information like CIN. The CIN number is the unique number that is used for identifying citizens. The application can also benefit from this for identifying voters uniquely.

The second database is the repository consisting of the application data. It is here that all the database tables will be stored.

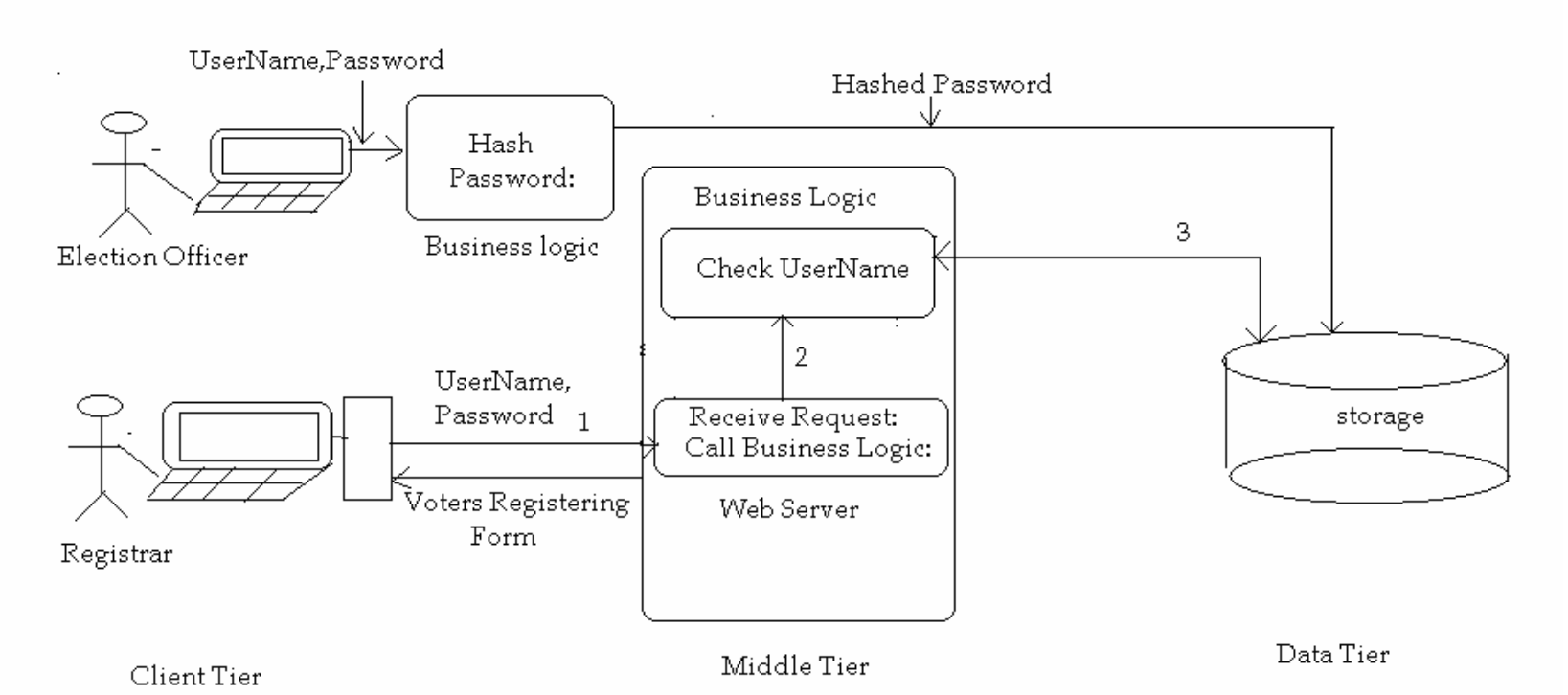

Fig.3.A Single Scenario Showing Interaction of the 3-layers

As shown in Fig.4. , the scenario shows the interaction of the client tier, the middle tier, and the data tier. The Election Officer creates the registrars user name and password. At the business logic, the password will be hashed, and the data goes to the data storage. The Election Officer has no interaction with the web server, because the application is runing only on desktops.

When the registrar wants to register a voter, he/she will login to the system using the user name and password created by the Election Officer. Since the registrar login form is dynamic web page, the request is directly sent to the web server. The web server calls the function in the business logic that hashes the password and checks whether the given user name and password matches with user names and passwords stored in the database. If it matches, the web server opens voters' registry form. Then the registrar can proceed registering of the voters.

4.2 Database Design

This section describes, first the Entity Relational diagram that will be used to design the database part of the system. Second, the architectural design, and lastly it describes about the network infrastructure required for the system.

4.2.1 Tables

As shown in Fig.2, the database will consist of several tables. The tables are used for storing the attributes of voters, candidates, polling stations, votes, pass-phrases and election rules. The design is constructed to be used for both the parliamentary and regional elections.

To read the attributes of the tables easily, the following abbreviations are described as follows.

Abbreviation	Description
PEVotes	Parliament Encrypted Votes
REVotes	Regional Encrypted Votes
PDVotes	Parliament Decrypted Votes
RDVotes	Regional Decrypted Votes
CPIN	Candidates Personal Identification Number
CCN	Candidates Constituency Number
VPSN	Voters Polling Station Number
VPIN	Voters' Personal Identification Number
VFirstName	Voters' First Name
VLastName	Voters' Last Name
VRegDate	Voters' Registration Date
CPIN	Candidates' Personal Identification Number
CFirstName	Candidates' First Name
CLastName	Candidates' Last Name

CPSN	Candidates' Polling Station Number
CRegDate	Candidates' Registration Date
PSN	Polling Station Number
PSName	Polling Station Name
PMaxVotes	Maximum votes for Parliamentary Candidates
RMaxVotes	Maximum votes for Regional Candidates
PMinVotes	Minimum votes for Parliamentary Candidates
RMinVotes	Minimum votes for Regional Candidates

Table .1 Descriptions of Database Table Attributes

There are four tables with the same attributes (see Fig.2), i.e., PEVotes, REVotes, PDVotes and RDVotes. The PEVotes and REVotes tables will hold votes submitted to parliament and regional candidates respectively. CPIN and VPSN are two of the attributes in these tables, which are stored with encrypted format. But at the end of the election, the content of PEVotes and REVotes table will be copied to the corresponding PDVotes and RDVotes tables by decrypting the encrypted attributes in the previous tables. The content of both PDVotes and RDVotes will remain empty until the votes become decrypted.

The voter table will consist of VPIN, VFirstName, VLastName, VPSN and VRegDate. The VPIN will uniquely identify each record of the voters .This attribute will be stored by converting its value into hashed format. The reason of hashing the VPIN is to hide its identity. In case, if an attacker gets the chance to access the database, it will be difficult to use the PIN. The voter table will be associated with PEVotes and REVotes tables with one-to-many relation. This is because with one VPIN, the voter will give votes for more

than one candidate, i.e., at least for one parliament candidates and for more than one regional candidates.

The Candidates table will consist of CPIN, CFirstName, CLastName, PatrySymbol, CCN and CRegDates. The CPIN attribute is the primary key which will uniquely identify each of candidate's record. CCN represents the constituency number where the candidate registered. In one constituency, there can be many polling stations. This tables associates with the PEVotes table with one-to-many relationship. This is to enforce that with one CPIN, so many votes can be given.

Similarly, PollingStation table will hold PSN and PSName for identifying the selected polling stations.

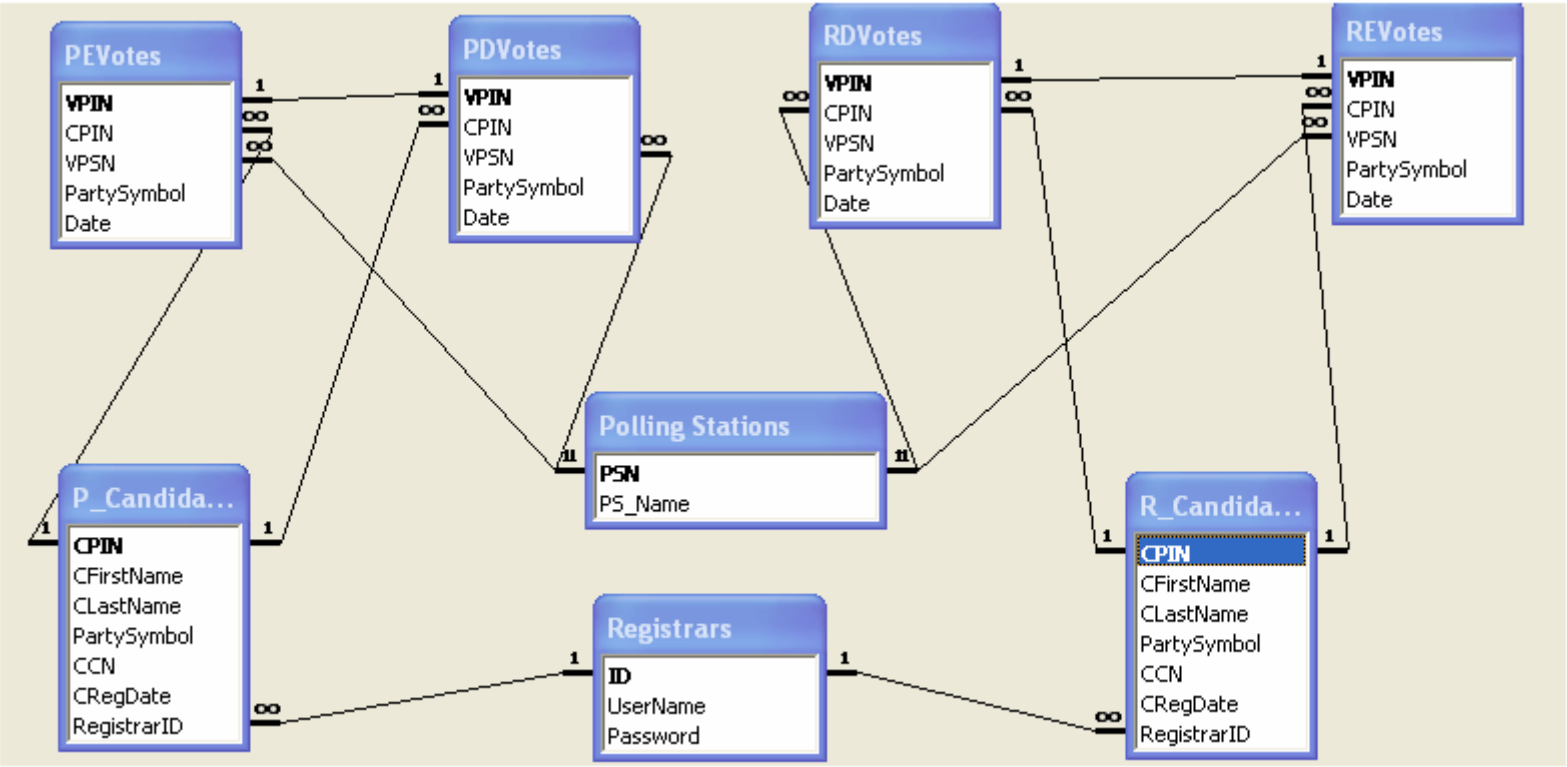

Fig.4. Database Design

4.3 Network Infrastructure

Election is not a daily activity for any country. The same is true for Ethiopia. It is not economically worth to consider a separate network infrastructure for handling the vote management process that is executed once in five years. So, it is better to consider reusing already existing network infrastructures like WoredaNet.

