

HYBRID SOLUTION FOR THE CURRENT NATIONAL ELECTION SYSTEM

A Thesis

Submitted to the Department of Computer Science & Engineering

Of

BRAC University

By

MD. NAIMUZZAMAN

Student ID: 01201018

In Partial Fulfillment of the

Requirements for the Degree

Of

Bachelor of Science in Computer Science & Engineering

June 2005



BRAC University, Dhaka, Bangladesh

DECLARATION

I, MD. Naimuzzaman, University ID# 01201018 have completed some modules of our proposed thesis, Hybrid Solution for National Election System, under CSE 400 course based on the results found by myself.

Therefore I declare that this project has been published previously neither in whole nor in part for any degree except this publication. I also mentioned materials of work found by other researcher by reference.

Signature of
Supervisor

Signature of
Author

ACKNOWLEDGEMENT

Firstly, I am grateful to all mighty ALLAH for giving me the strength to start such a project and thus conclude with solutions successfully.

I am grateful and take the honor to express my thanks to my respectable supervisor Dr. Yousuf Mahbubul Islam, PhD for his supportive opinions and suggestions. Without his co-operation and resources it would be a day dream to complete my work within this very short period.

I would like to thank our teacher Mrs. Bushra, Mr. Matin Saad Abdullah and Mr. Hossain Arif for their important and helpful suggestions.

My special thanks to our respective senior brothers of university and my friends who joined our acceptance testing session.

I want to specially thank all my teachers, friends who helped me during my works, and family members for inspiring me with their moral support.

Finally, I feel deepest admiration to my department for giving me the honor to perform the thesis as a partial fulfillment of the Requirement for the Degree of Bachelor of Science in Computer Science

ABSTRACT

Objective of this project is to understand the existing National Election System in depth, to find out the problems in each stage. According to the findings we will try to give possible solutions of the problems in different stages in the context of Bangladesh. Our main objective is to find out a “Hybrid” solution for existing National Election System for a smoother & transparent way from using current infrastructure & resources.

TABLE OF CONTENTS

TITLE.....	i
DECLARATION.....	ii
ACKNOWLEDGEMENTS.....	iii
ABSTRACT.....	iv
TABLE OF CONTENTS.....	v
LIST OF TABLES.....	x
LIST OF FIGURES.....	xi

CHAPTER 1: INTRODUCTION

1.1	Information on Bangladesh Electoral System.....	1
1.2	Criteria for Election Systems.....	1
1.3	Voter Awareness.....	2
1.4	Gender and the Electoral Process.....	3
1.5	Training and Technology.....	4
	1.5.1 Training Objectives of Bangladesh Election Commission	5
	1.5.2 Training Programs.....	5
	1.5.3 Training through Election Commission.....	6
	1.5.4 Role of Radio and Television.....	6
	1.5.5 Training through Computer Technologies.....	7

1.6	Poll and Count.....	7
1.6.1	Before Poll.....	7
1.6.2	Poll.....	7
1.6.3	Count of Votes.....	9
1.6.4	Recount.....	10
1.7	Our Findings from the current National Election System.....	10
1.8	Voting System Used in Abroad.....	11
1.9	Our Proposed Solution.....	11
1.10	Our proposed Voting System.....	12
1.11	Feasibility of our solution.....	15
1.12	Advantages of the System.....	15
1.13	Limitations of the System.....	15
1.14	Module Design.....	16

CHAPTER 2: METHODOLOGY

2.1	System Development Methodology.....	18
2.2	RAD Methodology.....	18
2.3	Spiral Development Methodology.....	19
2.4	Advantages of the Spiral Model.....	19

CHAPTER 3: SYSTEM DEVELOPMENT

3.1	Project Initialization and Planning.....	21
3.1.1	Party Registration Module.....	21
3.1.1.1	Benefits.....	21
3.1.1.2	Special Issues.....	21
3.1.1.3	Feasibility Analysis.....	21
3.1.2	Constituency Registration Module.....	22
3.1.2.1	Benefits.....	22
3.1.2.2	Special Issues.....	22
3.1.2.3	Feasibility Analysis.....	23

3.1.3	Candidate Registration Module.....	23
3.1.3.1	Benefits.....	23
3.1.3.2	Special Issues.....	24
3.1.3.3	Feasibility Analysis.....	24
3.1.4	Voting Data Security Module.....	24
3.1.4.1	Benefits.....	24
3.1.4.2	Special Issues.....	25
3.1.4.3	Feasibility Analysis.....	25
3.1.5	Test Plan.....	25
3.2	Analysis.....	26
3.2.1	Building the Prototype.....	27
3.2.2	Review and Suggestions from Advisor.....	33
3.2.3	Identifying Improvements.....	34
3.2.3.1	Informal Benchmarking.....	34
3.2.3.2	Problem Analysis.....	34
3.2.3.3	Technology Analysis.....	34
3.2.3.4	Outcome Analysis.....	34
3.2.4	Designing the Data Flow Diagram.....	35
3.2.5	Context Diagram.....	36
3.2.6	Data Flow Diagram: Level – 0.....	37
3.3	Design.....	39
3.3.1	Data Modeling.....	40
3.3.2	Architecture Design.....	42
3.3.2.1	Advantage of such Architecture.....	43
3.3.2.2	Infrastructure.....	44
3.3.3	User Interface Design	46
3.3.3.1	Input Design.....	55
3.3.3.2	Output Design.....	55
3.3.4	Data Storage Design.....	55
3.3.4.1	Party Registration System.....	55

3.3.4.2	Constituency Registration System.....	56
3.3.4.3	Candidate Registration System.....	57
3.4	Implementation.....	58
3.4.1	Party Registration System.....	58
3.4.1.1	Pseudo code for Showing Details of Parties.....	58
3.4.2	Constituency Registration System.....	59
3.4.2.1	Pseudo code for Showing Details of Constituencies.....	59
3.4.3	Candidate Registration System.....	60
3.4.3.1	Pseudo code for Searching of Candidates.....	61
3.4.4	Vote-data Security System.....	63
3.4.4.1	Bouncy Castle Encryption Algorithm.....	63
3.4.4.2	Bouncy Castle Decryption Algorithm.....	65
CHAPTER 4: SYSTEM TESTING		
4.1	Unit testing and Integration Testing.....	67
4.2	System Testing.....	72
4.2.1	Manual of Input/output.....	72
4.2.2	Actual Input Output.....	74
4.3	Acceptance Testing.....	75
4.4	Test Data.....	76
4.5	Results.....	79
CHAPTER 5: USER MANUAL		
5.1	User Instructions for Administrators.....	81
5.1.1	Party Registration System.....	81
5.1.2	Constituency Registration System.....	81
5.1.3	Candidate Registration System.....	82
5.2	User Instruction for Voter.....	82
CONCLUSION.....		83