The application is targeting to use network infrastructure that is secure, cost effective, and expandable and that has the potential to execute the requirement of the application. Currently, WoredaNet network is the ideal existing network infrastructure, which is administered and owned [12] by the government and suitable for this application. In addition, since it is extended to all the Woredas of the country, it makes the application realistic to use this infrastructure for the whole nation in the future.

4.4 Security Risks

Vote secrecy is limited by many factors outside the election system, so that, a practically zero probability of security problems in the election system itself, even possible, may not be required [6]. Instead, a notion of security enough, a bound on the number and pattern of compromises of security that are rare and limited enough not to endanger the general integrity of the process.

When considering the three tier architecture, the system components are found distributed physically at different machines. The user interface part is found on the client machine (client tier), the business logic and the web server on another server (middle tier) and the database is found on a different machine (data tier). When the information is recorded or transferred from the client machine to the application server, and then to the database server, or at the database, its security can be violated.

The first possibility for committing an attack may occur during registration of the voters. While the voter registers, some body else who is found near the registration place can look at the screen and could take the PIN.

As shown in Fig.5, the problem of the second and the third case is similar. The suspected problem is man-in-the-middle attack. Before the data reaching at the destination, it can be trapped and modified. For the case of the channel between the web browser and the web server, SSL technology is viable solution. Description about SSL technology is given in section 5.1.2.1. For the channel between the web server and the data store, and also at the data store cryptographic algorithms is the possible solution, explanation about some of the cryptographic algorithms is also presented in section 5.1.2.2 and in section 5.1.2.3.

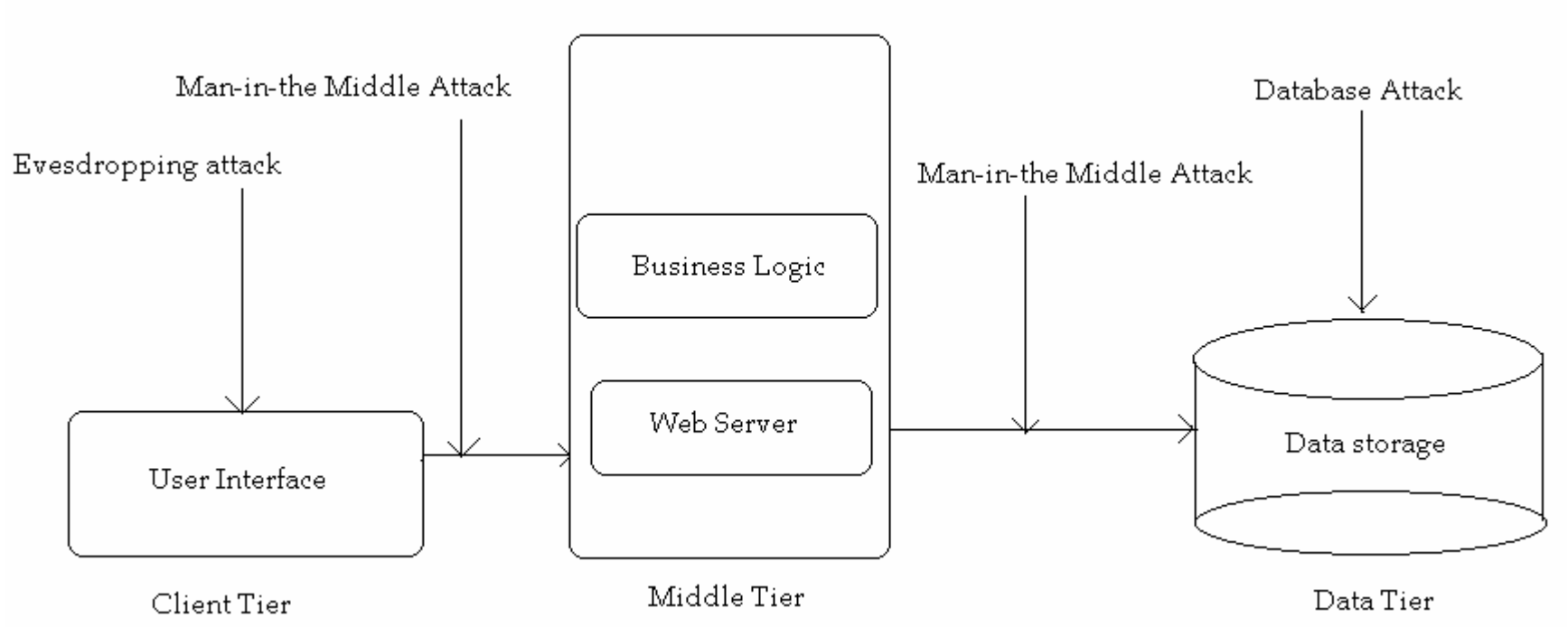

Fig.5. Possible Attacks on the System

5 Implementation

This section describes about the implementation of the product in two sections. The first section explains about the development tool, and the second section describes about the prototype of the system.

5.1 Development Tools

The development tools used in this section are described in two categories; the first section describes about the development and programming tools and the second part specifically describes about the security tools.

5.1.1 Development Environment

The programming language used for writing the code is Java. The reason for selecting Java is, it is object oriented programming language, which follows modern programming methodology. The edition used is J2EE. J2EE provides greater security, speed, reliability, improves development productivity, standardizes the platform, ensures portability of developed applications and supports component-based development of multi-tier enterprise applications [16].

As mentioned in the architecture of the system (see Fig.3), the system requires two kinds of applications. The first one is desktop application; consist of GUI and is developed using NetBeans. NetBeans is chosen as it has rich graphic tools with an easy drag and drop elements (Buttons, Textboxes, Labels).

The second application is web application. This part is developed using Eclipse 3.2, which is convenient Java programming tool for developing dynamic web applications.

Furthermore, it is freely available tool on the Internet, and suitable for developing multi-tier applications. Eclipse includes additional plug-in, called WTP, which helps for the dynamic web page development.

To avoid interface dependency problem, JDK version 1.5 is implemented. JDK contains the required tool for this purpose called, JVM. In addition, it also holds compiler and other security packages, which are source for security algorithms.

Application Server

The application server used for the system is Apache Tomcat 5.5. The reason for choosing Tomcat is because, it is a Java based Web Application container that was created to run Servlets and JSP in Web applications. Servlets and JSP are Java Web files. To communicate Apache Tomcat with the web editor (eclipse), the runtime environment variable, which is found in control panel, have been configured in such a way that the name of the variable is JAVA_HOME[1] and the value of the variable is Java_Home\jdk1.5.0_01.

Organization of Tools

The organization of some of the development tools is described in Fig.6. To describe the figure from bottom to top, at the first layer, the operating system is located. At the second layer the JDK platform is installed, this helps to avoid interface dependency to execute the application on any machine. At the third layer, Apache Tomcat web server is located, which handles the dynamic web pages, at the fourth layer, J2EE development environment and NetBeans IDE is located. At the last layer, the logics of the system have been coded.

[1] JAVA HOME is the name of the variable which indicates where JDK is installed

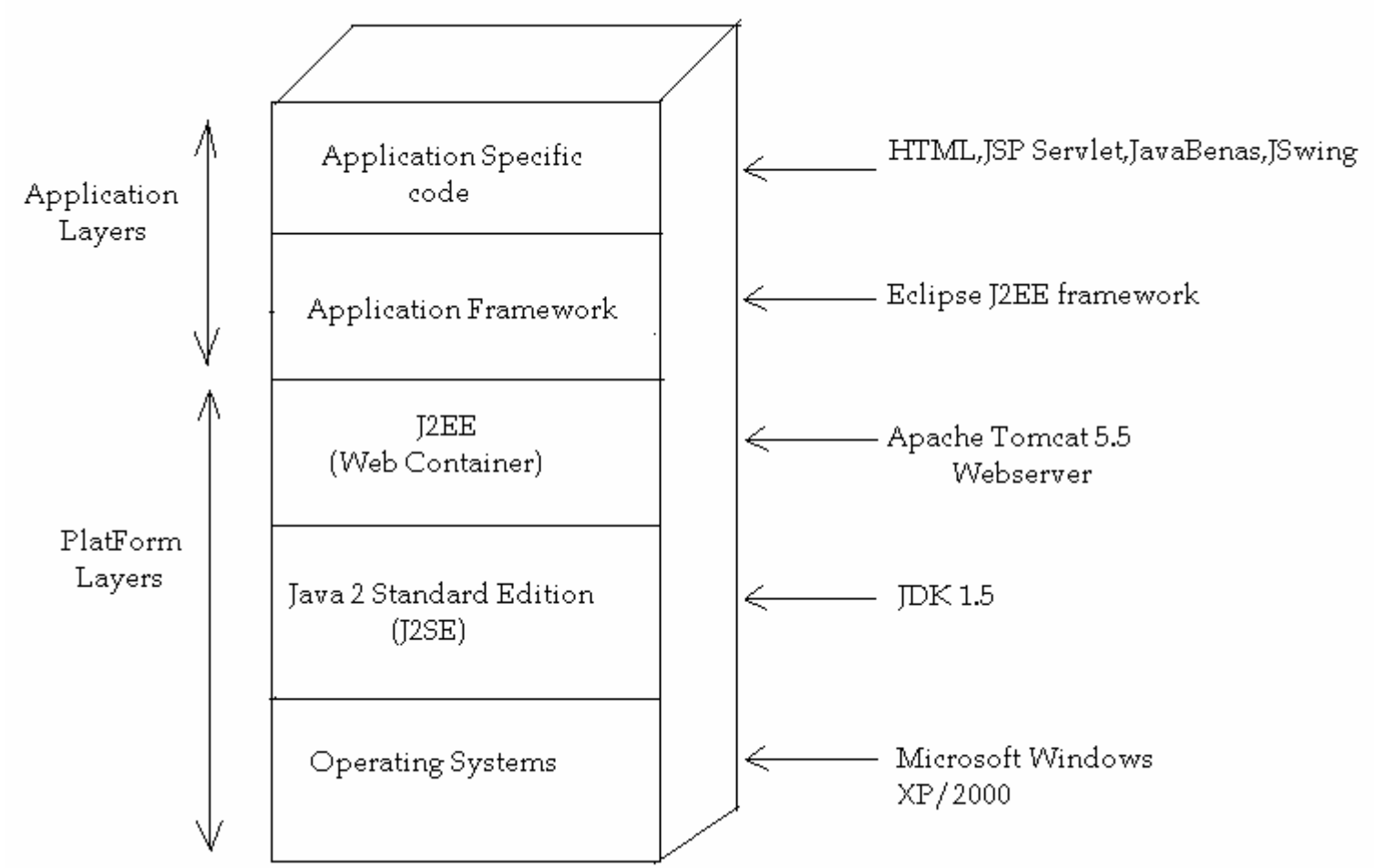

Fig.6. Platform and Application Layers

Database Management System

MySQL version 4.1 is used for managing the system database. MySQL has some better qualities which makes it preferable compared to the others relational database management systems. It is multithreaded, multi-user database management system, supports all known platforms including Windows-based platforms, requires less hardware resource for storage as well as for execution, much faster, supports Unicode character storage and more than that, it has free version product[17].