REFERENCES	84
APPENDICES	86

LIST OF TABLES

Table 3.3.4.1: PARTY.....	56
Table 3.3.4.2: CONSTITUENCY.....	56
Table 3.3.4.3: CANDIDATE.....	57
Table 3.3.4.4: CONSTITUENCIES_CANDIDATE.....	57
Table 4.1: Testing For Party Registration.....	67
Table 4.2: Testing For Constituency Registration.....	68
Table 4.3: Testing For Candidate Registration.....	69
Table 4.4: Testing For Candidate Search.....	70
Table 4.5: Testing for Encryption-Decryption of Voting Data.....	71

LIST OF FIGURES

Figure 1.10: Electronic Voting Device.....	14
Figure 1.14: Module Diagram of proposed Electronic Election System.....	16
Figure 2.4: The Spiral Model.....	20
Figure 3.2.1: Registration Module.....	28
Figure 3.2.2: Party Registration Module.....	29
Figure 3.2.3: Party Registration Data.....	29
Figure 3.2.4: Constituency Registration Module.....	30
Figure 3.2.5: Constituency Registration Data.....	31
Figure 3.2.6: Candidate Registration Module.....	32
Figure 3.2.7: Candidate Registration Data.....	32
Figure 3.2.8: Context Diagram for Hybrid Solution for National Election System.....	36
Figure 3.2.9: Level 0: DFD for Hybrid Solution for National Election System.....	37
Figure 3.2.10: Level 1 DFD for Hybrid Solution for National Election System.....	38
Figure 3.2.11: ER Diagram for Hybrid Solution for National Election System.....	41
Figure: 3.3.2 Computer Architecture.....	43
Figure: 3.3.3 Network Design.....	44
Figure 3.3.3.1: Party Registration.....	47
Figure 3.3.3.2: Party Registration: Party Details.....	48
Figure 3.3.3.3: Constituency Registration.....	49
Figure 3.3.3.4: Constituency Registration: Constituency Details.....	50
Figure 3.3.3.5: Candidate Registration.....	51
Figure 3.3.3.6: Candidate Registration: Candidate Searching.....	52
Figure 3.3.3.7: Voting Data Encryption.....	53

Figure 3.3.3.8: Encrypted Data.....	54
Figure 4.2.1: Vote Data Input.....	74
Figure 4.2.2: Decrypted Vote Data Stored in database server.....	75
Figure 4.5.1: Result by Constituency.....	79
Figure 4.5.2: Winning Candidate.....	80

CHAPTER 1

INTRODUCTION

1.1 Information on Bangladesh Electoral System

Bangladesh started its journey with Parliamentary System of Government, then switched over to Presidential System and in 1991 reverted back to Parliamentary system.

Parliament consists of three hundred members elected in accordance with law from single-member territorial constituencies. Besides this there was a provision for thirty seats reserved exclusively for women members up to the year 2000 who were elected according to law by the members of Parliament. Parliament has tenure of 5 years unless dissolved earlier.

1.2 Criteria for Election Systems

Based on the tradition of elections and voting systems in the Bangladesh, elections systems—whether through traditional voting methods or SMS voting are commonly expected to satisfy a number of criteria, including:

- Eligibility and Authentication - only authorized voters should be able to vote
- Uniqueness - no voter should be able to vote more than one time
- Accuracy - election systems should record the votes correctly
- Integrity - votes should not be able to be modified, forged, or deleted without detection
- Verifiability and Audit ability - it should be possible to verify that all votes have been correctly accounted for in the final election tally, and there should be reliable and demonstrably authentic election records
- Reliability - election systems should work robustly, without loss of any votes, even in the face of numerous failures, including failures of voting machines and total loss of Mobile communication

- Secrecy and Non-Coercibility - no one should be able to determine how any individual voted, and voters should not be able to prove how they voted (which would facilitate vote selling or coercion)
- Flexibility - election equipment should allow for a variety of ballot question formats (e.g., write-in candidates, survey questions) be compatible with a variety of standard platforms and technologies; and be accessible to people with disabilities
- Convenience - voters should be able to cast votes quickly with minimal equipment or skills
- Certifiability - election systems should be testable so that election officials have confidence that they meet the necessary criteria
- Transparency - voters should be able to possess a general knowledge and understanding of the voting process
- Cost-effectiveness - election systems should be affordable and efficient.

For new election systems to be adopted, it is likely that they will need to satisfy all, or nearly all, of these requirements.

1.3 Voter Awareness

Voter awareness is an important factor to conduct an election in a free, fair and impartial manner. Willingness of the eligible persons to be registered as voters and their participation in the voting process are important ingredients for a sound democratic process.

Right from enumeration work for registration of voters to the time of casting of votes at the Polling station, efforts are made to make people aware of their right of franchise and the importance of the exercise of this right. The Election Commission undertakes voter education programs on democracy and various aspects of election through different news media, cinema slides, Radio and TV.

The Mass Communication media, Department of Films and Publications also play significant roles to educate voters on their right of franchise and the method of casting votes. The Election Commission also arranges through the Divisional and District authorities including Thana administration meetings/rallies with the electorate, representatives of political parties, local elite and people of all walks of life for creating awareness about democracy, the right and value of franchise.

The public awareness campaign also includes a series of poster campaigns. Rallies and processions are organized to mobilize public support for free and fair elections. Local volunteers also organize special events like folk songs and drama.

Non-government organizations are also encouraged by the Election Commission to conduct voter education programs with the materials (posters, slides, films etc.) developed by them highlighting the importance of vote, the right of the voter, functions of the legislature, responsibilities of the elected representatives to the electorate.

The underlying idea of voter awareness programs is to ensure large-scale participation of citizens in the choice of their representatives so that establishment of a representative and responsible government is ensured.