MySQL Connector/J is a Java packages, which is an implementation of the JDBC used to connect MySQL relational database server with Java. JDBC is the industry standard for database-independent connectivity between the Java programming language and a wide range of databases. MySQL Connector/J can be downloaded freely from the web. The package holds many files which are not required for our case, the file name which is required for us is, *mysql-connector-java-3.1.14-bin.jar.* This file must be placed in a folder Java_Home\ jdk1.5.0_01\jre\lib\ext\.

The system is adopted with Ethiopic characters. Visual Geez Unicode, which supports Ethiopic Unicode, is used for the system. The name of the candidates is registered using Unicode encoding. The candidates' names are stored in the database with Unicode format. This has great benefit for those who have difficulties on reading Latin characters, because the name of the candidates on the vote screen is shown by Ethiopic characters, which is retrieved from the database dynamically.

5.2 Security Tools

The following section gives a short description about the security tools used for the project. These are SSL, MD-5 and DES algorithm, and also about security packages and utilities which are sources for most of the security algorithms.

5.2.1 Secured Socket Layer (SSL)

SSL was developed by Netscape in 1994, and with an input from the Internet community, has evolved to become a standard. It is now under the control of the International standards organization called the Internet Engineering Task Force (IETF) [13]. The IETF has renamed SSL to TLS, and released the first specification, version 1.0, in January 1999. TLS 1.0 is a modest upgrade to the most recent version of SSL, version 3.0. The differences between SSL 3.0 and TLS 1.0 are minor.

Data that travels between the client web browser and the web server can easily be accessed by someone who is not the intended recipient. When the data includes private information, action must be taken to make the data unintelligible to unauthorized one. It is also important to ensure the data has not been modified, either intentionally or unintentionally, on the way. SSL protocol was designed to help protect the privacy and integrity of data while it is transferred in the line between the browser and the web server.

SSL is the most widely used protocol for implementing cryptography on the Web, and uses a combination of cryptographic processes to provide secure communication over a network. It is a secure enhancement to the standard TCP/IP sockets protocol used for Internet communications. As shown in Table.2, the secure sockets layer is added between the transport layer and the application layer in the standard TCP/IP protocol stack. The application most commonly used with SSL is HTTPS. HTTPS is a Web

protocol developed by Netscape and built into its browser .It is sub layer under its regular HTTP application layering [13].

TCP/IP Layer	Protocol
Application Layer	HTTP, NNTP, Telnet, FTP, etc.
Secure Sockets Layer	SSL
Transport Layer	TCP
Internet Layer	IP

Table.2. TCP/IP Protocol Stack with SSL

As shown in Fig.5. , there is a possiblity of reading and modifying the vote data while traveling across the channel between the client tier (web browser) and middle tier (the web server). At this particular channel, SSL protocol is implemented to secure data transmission.

5.2.2 Message Digest Algorithm (MD-5)

A message digest is also known as a cryptographic hash function [14]. It is basically a mathematical transformation that takes a message of arbitrary length, and transforms it into a string of bits, and computes the hash value from the bits. A cryptographic hash function does this transformation in a way that makes it extremely difficult to convert the hashed value to the original data. Cryptographic hash functions typically produce hash values of 128 or more bits.

There are several message-digest algorithms used widely today. MD-5 and SHA-1 are the most known algorithms, which are freely available on the web. MD-5 algorithm uses a key length of 128 bit where as SHA-1 uses 160 bit. SHA-1 is slower than MD5, but the message digest is larger, which makes it more resistant to brute force attacks

For this project application, MD-5 algorithm is implemented. The reason for selecting MD-5 is because of its speed. MD-5 algorithms is used for hashing the voters' PIN, when the registrar registers the voters, the PIN of the voters is hashed and stored in the

database. Similarly, when the voter enters the VPIN at the login form for authentication; it will be hashed and compared against the corresponding value already stored in the database. This helps to secure voter data transfer between the middle tier and the data tier, and also to keep its anonymity at the database (see Fig.5). For this application, speed is highly required to serve many voters within short period of time, where as MD-5 is much faster compared to SHA-1 algorithm and the application also need to have faster response time. Using MD-5 algorithms has an advantage for hashing some of security seeking data [14].

5.2.3 Symmetric Key Algorithm (DES)

Encryption is the process of transforming information to become unintelligible to anyone but to the intended recipient. Decryption is the process of transforming back the encrypted information to the original format. A cryptographic algorithm, also called a cipher, is a mathematical function used for encryption or decryption. In most cases, two related functions are used, one for encryption and the other for decryption. Encryption and decryption are done using a cipher.

With most modern cryptography, the ability to keep encrypted information secret is based not on the cryptographic algorithm, but on a number called a key that must be used with the algorithm to produce an encrypted result or to decrypt previously encrypted information. Decryption with the correct key is simple. Decryption without the correct key is very difficult. There are two categories of encryption algorithms, i.e. symmetric key and asymmetric key algorithm. With symmetric key algorithms, the same key is used for both encryption and decryption.

Implementations of symmetric-key encryption can be highly efficient with regard to speed of operation compared to asymmetric algorithm, so that users do not feel any significant time delay as a result of the encryption and decryption. Asymmetric encryption involves a pair of keys. i.e., public key and a private key-associated with an

entity that needs to authenticate its identity electronically or to encrypt data. For additional explanation about cryptographic algorithms refer [15]

There are different kinds of symmetric key algorithms. For this aplication, DES symmetric key algorithm is implemented because of two reasons. The first reason is, it is freely available, and the other is it uses 64bit key for encryption. Using this smaller key length would make the algorithm to be faster for the encryption and the decryption process.

The possible application area of the DES [20] algorithm for the system is for encrypting the votes which are entered to the database and similarly to decrypt it back later on. i.e., when the voter submits his choices of candidates, the candidate PIN and the party code will be encrypted. This helps to keep the anonymity of the votes, and to secure the vote data from eavesdroppers in the channel between the application server and database server, and also at the database [see Fig.5].

5.2.4 Security Packages and Utilities

The security packages are used as sources for the security tools, to mention them, JCA is a source for MD-5 and DES algorithms, JSSE is the source for SSL protocol and Keytool for certificate generation.

JCA

Java has an API that helps to access the standard security algorithms, which is found in Java_Home\jdk1.5.0_01\jre\lib\security folder. But the files in the security folder are not adequate enough to get the required algorithms. Additional files are used that are available in JCA 1.2 package, and included in the security folder of Java. The JCA introduced the notion of a Cryptographic Service Provider. It is a framework for working with cryptography using the Java programming language. It forms part of the Java security API, and was first introduced in JDK 1.1 in the java security package, and used as the source of hashing and encryption algorithms [18].

JSSE

The JSSE enables secure Internet communications. It provides a framework and an implementation for a Java version of the SSL and TLS protocols and includes functionality for data encryption, server authentication, message integrity, and optional client authentication.

For this project, JSSE is used for implementing SSL protocol. The package is found in Java_Home\jdk\jre\bin folder. This folder must be configured in the environment variable[2] setting window, i.e., the variable name will be JSSE, and the value of the variable will be Java_Home\jdk\jre\bin folder.

KeyTool

SSL protocol was created to ensure secure transactions between web servers and browsers. This protocol uses a third party called CA, to identify one end or both end of the transactions. A certificate can be either signed by a commercial CA or can be self signed using key management utilities.

Keytool is a key and certificate management[19] utility that is used for this project for creating and generating self signed certificate, which is available in JDK 1.5. The toolkit is found Java_Home\ jdk1.5.0_01\jre\bin folder.

5.3 Prototype of the System

The prototype of the system describes the screen shoots taken from the different parts of the application. The first sections show some of the tables of the database taken from MySQL database. The second part shows messages that confirm the establishment of secure channel. The third part shows the web forms taken from the web application, and the last section shows forms taken from the desktop application.

[2] The environment variable is runtime variable which is configured in the Environment Variable Window , It is available in the control panel

5.3.1 Database Tables

This section describes about the screen shoots taken from MySQL database. To mention them, Voters table contains information regarding to the registered voters. Parliament and Regional candidates' tables contain information regarding to the registered candidates. Encrypted votes and Decrypted votes tables contain information regarding to votes, which are encrypted and decrypted respectively. There is also a table which sets the maximum votes given by a voter. And at the last, the Pass-phrase table shows the pass-phrase text in encrypted format, which is an input for generating a key.

Voters' Table

The voters table holds three attributes; VPIN, VName and VPSN (see Table.3). The VPIN is used to uniquely identify each voter and stored in hashed format. The VName is the name of the voter, which is entered with Ethiopic characters and stored with Unicode format. Finally, the VPSN is used to describe at which polling station that the voter registers.

```
mysql> select * from voters;
+--------------------------+-----------------+------+
| VPIN                     | VName           | VPSN |
+--------------------------+-----------------+------+
| 19zXm3c9yFyJuEhize22zw== | &#4704;&#4672;& | 2    |
| 7R23cTIRBbPA28cKZhubEA== | &#4768;&#4704;& | 2    |
| gF2U0UBGUJ+Cx72xgZxkrw== | &#4632;&#4782;& | 1    |
| r8t6LxwVgoa0gGLNiFqYZg== | &#4608;&#4755;  | 1    |
| sLrunSedNPod/XGq25CMPw== | &#4656;&#4616;& | 1    |
| SwCcL46NIwxJjC2yZnjddw== | &#4777;&#4777;  | 1    |
| Tk+q5yscPL1EanDonlnY/A== | &#4846;&#4755;& | 2    |
+--------------------------+-----------------+------+
```

Table.3. Voters table sample data

Parliament and Regional Candidates' Tables

As shown at Table.4. and Table.5., both PCandidates and RCandidates tables have the same attributes. The CPIN attribute is used to uniquely identify each of the candidates. The CName represents the name of the candidates. The PartySymbol is used as the name of Party, PartyPicture is used to represent the party identification symbol, and at

last PSN, is used to identifying the constituency number where the candidates would collect votes.

```
mysql> select * from pcandidates;
+------+-----------------------------+-------------+--------------------+------+
| CPIN | CName                       | PartySymbol | PartyPicture       | PSN  |
+------+-----------------------------+-------------+--------------------+------+
| 1000 | &#4768;&#4704;&#4704;       | X           | /images/tomcat.gif | 001  |
| 1001 | &#4635;&#4638;              | V           | /images/orange.GIF | 001  |
| 1002 | &#4768;&#4621;&#4635;&#4829; | X           | /images/tomcat.gif | 002  |
| 1003 | &#4872;&#4632;&#4729;       | V           | /images/orange.GIF | 002  |
+------+-----------------------------+-------------+--------------------+------+
```

Table.4. Parliament Candidates Sample Data

```
mysql> select * from rcandidates;
+------+----------------------+-------------+--------------------+------+
| CPIN | CName                | PartySymbol | PartyPicture       | PSN  |
+------+----------------------+-------------+--------------------+------+
| 2000 | &#4704;&#4672;&#4616; | X           | /images/tomcat.gif | 001  |
| 2001 | &#4877;&#4653;&#4635; | V           | /images/orange.GIF | 001  |
| 2002 | &#4720;&#4936;&#4651; | X           | /images/tomcat.gif | 001  |
| 2003 | &#4872;&#4752;&#4725; | X           | /images/tomcat.gif | 001  |
| 2004 | &#4768;&#4616;&#4633; | V           | /images/orange.GIF | 001  |
| 2005 | &#4723;&#4848;&#4656; | V           | /images/orange.GIF | 001  |
+------+----------------------+-------------+--------------------+------+
```

Table.5. Regional Candidates Sample Data

Encrypted Votes tables

The PEVotes and REVotes table holds votes given for parliamentary and regional candidates respectively. Each table contains four attributes. The VPIN attribute identifies the identity of the voter. The CPIN attribute identifies the identity of the selected candidates. The PartySymbol attribute identifies for which party the candidate is represented. Both CPIN and PartySymbol are stored in encrypted format. The VPSN is used to indicate at which polling station the vote has given to the candidate (see Table 6 and Table. 7).

```
mysql> select * from pevotes;
+-------+--------------+--------------+------+
| VPIN  | CPIN         | PartySymbol  | VPSN |
+-------+--------------+--------------+------+
| 11110 | 3ttSHUApugg= | B7R2s2HA79M= | 0001 |
| 11111 | MLncc+vWgaY= | B7R2s2HA79M= | 0002 |
| 11112 | Oh+6URfoqhA= | B7R2s2HA79M= | 0001 |
| 11113 | V1E3KwS+LNg= | B7R2s2HA79M= | 0002 |
+-------+--------------+--------------+------+
```

Table.6. Votes for Parliament Candidates

```
mysql> select * from revotes;
+-------+--------------+--------------+------+
| VPIN  | CPIN         | PartySymbol  | VPSN |
+-------+--------------+--------------+------+
| 11110 | icE05MziqWs= | B7R2s2HA79M= | 0001 |
| 11110 | rY82iE07EA4= | 9BXJm624M48= | 0001 |
| 11110 | 0wkmLiMRzIY= | B7R2s2HA79M= | 0001 |
| 11111 | jqvdXmMw384= | B7R2s2HA79M= | 0002 |
| 11111 | 3myuDRIp5XE= | 9BXJm624M48= | 0002 |
| 11111 | HB5h0q5r8so= | 9BXJm624M48= | 0002 |
| 11112 | icE05MziqWs= | B7R2s2HA79M= | 0001 |
| 11112 | rY82iE07EA4= | 9BXJm624M48= | 0001 |
| 11112 | rkjRHXrfnJs= | B7R2s2HA79M= | 0001 |
| 11113 | jqvdXmMw384= | B7R2s2HA79M= | 0002 |
| 11113 | 3myuDRIp5XE= | 9BXJm624M48= | 0002 |
| 11113 | HB5h0q5r8so= | 9BXJm624M48= | 0002 |
+-------+--------------+--------------+------+
```

Table.7. Votes for Regional Candidates

Decrypted Votes Tables

At Table .4. , and Table.5, the tables' attributes, i.e., CPIN and PartySymbol stored the data in encrypted format. At the end of the election, these two attributes will be decrypted and the whole data will be copied into two corresponding tables called PDVotes and RDVotes. PDVotes contains the decrypted data of PEVotes(see Table.8) and RDVotes contains the decrypted data of REVotes(see Table.9).

```
mysql> select * from pdvotes;
+-------+------+-------------+------+
| VPIN  | CPIN | PartySymbol | VPSN |
+-------+------+-------------+------+
| 11110 | 1000 | X           | 0001 |
| 11111 | 1002 | X           | 0002 |
| 11112 | 1004 | X           | 0001 |
| 11113 | 1003 | X           | 0002 |
+-------+------+-------------+------+
```

Table.8. Decrypted Parliament Votes

```
mysql> select * from rdvotes;
+-------+------+-------------+------+
| VPIN  | CPIN | PartySymbol | VPSN |
+-------+------+-------------+------+
| 11110 | 2000 | X           | 0001 |
| 11110 | 2001 | V           | 0001 |
| 11110 | 2005 | X           | 0001 |
| 11111 | 2003 | X           | 0002 |
| 11111 | 2006 | V           | 0002 |
| 11111 | 2007 | V           | 0002 |
| 11112 | 2000 | X           | 0001 |
| 11112 | 2001 | V           | 0001 |
| 11112 | 2004 | X           | 0001 |
| 11113 | 2003 | X           | 0002 |
| 11113 | 2006 | V           | 0002 |
| 11113 | 2007 | V           | 0002 |
+-------+------+-------------+------+
```

Table.9. Decrypted Regional Votes

Maximum and Minimum Vote Setting Table

The Election-Rule table contains some of the rules that can be entered from the electoral officers. The table holds four attributes. The PMaxVotes and RMaxVotes notify the maximum votes given by one voter for the Parliament and Regional candidates respectively (see Table.10). The PMinVotes and RMinVotes notify the minimum votes given for Parliament and Regional candidates respectively.

```
mysql> select * from electionrule;
+-----------+-----------+-----------+-----------+
| PMaxVotes | RMaxVotes | PMinVotes | RMinVotes |
+-----------+-----------+-----------+-----------+
|         1 |         3 |         0 |         0 |
+-----------+-----------+-----------+-----------+
```

Table.10. Rule Setting Table

KeyGenerator Table

The keyGenerator table contains only one attributes (see Table.11). The content of the attribute is pass-phrase that is used to generate encryption/decryption key. For the sake of hiding the identity of the pass-phrase, it is stored in encrypted format. When the voter submits his/her votes, the encryption key will be automatically generated from the pass-phrase.

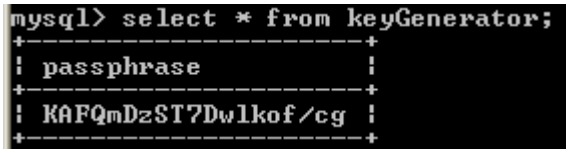

Table.11. Pass-Phrase Table

5.3.2 HTTPS Protocol

HTTPS is a standard protocol, which is used for accessing a secure Web server using authentication and encrypted communication. Using HTTPS in the URL instead of HTTP directs the message to a secure port number rather than the default Web port number of 80. The default TCP/IP port of HTTPS is 443. The session is then managed by a security protocol. HTTPS encrypts the session data using the SSL protocol ensuring protection from eavesdroppers and man-in-the-middle attacks. SSL is a protocol for encrypting and decrypting data across a secure connection from a client to a server with SSL capabilities. To authenticate the server, a client certificate has to be generated.

Certificates are digital identification documents that allow both servers and clients to authenticate each other. Server certificates contain information about the company and that issued the certificate, and the client certificates contain information about the user and the organization that signed the certificate.

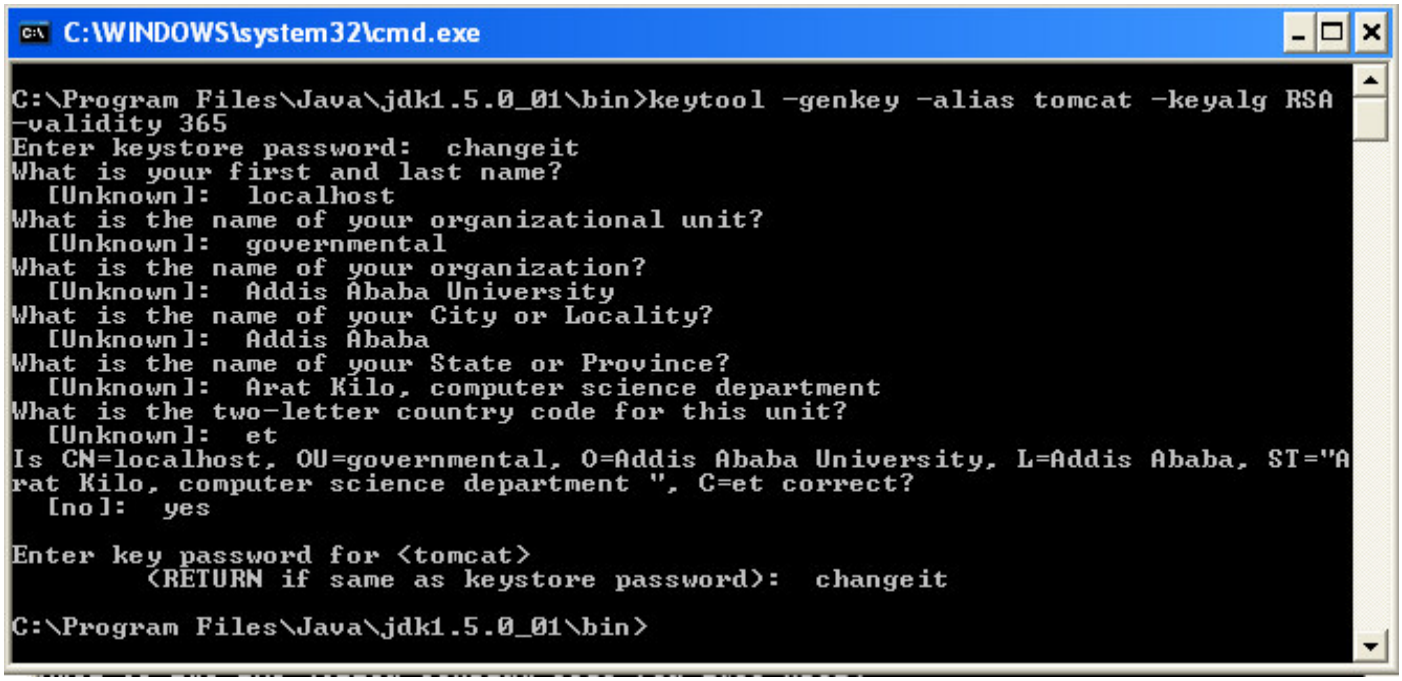

Fig.7. Certificate generation

For this project case, the certificate is generated by using Java certificate generating tool called keytool. Fig.7 shows the sequential steps used to generate the certificate. The certificate will hold the public private key pair that is used for encrypting and decrypting the data between the browser and the web server.