1.4 Gender and the Electoral Process

Nearly fifty percent of the total populations in the country are women. It is, therefore, essential that they participate in large numbers in the electoral process.

In the electoral process, persons irrespective of gender status can contest the elections for general seat in the Parliament and also elections to local bodies.

During the last general elections to the Parliament in October 2001, 38 women contested in 46 general constituencies. Of them 6 won seats. One woman won in all the 5 seats she contested. Another woman won 4 seats out of 5 she contested. Besides, there are reserved seats for women candidates in the local level elections. But women participation in the electoral process has been found to be discouraged by a number of factors. Conservative women feel hesitant to meet male registration personnel due to social and religious restrictions. Potential violence and absence of convenient transportation system, especially in the rural areas, also discourage women from participating in the electoral process.

For the convenience of women voters, electoral rolls are prepared separately for them and separate polling booths are set up in the polling centers. Women polling personnel are generally appointed to help women voters go about meeting voting formalities in the polling station. Deployment of women security personnel and magistrates in and around the polling centers are preferred, so that women voters can cast their votes without intimidation, fear and hindrance. Extensive voter education program for large-scale female participation is also conducted. All these steps have resulted in noticeably large turnout of women voters in large numbers.

What is needed to attain their extensive participation in exercising suffrage is to motivate them adequately through education while creating a reassuring environment in which female voters can come to the polling station and cast their vote without intimidation and fear.

1.5 Training and Technology

Election is an integral part of the institution of democracy and as such, a free, fair and efficient election process is a must for safeguarding democracy. Effective and fairly conducted election largely depends on skilled and well-trained election

personnel as well as on the awareness of the voters and political activists about their franchise rights and knowledge of election rules and regulations.

1.5.1 Training Objectives of Bangladesh Election Commission

The Bangladesh Election Commission is putting in considerable efforts in making the existing election process effective and smooth. In a bid to cope with the changing circumstances and to familiarize the election officials, political activities and voters with the election process, the Election Commission has established one Electoral Training Institute in Dhaka. Since election process involves complex functions and procedures it is necessary that the election personnel take extensive training in performing their task properly and effectively. This applies also to voters and political activists so that they also share similar knowledge about election procedures. The objectives of such specialized training are:

- To create an efficient electoral management system.
- To provide training facilities for the polling personnel.
- To educate the polling agents and political activists.
- To make the voters aware about their civil, political and franchise rights.

1.5.2 Training Programs

So far training programs have been conducted on the methods and procedures of -

- Voter Registration.
- Up-dating the electoral rolls of election.
- Election offences.

- Pre-poll irregularities.
- Duties and responsibilities of the polling personnel.
- Role of Judicial officials of Electoral Enquiry Committees.
- Duties and responsibilities of law enforcing agencies.
- The requirement and the use of different forms, packets and materials at the polling station.
- Conducting polls, franchise rights and role of the voters.
- Role of observers.
- Role of political activists in ensuring fair election.
- Process of counting of votes.
- Preparation of ballot paper account.
- Statement of counts and consolidation of results etc.

1.5.3 Training through Election Commission

The Election Commission arranges several training programs for training of the polling personnel on election process centrally at the Electoral Training Institute in Dhaka as well as at Divisional, District and Thana/Upzila head quarters. Separate handbooks and manuals on election process for the guidance of the Returning Officers, Presiding and Assistant Presiding Officers, Polling Officers etc. are also prepared and distributed under the direction of the Election Commission.

1.5.4 Role of Radio and Television

Extensive use of the mass media including Radio & TV has been made in relaying voter education message through radio spots, documentaries, and short films etc.

1.5.5 Training through Computer Technologies

The Election Commission Secretariat already houses several stand-alone PCs. Projects are underway to equip the secretariat with modern powerful computers which will be connected to the computers located in all districts of Bangladesh. Upon successful completion of such countrywide network, the Election Commission Secretariat will be able to train all district election personnel through this network. The Electoral Training Institute that already uses some of its computers for preparing training materials will be able to send training manuals electronically to all district office computers.

1.6 Poll and Count

According to law, casting of votes and counting of votes are the pivotal and final tasks in the whole process of the election, though the consolidation of results and declaration of the names of returned candidates are the subsequent legal requirements.

1.6.1 Before Poll

The Returning Officer provides each Presiding Officer with necessary ballot boxes of such material and the Commission approves design as. Not more than one ballot box is used at a time for the purpose of the poll at any polling booth.

1.6.2 Poll

At least half an hour before the time fixed for the commencement of the poll, the Presiding Officer is required to ensure that every ballot box to be used is empty, show the empty ballot box to the contesting candidates and their election agents and polling agents whoever may be present, close and seal the ballot box and place the ballot box so as to be conveniently accessible to the elector visible to

all present in the booth officials and election or polling agents as may be present. Every voter will mark his ballot paper in secret before the same is folded and dropped in to ballot box by the voter.

The Presiding Officer regulates the number of voters to be admitted to the polling station at a time and excludes from the polling station all other persons except those connected with the polling. The Presiding Officer is responsible for keeping order at the polling station so that a voter can exercise his free will to cast his/her vote at the polling center.

Where a voter presents himself/herself at the polling station to vote, the Presiding Officer shall, after satisfying himself about his/her identity, issue to him/her a ballot paper after giving him/her a personal mark made with indelible ink on his/her thumb or any other finger of either hand, placing a mark on the electoral roll against the number and name of the voter to indicate that a ballot paper has been issued to him and recording the voter's number and procuring signature of the voter on the counter foils of electoral roll and ballot paper respectively .

The voter, on receiving the ballot paper, shall forthwith proceed to the place reserved for marking the ballot paper, put the prescribed mark on the ballot paper at any place within the space containing the name and symbol of the contesting candidate for whom he wishes to vote and after he has so marked, fold the ballot paper and insert it in the ballot box. He has to do the whole thing at the quickest speed.

If a person representing himself as a voter applies for a ballot paper when another person has already represented himself as that voter and has voted under the name of the person so applying, he shall be entitled to receive a ballot paper, which is called a tendered ballot paper. The Presiding Officer maintains separate accounts of tendered and challenged votes and also spoilt ballot papers as per law.

1.6.3 Count of Votes

The polling time is generally 0800-1600 hrs local time. No person is allowed entry into the polling station enclosure after 1600hrs.

Immediately after the close of the poll with the casting of vote by the last voter of the day, the Presiding Officer, in the presence of such of the contesting candidates, election agents, polling agents and election observers as may be present, proceeds with the count of votes.

The Presiding Officer gives such of the contesting candidates, election agents and polling agents as may be present, reasonable facility of observing the count and gives them such information with respect there to as can be given consistent with the orderly conduct of the count and the discharge of his duties in connection therewith.

Under the law no person other than the Presiding Officer, the Polling Officer, any other person on duty in connection with the poll, the contesting candidates, their election agents and polling agents are to be present at the count. However, authorized observers are allowed by the Election Commission to observe the count as a special dispensation. The Presiding Officer shall open the used ballot box or ballot boxes and count the entire lot of ballot papers taken out there from in presence of these persons.

The valid ballot papers cast in favor of each contesting candidate are preserved in separate packets. The Presiding Officer, immediately after the count, prepares a statement of the count and if so requested by any candidate or election agent or polling agent present, gives him a certified copy of the statement of the count and the ballot paper account. The Presiding Officer puts in good order all records of the poll and sends them to the Returning officer immediately.

The Returning Officer is required to give the contesting candidates and their

election agents a notice in writing of the day, time and place for the consolidation of the results and, in the presence of such of the contesting candidates and election agents as may be present, consolidate in the prescribed manner the results of the count furnished by the Presiding Officer, including there in, the postal ballots received by him before the time aforesaid.

1.6.4 Recount

The Returning Officer shall recount the valid ballot papers in respect of any polling station if the count by the Presiding Officer is challenged in writing by a contesting candidate or his election agent and the Returning Officer is satisfied about the reasonableness of the challenge or he is directed so to do by the Commission.

1.7 Our Findings from the current National Election System

Composite paper ballot elections have been prone to human error, particularly -

- Subjective discretion applied when deciding valid votes.
- Tallying votes when the deputy returning officer is communicating votes to the poll clerk orally.
- Transposition errors when carrying figures from tally sheets to final statements.

In addition, the operating costs associated with composite paper ballot elections are as much as three times that of an automated election. The increase in costs include –

- The requirement for more voting subdivisions with fewer voters to ensure the manageability of the counting process.

- The employment of staff at the voting places and additional staff to count ballots at the close of voting and
- The associated recount costs.

1.8 Voting System Used in Abroad

It examines the following types of voting systems:

- Mechanical Lever Machines
- Punch cards
- Optical Mark Reading (Optical Scan)
- Direct Recording Electronic (Touch Screen)
- Telephone
- Mail
- Automated Terminals or Kiosks
- Internet

1.9 Our Proposed Solution

- Greater professionalism, transparency and accountability in delivering cost-effective elections.
- Re-delimitation of the country into voting districts to improve access to polling stations.
- Increasing voter participation.
- Conducting ongoing and specific registration activities to grow the existing voters' roll.

- Enhancing the information technology (IT) infrastructure.
- Increasing the use of emerging technologies to improve efficiency.
- Counting, verification and announcing of results within short period of time.

To improve the overall efficiency of this processes and to provide multiple service channels to both its election commission employees and the public, we implemented leading edge Short Message Service (SMS). The SMS and Wireless Application Protocol (WAP) services provided included the following:

- On Election Day the voter will cast their vote by pressing the button and through SMS (Short Message Service) system this vote will send to the main database server. At the end of the Election Day the database server will automatically generate the result for each constituency.
- Voters could obtain voter registration information using their mobile phone simply by sending an SMS with their 13-digit identity number. The voters would then receive reply SMS containing information about their voter status and where they were registered to vote.
- The public SMS service was expanded during election period to provide the public with news headlines and election results. The public could obtain national election results by sending an SMS with key words.

1.10 Our proposed Voting System

Our system works in three phases. The workflow of our system is described below:

- **Initial Setup of the System:**
 - *Mobile Phone Registration:* Each Polling Booth will be registered with a unique mobile number in the system's database
 - *Candidate Registration:* Each candidate will be registered in the system's database with their unique candidate ID's
 - *Party and Constituency Registration:* Each party and constituency will be registered in the system's database with their detail information

- **Vote Casting Process:**
 - *Voter Authentication:* When a voter comes to the polling center for voting he/she is manually authenticated by the Polling Officer whether he/she is a valid voter
 - *Electronic Voting:* Voters send the unique candidate IDs as their votes using the Voting Device which utilizes SMS technology
 - *SMS Delivery Notification:* Voter is notified of successful SMS delivery. The mobile network service providers like GP, Aktel, and Bangla Link etc will do this.
 - *Invalid Vote Cast Notification:* Voter is notified of unsuccessful Vote Cast like invalid voting format or mobile number
 - *Electronic Vote Recording:* Successful vote casts are updated in the database server accordingly

- **Result Generation:**
 - *Electronic Vote Counting:* After polling hour Super User initiates the counting command, the stored data is then retrieved from the database for counting by the system
 - *Electronic Report Generation:* Based on the counting results the system will generate following reports:

- Result by Constituency
- Result for each polling center
- Determining the winning candidate

In the Vote Casting Process for voting we will use an Electronic Device on the National Election Day. The device will have two components. First one is a Control Unit, which will be kept to the Polling Officer to Activate the Voting Machine. Another one is the main voting machine, which will be kept into the Polling Booth. The voter will just have to press the button besides his/her preferred candidate. Voters can select any candidate for several times till he/she press the final voting button. Once the voter press the final Voting button the vote will be casted and the device will be inactive. Now again the Polling Officer will have to re-active the device by pressing the control button for next voter.