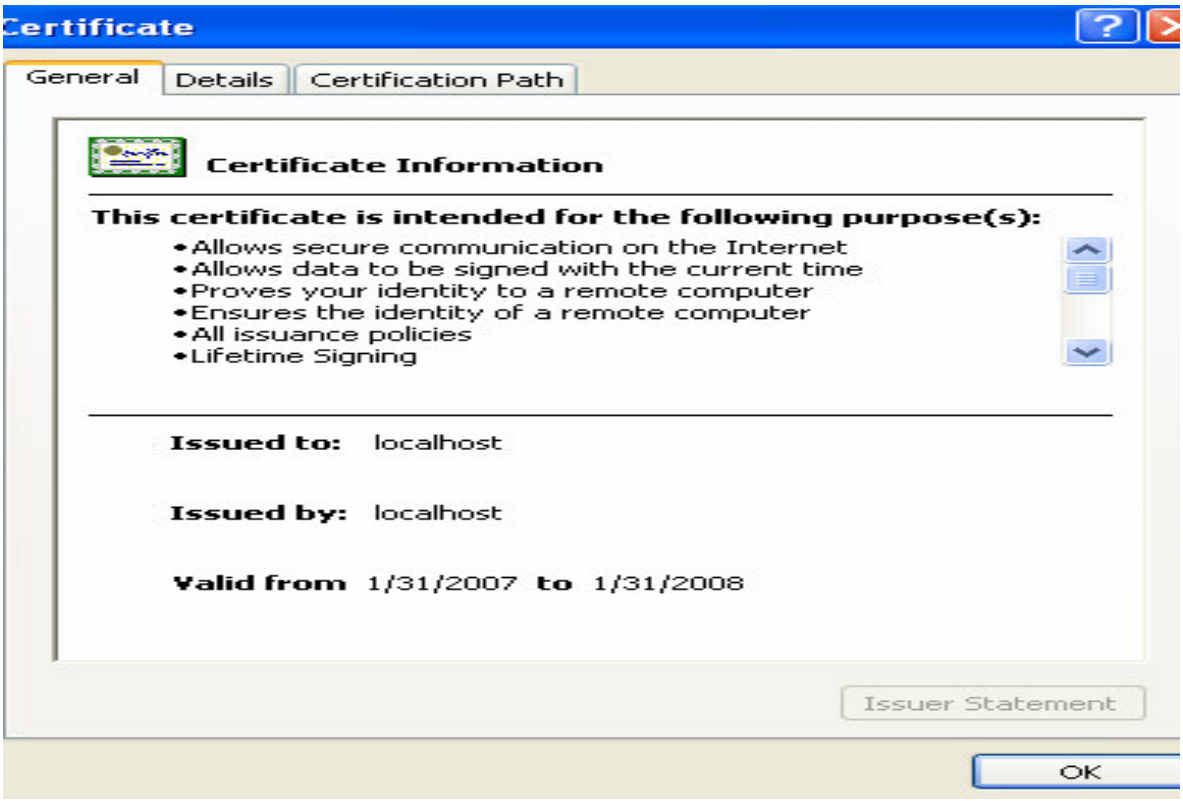

Fig.8. Certificate Information

Tomcat server must be configured to handle SSL communication. The configuration file is located in tomcat_home[3]/conf[4]/server.xml[5] file. The purpose of configuring the web server is to open port 443, which is disabled by default. The opening of this port enables SSL protocol to start work. Then, all sensitive accesses will get redirected to the port.

When the user tries to access a site through HTTPS protocol, the browser automatically displays a security alert message. This message shows an attempt to make a secure connection to the Web site. Secure communication means that information you provide is encrypted so that it can't be read or intercepted by other people [11]. When the user gets in the secured site, Internet Explorer displays a dialog box and a lock icon in a locked position on the status bar (See Fig.10).

[3] Describes the installation folder of tomcat
[4] describes the folder where configurations files are stored
[5] A files that holds Tomcat configuration settings

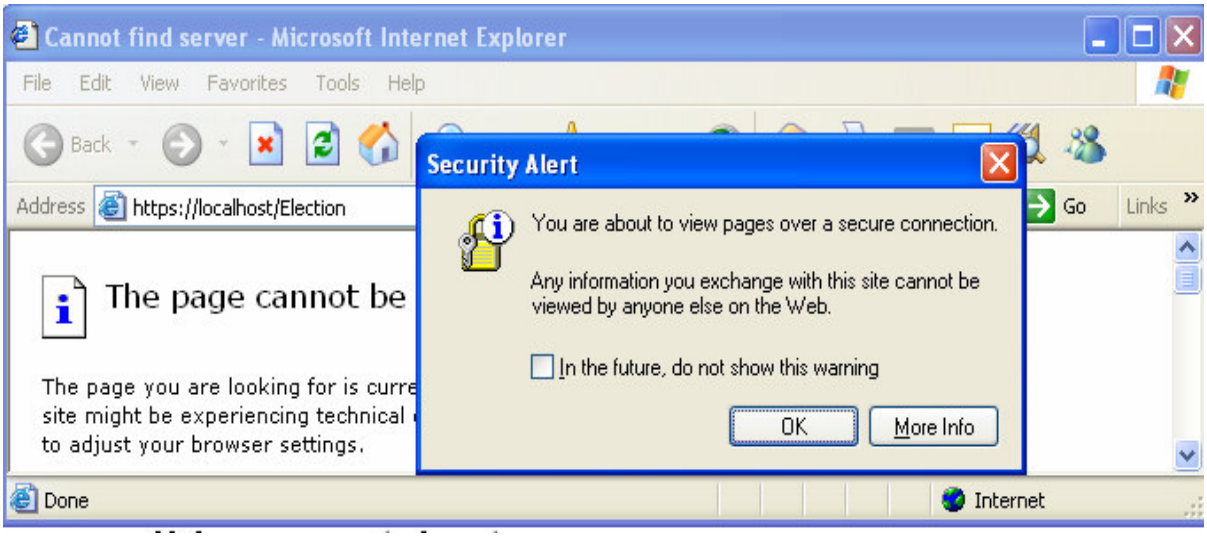

Fig.9. Security Alert Message for SSL Connection

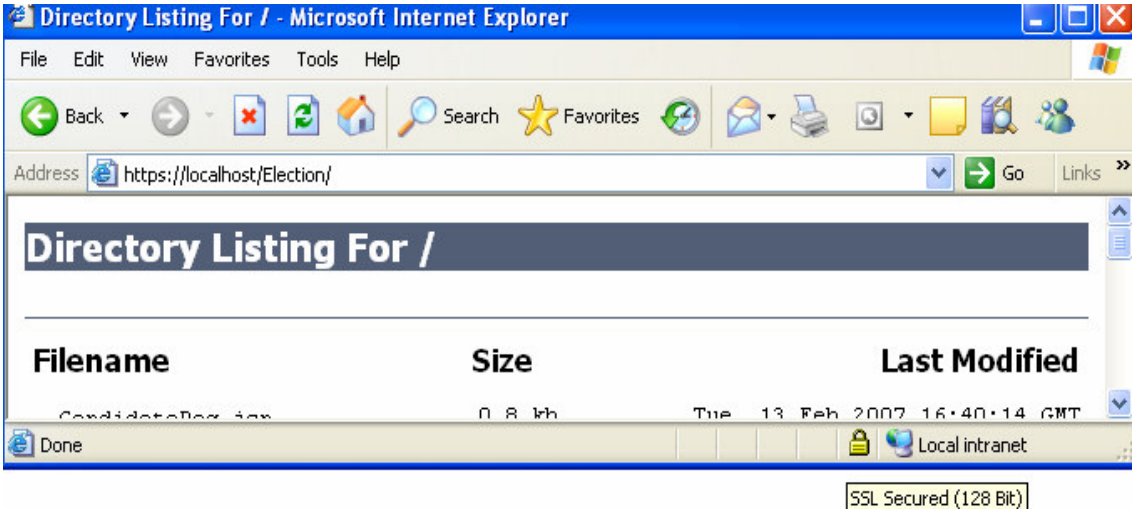

Fig.10. Taskbar showing SSL connection

5.3.3 Users Screen Shots

The following sections show the screen shots taken from the system including their description. The screen shoots are taken from the web and desktop applications. For the purpose of simplifying the forms, some of the attributes are not included, and the basic ones are taken. The full attributes of the tables is shown at the database design (see Fig.2.)

5.3.3.1 Web Application

The web forms include voters' registration form, candidates' registration form, vote casting form, and Login form. In addition to that some users' alert messages that control users from certain illegal actions are also included.

Voters' Registration Form

Fig.11 shows the screen used by registrars for the purpose of registering voters. When the voter registers, the three basic attributes, i.e. PIN, Name and PSN are registered.

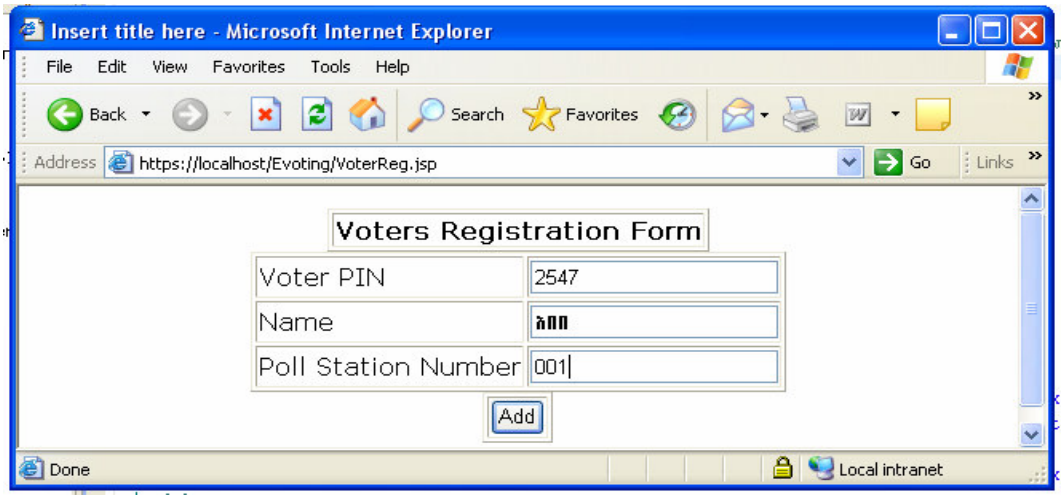

Fig.11. Voters Registration form

Candidates' Registration forms

Forms shown at Fig.12, and Fig.13, are used to register parliament and regional candidates respectively. The attributes used to describe the candidates are, PIN, Name, Party Symbol and CCN where the candidates registers.