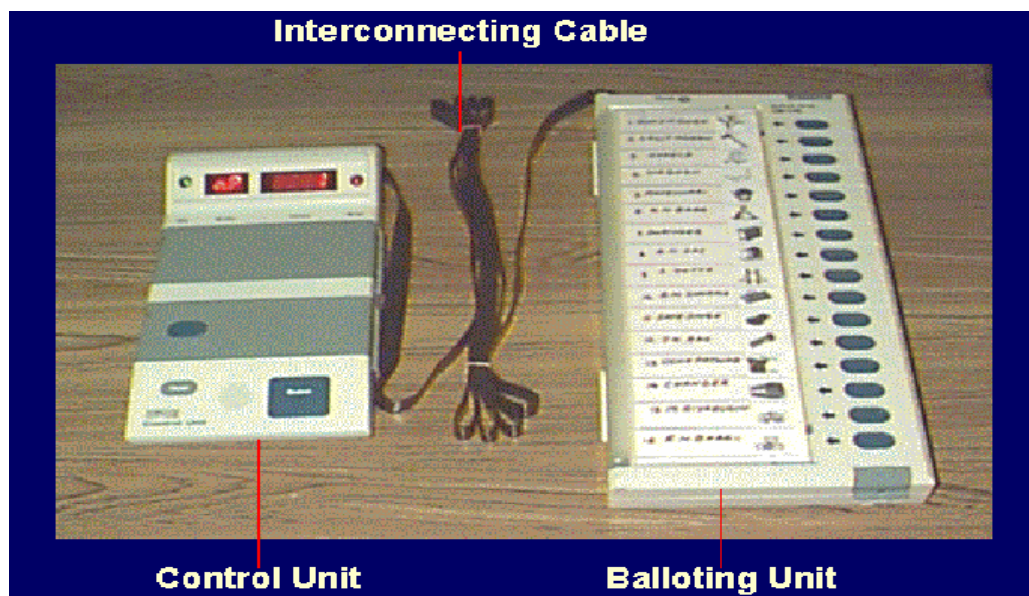


Figure 1.10: Electronic Voting Device

For the Demo Software we used Mobile phone instead of Electronic Voting Device

1.11 Feasibility of our solution

- May be initially installed in highly risked areas where the risk of ballot box hijacking is very high. We can use our system as the Pilot Project.
- For election it is possible to switch off all the mobile connections except registered mobiles with Dedicated Network.
- So the possibility of the mobile network congestion will not occur as there will be less numbers of mobiles under each Base Transceiver Station (BTS)
- Our system will be re-usable in the next election by simply resetting the machine
- It is a very simple system to operate and can be installed in short time.

1.12 Advantages of the System

- System has simple voting interface for the voters.
- System Counts and Generates Results automatically within short period of time.
- By using our system Involvement of high human workforce will go down
- This system is more Secured, more Dependable and more Efficient

1.13 Limitations of the System

- Though we implemented the voting data encryption-decryption but has not yet been integrated to the system
- We could not able to test the system with huge amount of data for shortage of human resource
- We could not able to test the system with huge number of mobiles for the shortage of adequate number of mobile phones

1.14 Module Design

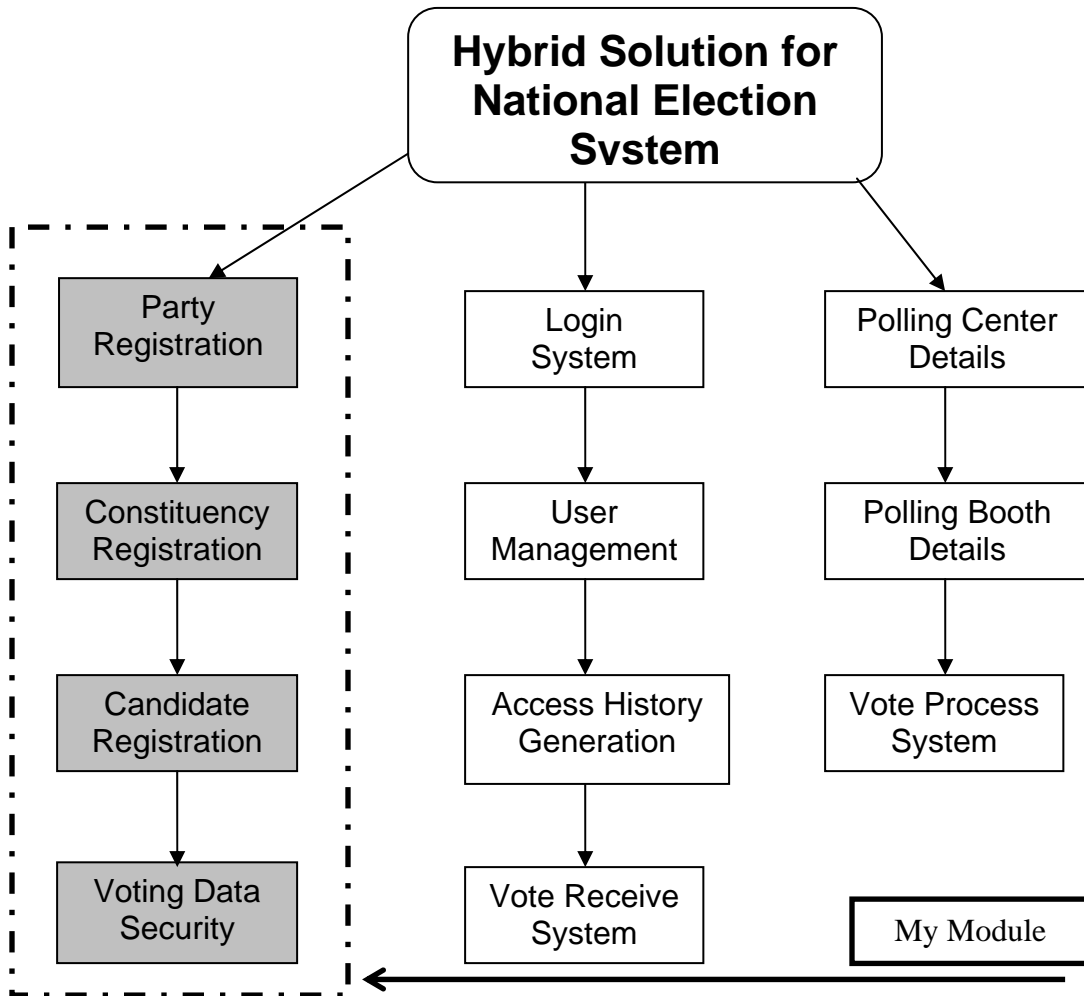


Figure 1.14: Module Diagram of proposed Electronic Election System

The upper figure shows the full system block diagram for an interactive participatory solution to Hybrid Solution for National Election System. There are 11 modules in the diagram that were distributed to the team members. The list of the team members and corresponding modules are as follows:

Team Members	Modules
1. <i>MD. Naimuzzaman</i>	<i>Party Registration</i> <i>Constituency Registration</i> <i>Candidate Registration</i> <i>Voting Data Security</i>
2. MD. Hasanul Bari	Login System User management Access History Generation Vote receive System
3. MD. Rashidul Hasan	Polling center Details Polling booth details setup Vote process System

CHAPTER 2

METHODOLOGY

2.1 System Development Methodology

The systems development methodology is meant to provide a uniform approach to managing systems development while providing sufficient flexibility to choose the techniques and tools best suited for a specific task. It is to be used as a guideline to all of those involved in systems development, acquisition, implementation, and conversion. Each model defines the deliverables that are to be produced during the process as well as the tasks to be performed and who is to perform them. It also defines what should be created and what tasks are likely to be executed to create the deliverable

As we were to develop National Election System software where we need a huge amount of data collection like constituencies details, polling center details, candidate details and party details so we chose RAD (Rapid Application Development) methodology for our system development. There was another reason behind that we had only 5 weeks ahead us when we started that means we had time constraints.