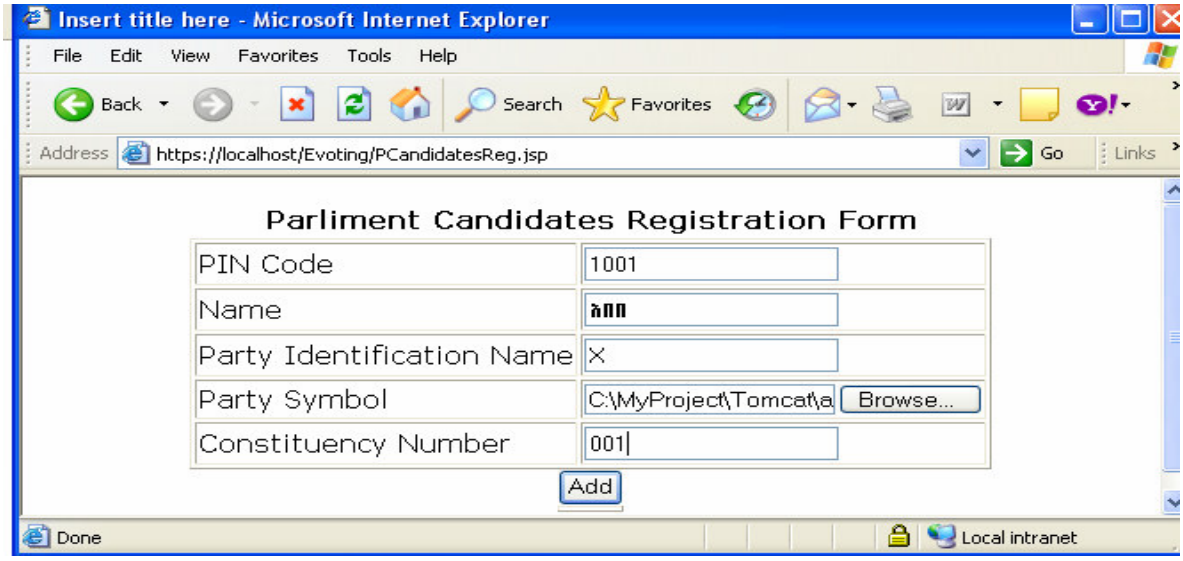

Fig.12. Parliamentary Candidates Registration Form

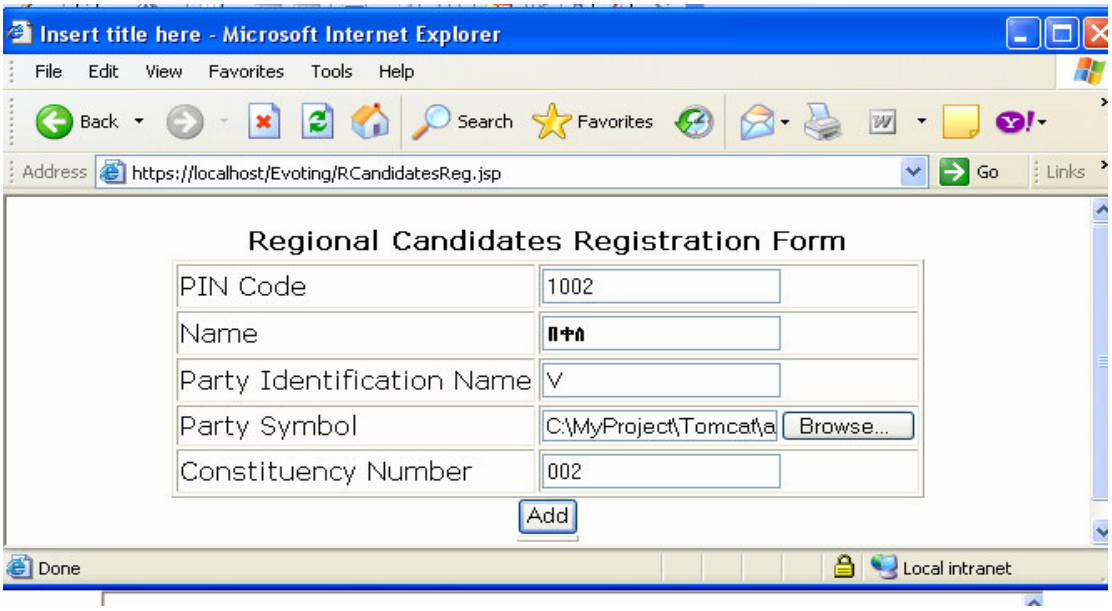

Fig.13. Regional Candidates Registration Form

Voter Login form

By using the form shown at Fig.4,the voter logins to the system with the PIN and polling station numbers at the space provided. If the voter is registered properly and has not

cast a vote previously, the system will retrieve (see Fig.15) the list of candidates (for both Parliament and Regional) that are computing in the specified polling station.

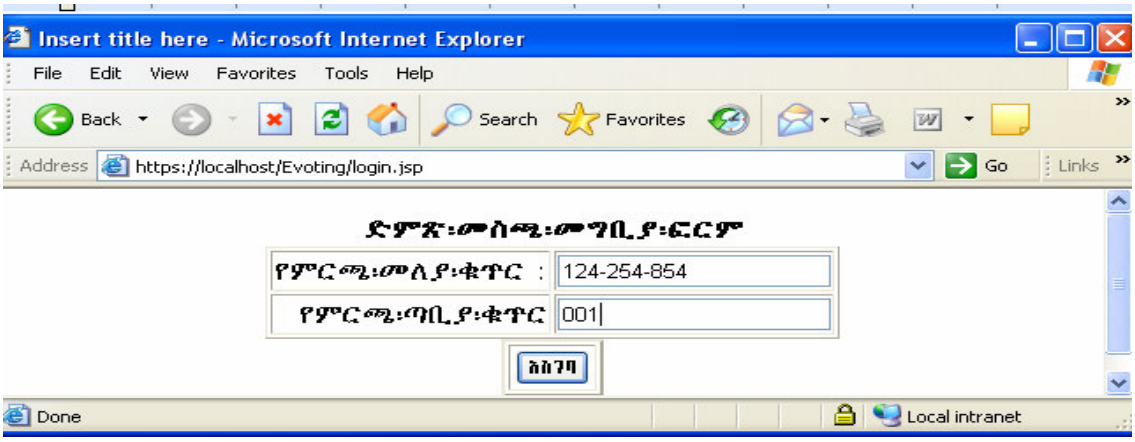

Fig.14. Voters Login form

Vote Casting Form

The screen that consists of candidates list (see Fig.15) will be prompted right after the voter login to the system successfully. The name of candidates which is shown on the form is retrieved based on, the PIN and PSN values which are entered at voters' login form. The form separately displays the Parliament and Regional Candidates, along to their names a checkbox is also provided to voters to cast by checking the boxes. This is done just for making the user interface more users friendly. In addition, it shows symbols that represent the party of the candidates; this makes the identification of candidates easier. The pictures are dynamically retrieved from the files based on their unique URL stored in the tables.

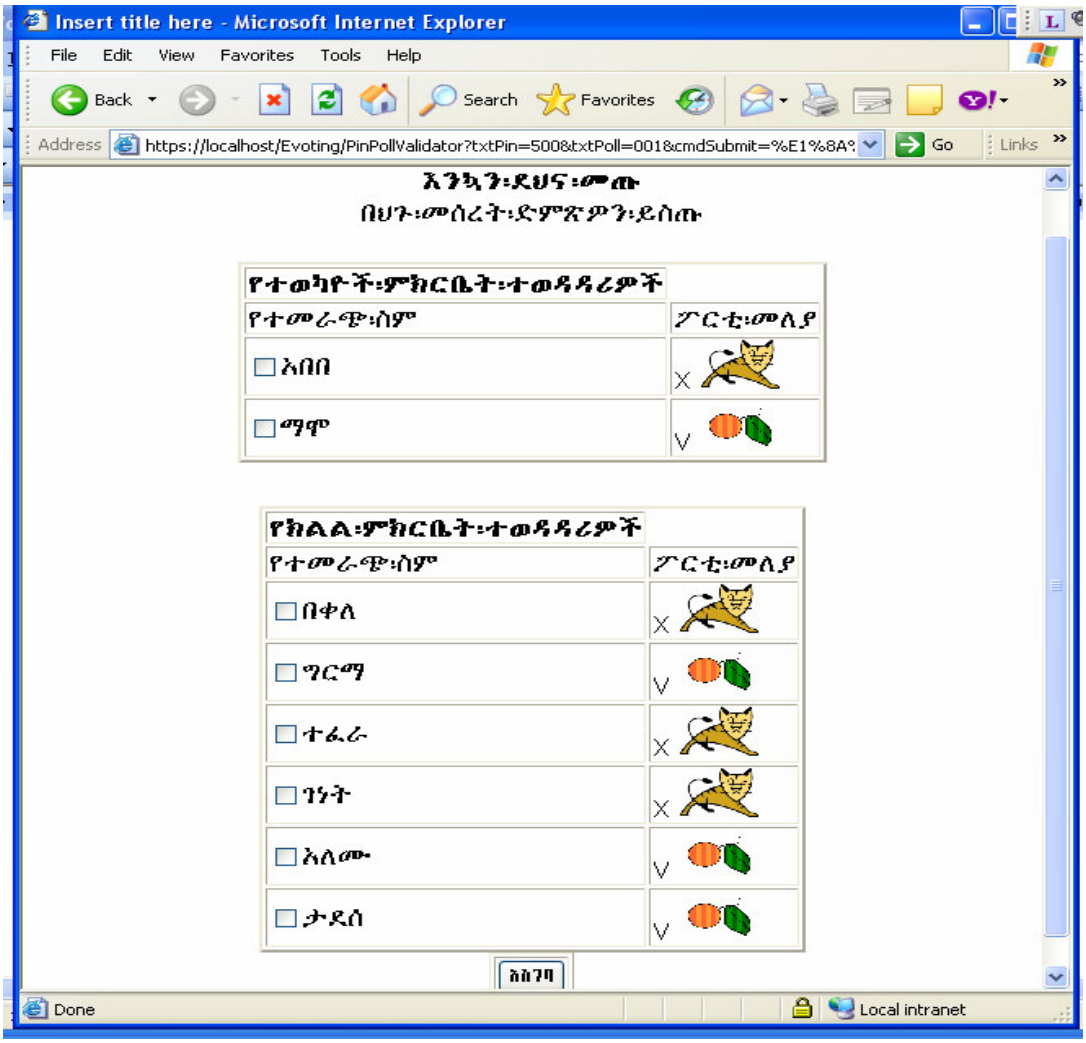

Fig.15. Vote casting form

The system also displays messages which alert voters for illegal actions. The messages are used to control over votes. This is determined by the election policy which is created by the election officer at Table.10. For this prototype case, an assumption is taken, maximum vote for parliamentary candidates to be one and for the regional candidates to be three. If a voter selects more than one parliamentary candidate or more than three regional candidates, alert message will appear to the voter for reminding the rules.

5.3.3.2 Desktop Application

The other categories of forms are taken from the desktop application that helps to create registrars, pass-phrases and a form that shows vote results.

The screen shot which are mainly used by the voter and registrar are mentioned before in section 5.2.3.1. This section specifically describes the screen shots taken from the desktop application. The only user of the desktop application is the Election Officer, or someone else who is responsible for the case.

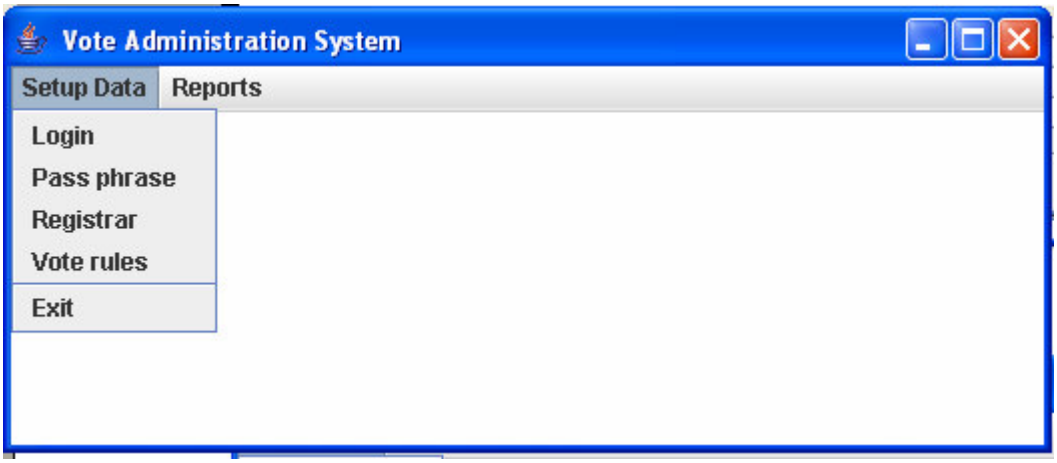

Fig.16. MDI Form of the Desktop application

Fig.17 and Fig.18 show login form to the desktop application and registrars creating form respectively. Fig.19 and Fig.20 show vote rule creating form and pass-phrase creating form respectively. Finally, Fig.21 and Fig.22 show vote decrypting and report generating forms respectively.