“Rapid Application Development (RAD) is a development lifecycle designed to give much faster development and higher quality than the traditional lifecycle. It is designed to take advantage of powerful development software. RAD is used for building large Information System applications of the kind which occur in every large business.”

- Rapid Applications Development by James Martin

2.2 RAD Methodology

A methodology must be used which has been adapted to match the needs of the toolset being used. Toolsets should integrate:

- Prototyping

- Graphical computer aided modeling and design
- A repository of design information and reusable components
- Automation for enforcing design integrity
- Integrated code generator, testing tools
- Thorough end-user interaction with developer, aided by tools

2.3 Spiral Development Methodology

In our system development process we used throwaway prototyping. Our throwaway prototyping methodology is a modified version of the spiral development methodology developed by Barry W. Boehm, "A Spiral Model of Software Development and Enhancement" Computer, May 1988, 21(5): 61-72.

2.4 Advantages of the Spiral Model

- The spiral model is a realistic approach to the development of large-scale software products because the software evolves as the process progresses. In addition, the developer and the client better understand and react to risks at each evolutionary level.
- The model uses prototyping as a risk reduction mechanism and allows for the development of prototypes at any stage of the evolutionary development.
- It maintains a systematic stepwise approach, like the classic life cycle model, but incorporates it into an iterative framework that more reflect the real world.
- If employed correctly, this model should reduce risks before they become problematic, as consideration of technical risks are considered at all stages.

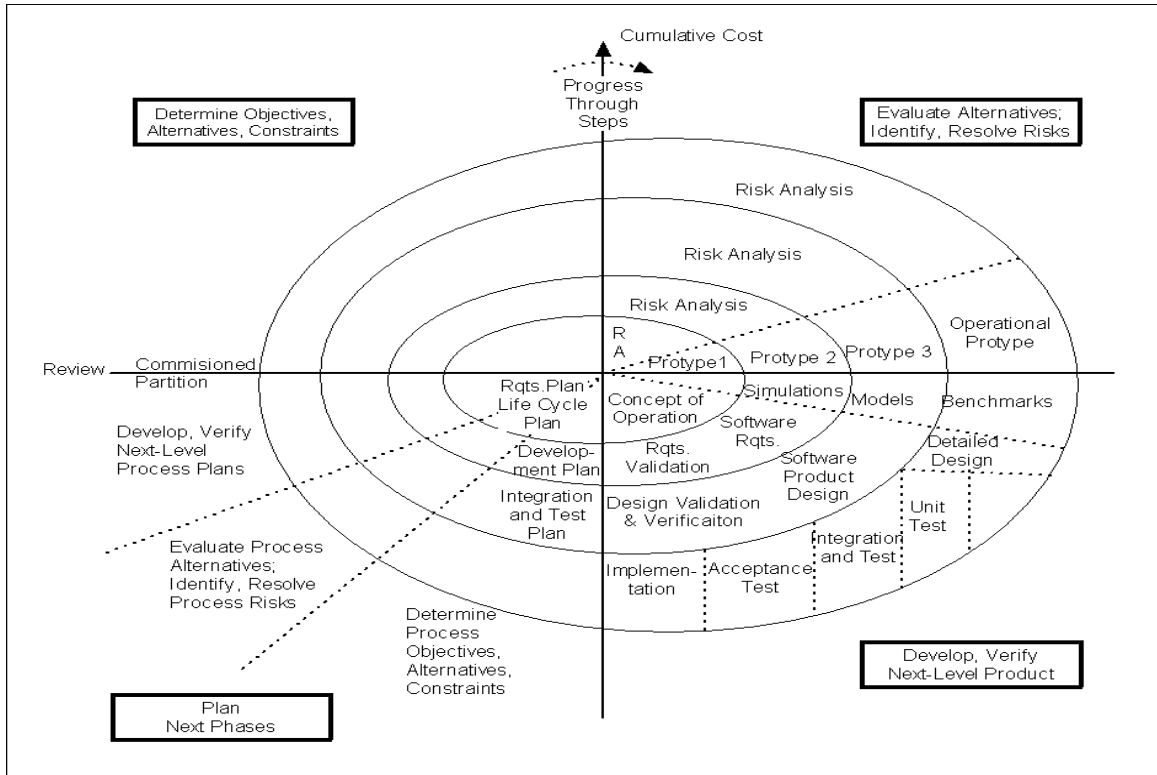


Figure 2.4: The Spiral Model

CHAPTER 3

SYSTEM DEVELOPMENT

3.1 Project Initialization and Planning

3.1.1 Party Registration Module

As our system is an election system so there has to be a registration module where party details will be input. The administrator does this registration because there is a matter of security. Otherwise unauthorized party name can be registered. Party Registration module process includes the following tasks:

- Party registration
- Register the party name
- Register the party ID number
- Administrators can see the details of the parties

3.1.1.1 Benefits

- Can get detail list of contesting parties
- Easy to get the party list
- Easy to generate reports based on parties

3.1.1.2 Special Issues

This module is secured by the authentication of administrators so, other users will not be able to give the inputs. It shows the detail list of registered parties.

3.1.1.3 Feasibility Analysis

- Party registration is done manually which is a lengthy process. Hence this process is easier, short and faster

- In existing party registration scheme, they use MS Excel to store information which is not secured whereas my module gives total storage security

3.1.2 Constituency Registration Module

The election is done in 300 constituencies and constituencies generate results. So, registration of constituencies is a mandatory process. The election commissions determine name of constituencies. The administrator does this registration because there is a matter of security. Otherwise an unauthorized constituency name can be registered. Constituency registration module is a process that does the following tasks:

- Constituency registration all over the country
- Constituency name registration
- Assign unique ID number
- Assign District name and division name
- It shows detail candidate list of any constituency

3.1.2.1 Benefits

- Get list of registered constituencies
- Easy to get constituency details
- Easy to generate reports based on constituencies

3.1.2.2 Special Issues

This module is secured by the authentication of administrators so, other users will not be able to give the inputs. It shows the detail list of registered constituencies.

3.1.2.3 Feasibility Analysis

- Constituency list is made manually which is a lengthy process. Hence this process is easier, short and faster
- In existing constituency registration scheme, they use MS Excel to store information which is not secured whereas my module gives total storage security

3.1.3 Candidate Registration Module

In case of election, vote is done against the candidates of several parties. So candidate registration is very important for election system. The administrator does this registration because there is a matter of security. Otherwise any candidate name can be registered. Candidate registration module is a process that does the following tasks:

- Candidates registration against parties
- Candidate name registration
- Candidate ID registration
- Registration of symbol of the candidate/party for which he/she is contesting and other details
- It shows detail candidate list of any constituency

3.1.3.1 Benefits

- Get list of candidates list of any constituency
- Can search the a candidate by his/her name, ID or constituency
- Easy to get candidate details
- Easy to generate reports based on candidates

3.1.3.2 Special Issues

This module is secured by the authentication of administrators so, other users will not be able to give the inputs. It shows the detail list of registered candidates. It also gives the option to search for an individual candidate

3.1.3.3 Feasibility Analysis

- Candidate registration is done manually which is a lengthy process. Hence our process is easier, short and faster
- Use MS Excel to store information, which is not secured. It gives the storage security
- Effective searching method

3.1.4 Voting Data Security Module

As our system is an election system so there has to be a voting data security module where the voting data will be encrypted and sent to the database server. The encrypted data that has been received through SMS will now be decrypted and then stored in database accordingly. The encryption-decryption both is implicit modules of the system. This makes the system more reliable by protecting the vulnerable data from unauthorized access. Voting Data Security module process includes the following tasks:

- Encrypting Voting Data before sending to the database server
- Decrypting Voting Data before storing in the database server

3.1.4.1 Benefits

- More Secured data

- More Reliability

3.1.4.2 Special Issues

This makes the system more reliable by protecting the vulnerable data from unauthorized access. Makes the system more robust by protecting it from the hackers.

3.1.4.3 Feasibility Analysis

- Current Election System is more dependable on human integrity and honesty, which is very risky and uncertain. On the other hand this module enhances system's security by automatically encrypting and decrypting using its own methodology and thus avoids human interferences.
- Encryption-decryption is implicit to the system which is not visible to anybody including the administrators

3.1.5 Test Plan

There is often a temptation to rush into testing as soon as the very first program modules are complete and spontaneously test different events and possibilities without spending time to develop a comprehensive test plan. This is dangerous because important tests may be overlooked, and if error does occur, it may be difficult to reproduce the exact sequence of events that caused it. So instead, testing like that we do testing systematically and the results keep inform of documentation so that we must know what has and has not been tested. Below is my test plan sequence:

Unit Testing: Unit testing focuses on one unit- Party input module, candidate input module, constituency input module, data security module; it focused on the performance of each module that I built. I used black-box testing method as being a programmer I tested the unit. So, no need for interpretation. [Ref to testing, Chapter 5]

Integration tests: After my unit testing I checked whether my modules worked properly. So I ensured that the interfaces and the linkage between my modules are working accurately. The focus moved to the flow of controls among my first three modules and on the data sending from mobile device to server securely.

System tests: Our respected supervisor conducted system testing. Our complete system was tested in broad version. It examined how well the system meets our national election purposes and its usability, security, and performance under heavy load.

Acceptance testing: It was more likely beta testing. Our real virtual remote users were sitting back as users and our respected supervisor conducted the polling. There were no test data. We used real data and closely monitor the system for errors or use.

3.2 Analysis

Requirement analysis unambiguously describes what has to be built. There are many ways of specifying requirements like plans, models, prototypes and simulation. Prototyping is excellent choice because they best enable the project team to adjust the functionality in the system on the basis of a specific delivery date. We being the project developer had our solution with mobile technology and we use SMS for communication. It is a new technology adopted by the

computer programmer. So there is high risk with such technology. Prototype is particular appropriate for a lack of familiarity with technology because it explicitly encourages the developers to develop design prototypes for areas with high risks. So we had chosen prototype for our initial requirement gathering after fieldwork of requirement gathering.

3.2.1 Building the Prototype

There are two important aspects here. One aspect is communication. In all of these processes it is necessary to reach agreement, to specify what we are to do and to represent it in an unambiguous way. The second aspect is organization of this work into a process that must eventually produce a new system. Doing so is not an easy work to accomplish. Our respective supervisor asked us to go to the National Election Commission (NEC) to know in depth the whole election process. We first talked to the External Relation Officer (ERO) to know the whole working system on the Election Day. We tried to find out how the voting is done and who plays the roles of several responsibilities. Then we personally did all steps of voting like coming to the polling center to result generation. We also did some paper works to calculate the time difference between existing system and our planned system. We were concerned about the triggers in the complete scenario. We must need to understand some important aspects:

- The main objectives that drive how voting is done
- The information people need for the voters and also to do vote
- The data (party info, candidate info, constituency info, voter info) handled within the NEC
- When, how, and by whom vote are counted
- The sequence of voting process
- Security, counting, result generation issues

To work out such difficulty our supervisor recommended us to put up a prototype model. He advised us to exploit excel as the computer tool. Because in excel we be able to see the unprocessed data in front of us and then also monitor the data flow which can solve our data-handling problem. So we designed our prototype using excel and macros. We noticed that here we have three stakeholders; first stake holder is developer who will design and offer program, NEC are responsible for storing votes and other information and also for result generation and voters will cast their votes. Therefore, we divided entire process in respect of activities.