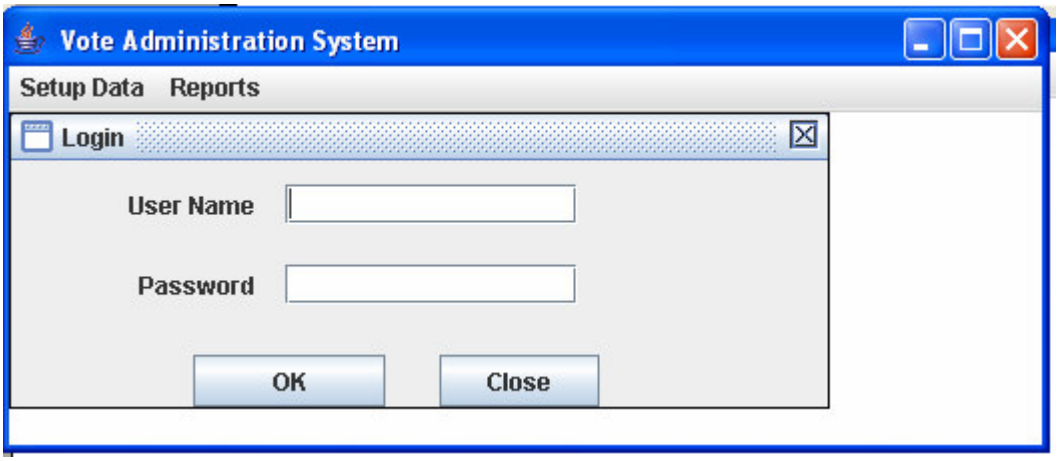

Fig.17. Login Form to the application

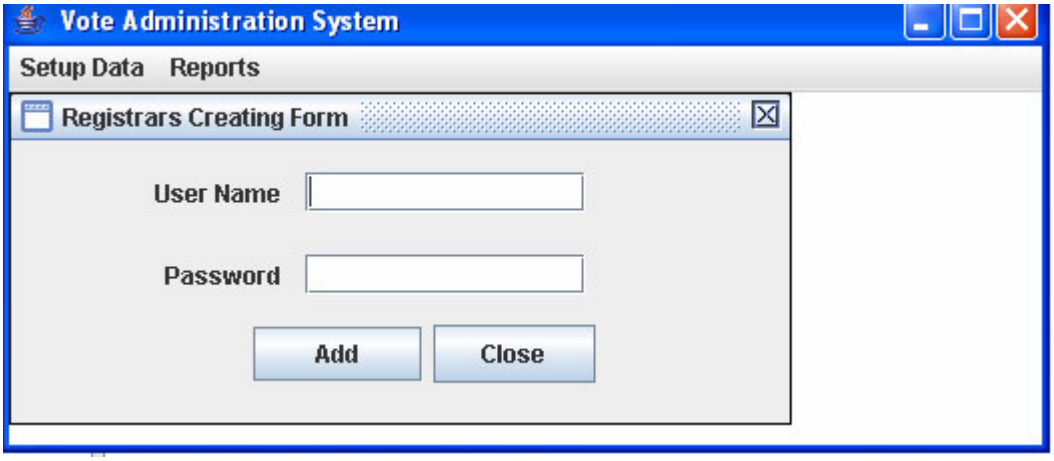

Fig.18. Registrars Creating Form

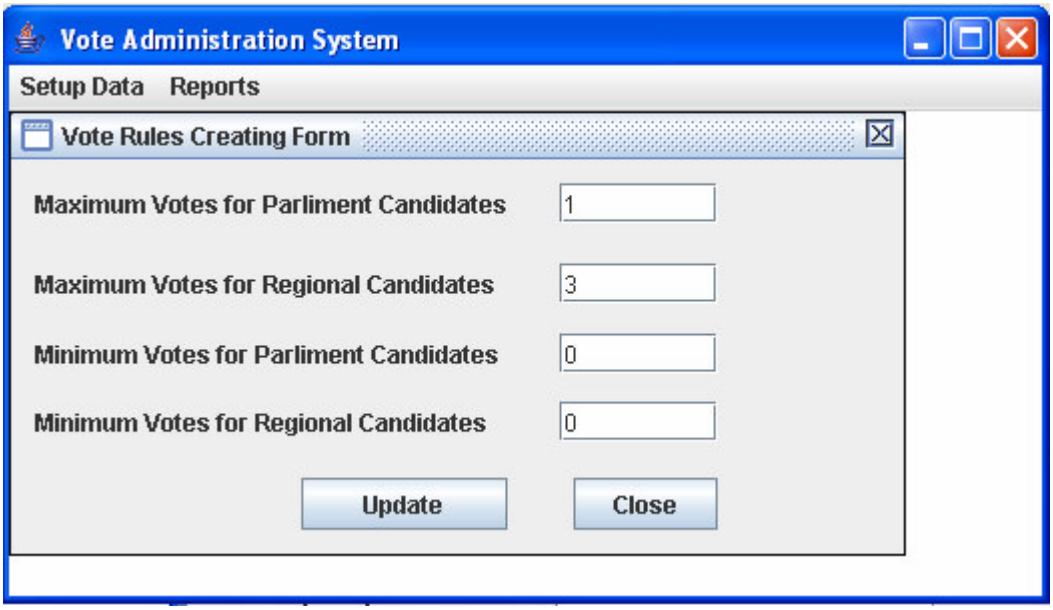

Fig.19. Vote Rule Creating Form

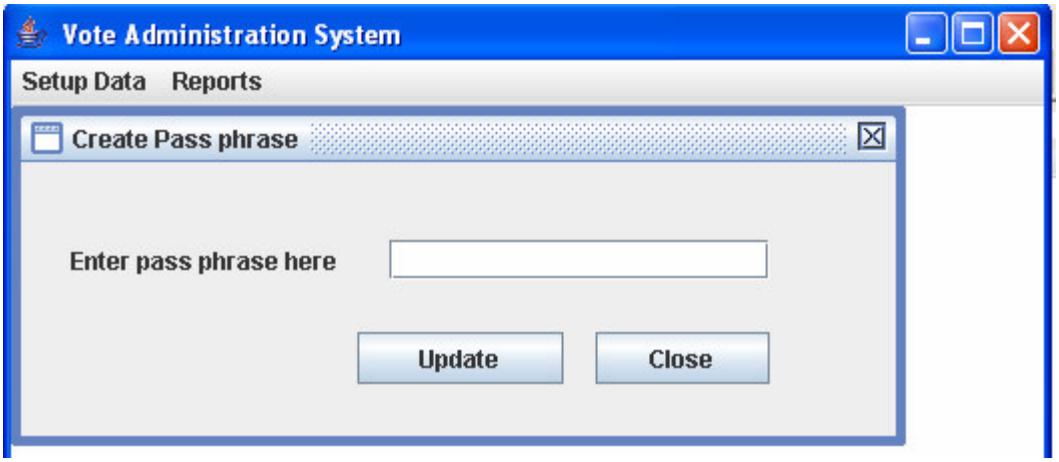

Fig.20. Pass Phrase Creating Form

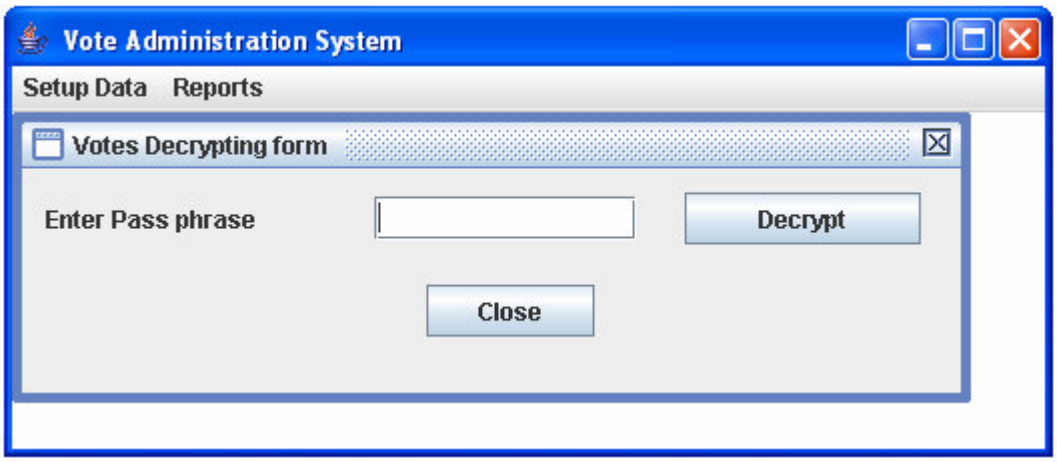

Fig.21. Vote Decrypting Form

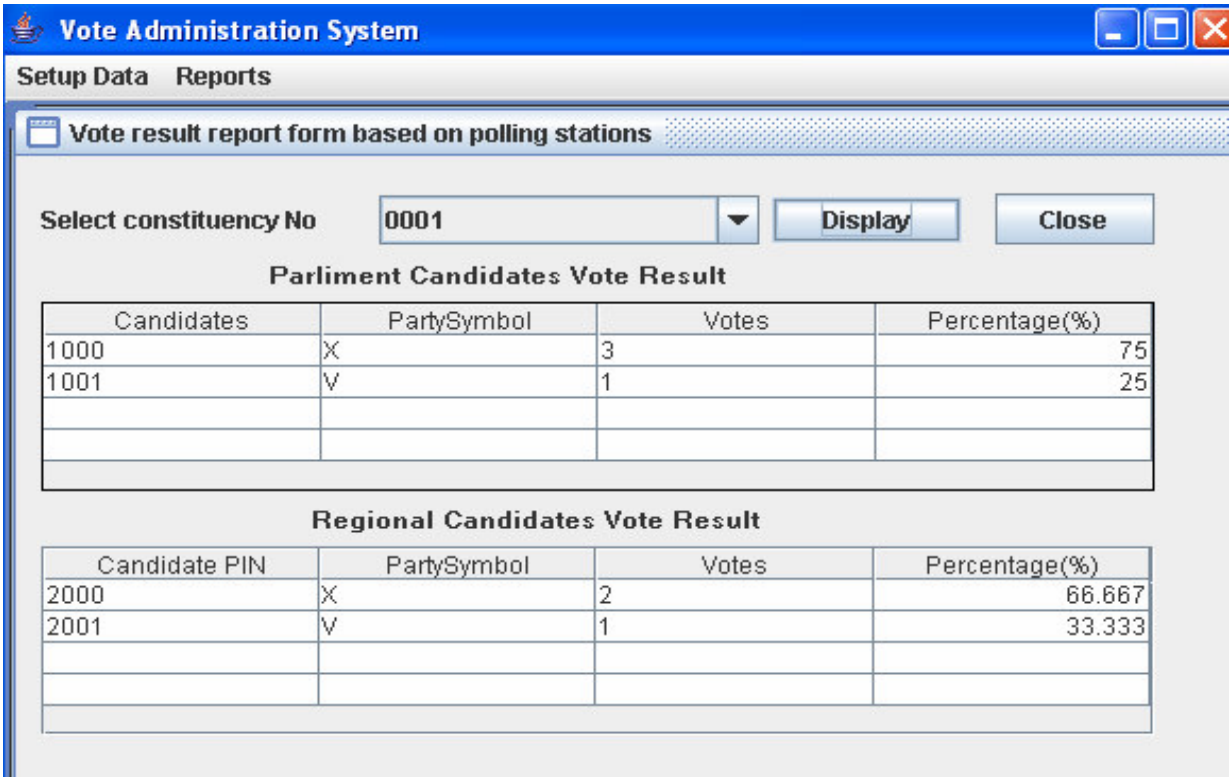

Fig.22. Result Generating Form

6 Summary

The target of the project is proposing a system that will automate the voting system of Ethiopia, in particular Addis Ababa City. The problem of the current paper voting system as described in the problem statement section is obvious. The limitations and the scope of the work also described separately. The experience of other countries on the related work is reviewed. The reason for reviewing others work is to share experience on how to cope up the difficulties of the work, to know in advance the pros and cons of electronic voting, and to learn techniques.

The requirement analysis of the system is discussed within the scope of the project. First the general requirement of e-voting is stated, and then the specific requirement is defined based on historical information and the source document taken from Ethiopia Election Board. Based on this document, some of the rules and regulation that should be incorporated in the system is collected. Under the specific requirement, the functional and non-function requirements are described separately. The functional requirement defines the business logic of the system, whereas the non-functional requirement describes constrains that needs to be considered for using the system. The interaction of users with the system is illustrated with the help of Use Case diagram.

The system design is done by considering the main design elements like the database design, the system architecture, the expected places for security holes, the network infrastructure, and a scenario that show the interaction of the components of the system architecture. A model that shows all the tables of the database is illustrated, and an explanation about each of the attributes of the tables is also given.
The system architecture is a three tier model. It shows the organization of the main components of the system. These components are the client tier, which is found on the user side; the business logic, which implements the functional requirements of the system; the database system, which will store the application data. The components

would be placed in different machines, and communicate to each other through the network.

Since the components of the system are distributed on different places, it is expected that an attack may be committed on the line of communication, or at the storage. To protect this attack, the possible security holes are identified and addressed.

With regard to network infrastructure, this project proposes WoredaNet network, which is owned and administered by the government.

Finally, the system implementation is described in two parts. In the first part, the development and security tools are explained. The reason for selecting the tools is also supported with explanation.

The second section shows the screen shots taken from the different parts of the application. The application is divided into two categories. The first one is the web application which is used by the voters, registrars and the second part is used by the Election Officers, which is used for administrating the system and for generating reports.

7 Conclusion and Recommendation

In democratic society, political leaders are assigned by public elections. The nature of election process is complex, error prone and mostly exposed to fraud. Ethiopia is not an exception to this condition. Currently, In Ethiopia, the only tool to manage the voting process is manual. However, many countries have either changed the paper based voting system totally or they provide supplemental voting system. This project proposes a supplemental voting system for Ethiopia, particularly to Addis Ababa City, and shows how to solve some of the technical problems. The supplemental voting system targets on providing a voting system, which is cost effective, reduces the security problems, and helps to declare the election results on time. The technology is applied in many countries and brought significant benefits. Similarly, if it is used for Ethiopia, it will have contribution to easily manage the voting process.

In general, this project contributes an initial work on electronic voting system for Addis Ababa City. But, this work needs to mature in other similar projects in the future, to be scaled up to the whole country. It is recommended also that the government will take this opportunity to entertain such alternative voting system.

Reference

1. Kassahun F.,Tessga Z., August 2006, Audience Response System, Addis Ababa University, Electrical and Computer Engineering Department.
2. Electronic Voting, Available from: http://en.Wikipedia.org/Wiki/Electronic voting (accessed 04 February 2007).
3. Doug D., How Electronic Voting Impacts the Trustworthiness of Elections, Available from: WWW.OpEdNews.com (accessed 04 February 2007).
4. Electricnews.net, All internets Voting is Insecure, Available from: http:www.theregister.co.uk/2004/01/23 (accessed 08 January 2007).
5. Steven M., A Better Ballot Box, Available from: http://www.notablesoftware.com/papers/1002evot.pdf (accessed 15 January 2007).
6. Pipaa N., Evoting as a magic Ballot, Available from: http://ksghome.harvard.edu (accessed 04 February 2007).
7. Every One Counts PL, A Virtual Private Network for Internet Voting, Available from: http://www.everyonecounts.com (accessed 26 February 2007).
8. Joseph R., Alen E., Dermot C., Fintan F., the KOA Remote Voting System, Available from: http://secure.ucd.ie/documents/submitted/KOAEVT06.pdf (accessed 20 February 2007).
9. 30th meeting of the working Group on 28th August 2001 in Berlin, Data Protection and Online Voting in Parliament and Other governmental elections, Available from: http://www.datenschutzberlin.de/doc/int/iwgdpt/Online_Voting.htm(accessed 28 January 2007).
10. http://www.electionsethiopia.org (accessed 10 February 2007).
11. Kipp E., B. Hickma, Netscape Communication Corp., The SSL Protocol, Available from: www.cs.bris.ac.uk/~bradley/publish/SSL/Appendix/SSL_old.htm(accessed 01 March 2007).

12. Fikreyohannes L., Solomon A., Samuel K., Design of Architecture for Terrestrial LAN and VSAT based National Telemedicine Network in Ethiopia, Available from: http://www.digitaladdi.com/sk/TeleMedicine_Ethiopia_Paper2.pdf(accessed 10 February 2007).
13. Arthur G., Robert B., Andrew S., A comparison of HTTP and HTTPS performance, Courant Institute of Mathematical Science,New York University, Available from: www.cs.nyu.edu/cs/faculty/artg(accessed 20 January 2007).
14. R.Riverst, The MD-5 Message Digest Algorithm,MIT Laboratory for Computer Science and RSA Data Security, Inc, April 1992, Available from:http://www.ietf.org/rfc/321.txt(accessed 8 January 2007).
15. Kurt G., 28-08/2000, Symmetric vs. Asymmetric algorithms, Available from:http://www.suse.de/~garloff/writings/mutt_gpg/node3.html (accessed 15 February 2007).
16. http://Java.sun.com/javaee.
17. Open Source,http://www.Opensource.org/Opensource.
18. Java Cryptographic Architecture API Specification and Reference, Available from:http://Java.sun.com/j2se/1.4.2/docs/guide/security/cryptospec.html.
19. KeyTool, http://java.sun.com/j2se/1.3/docs/tooldocs/win32/keytool.htm.
20. DES Encryption,http://www.tropsoft.com/stronggenc/des.htm.

Appendix 1

1. Ethiopia electoral rule

The following are some of the election rules and regulation of Ethiopia, these rules and regulations are sources of input for requirement analysis.

- Voting in any election shall be carried out in secret
- Each vote shall carry equal weight
- Any person shall be registered once and at one place only
- Registration shall be carried out at the polling station within the Keble of the elector's residence, provided however registration from house to house or in similar places outside the polling station is prohibited
- The elector shall be issued with an elector's card
- The disabled and the blind may be registered accompanied by their assistants
- Registration shall be carried out at a polling station
- Any person duly registered shall be issued with an elector's card bearing his name place of birth, designated polling station, registration number and his signature or thumb mark
- Upon conclusion of registration, the electoral roll shall be marked with closing indications and signed by the electoral officials
- Subsequent to closure of the electoral roll, each polling station shall transfer same, or a copy of it, and other necessary documents to the respective Woreda electoral office, in accordance with directives to be issued by the Board
- Any person shall stand as a candidate only in one constituency
- In case candidates have equal number of votes, they will be identified by drawing a lot
- Every elector shall vote by appearing in person
- Each elector should vote only once

- Any elector may cast his vote only upon confirmation that he is carrying the elector's card
- Any elector may cast his vote only at the polling station where he had registered
- The elector shall hand his elector's card to the electoral coordinators of the polling station, where upon they shall proceed to verify his identity by examining the card
- After verification of the voter identity, the thumb of the elector shall be put into the ink provided for the purpose, after which he shall be handed with a ballot paper and pointed out to the voting booth;
- Any elector shall have the right to choose a person who can assist him to mark the ballot paper and put it in the ballot box during the voting process
- Soon after closure of the polls, counting of ballots shall be carried out at polling stations, in accordance with directives to be issued by the Board
- The results of counting made at a polling station shall be publicized forthwith
- Upon the conclusion of election and collection of the necessary information, the board shall forthwith issue an official declaration containing the following particulars; the number of registered electors, the number of electors having cast their vote, the number of blank and null ballot papers, the percentage of registered electors having and not having cast their vote, the percentage of unregistered electorate, the list of elected candidates and their respective constituency
- Voting shall be carried out without interruption during the voting hours
- The elector shall handover his elector's card to the election coordinators of the polling station, where upon, by referring to the electoral roll, they shall proceed to verify his identity and that he has not voted
- By examining both hands of the elector the election coordinators ascertain that there is no identifying ink that shows he has voted

- In the booth, the elector shall put, on the ballot paper, an "X" or a thumb mark in the square corresponding to the symbol of the candidate for which he wants to vote
- Counting of votes shall be conducted by the Polling Station Officers only, and others shall have the role of observers
- The counting shall be made by picking one of the arranged votes and count them three times by three different officers