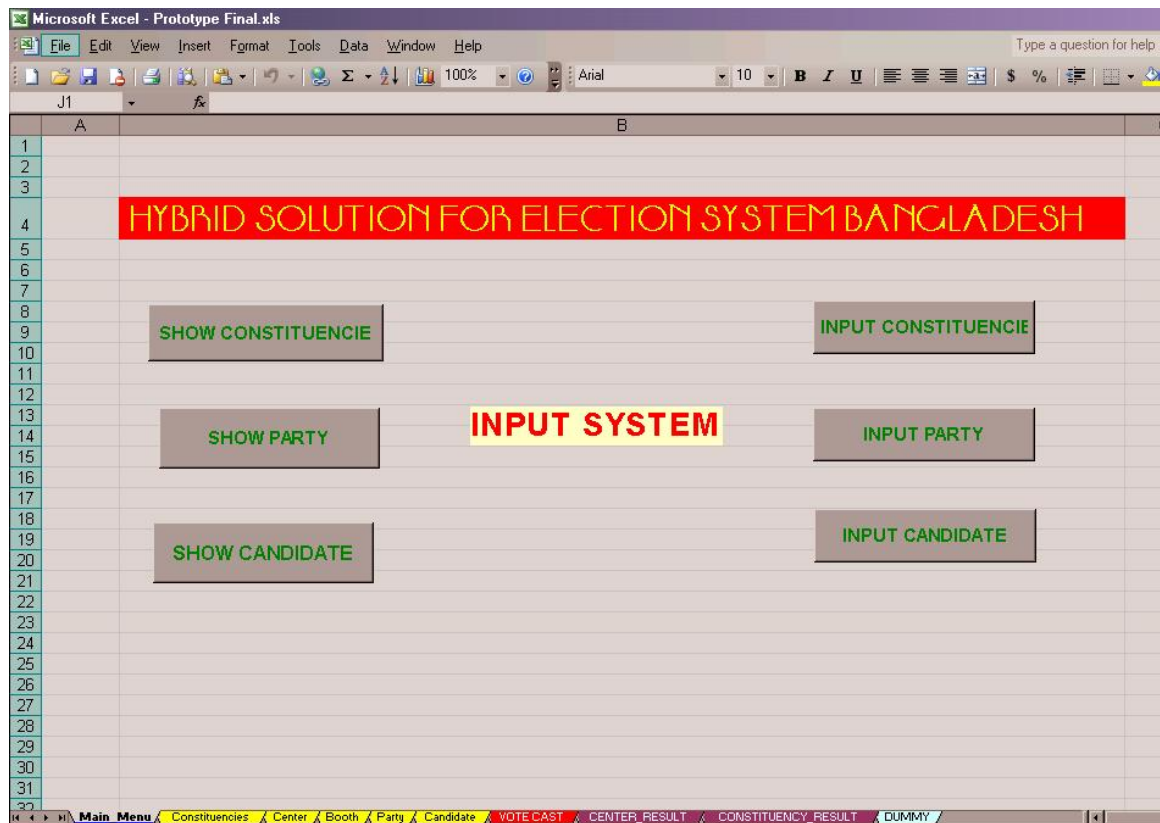


Figure 3.2.1: Registration Module

At the beginning I tried to figure out what types of information are required to do the voting for the National Election. As my module was registration of parties, candidates, and constituencies by giving inputs necessary information, I worked out that module. I, using visual basic scripts on excel, designed the interface and put data. I saved that data on another excel sheet. Thus I distinguished and observed the data flow.

The screenshot shows a dialog box titled 'UserForm1'. It has a title bar with a close button. The main area contains three text boxes for input: 'Party Name' (a wide box), 'Party Number' (a narrow box), and 'Symbol' (a wide box). Below these are two buttons: 'SAVE' on the left and 'EXIT' on the right.

Figure 3.2.2: Party Registration Module

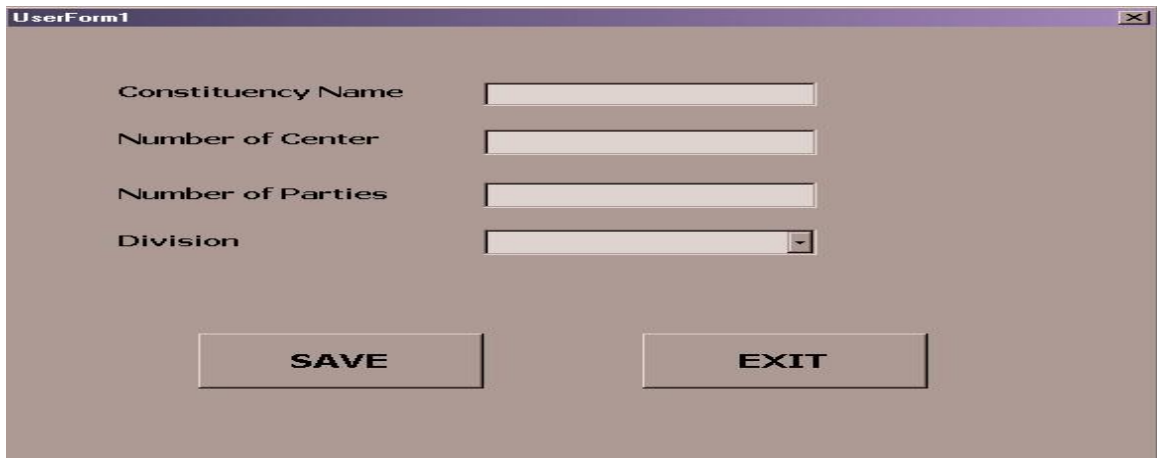
The screenshot shows an Excel spreadsheet with the following data:

party_name	party_no	symbol
BAL (Bangladesh Awamileague)	1	Boat
BNP	2	Sheaf of Paddy
JAMAT	3	Kula
Independent	4	clock

A red banner at the top of the spreadsheet reads "HYBRID SOLUTION FOR ELECTION SYSTEM BANGLADES". A button labeled "GO TO MAIN MENU" is located on the right side of the spreadsheet.

Figure 3.2.3: Party Registration Data

In figure 3.2.2, you can see that the administrator is doing registration of a party by registering party name, number and symbol of the party. Here I gave the party number to identify the parties because there were more than 450 independent candidates in last National Election and their party name is "*Independent*". Figure 3.2.3 shows that how the information are stored in the excel sheet. These data will be used to compare



The image shows a software window titled "UserForm1" with a light brown background. It contains a registration form with four input fields and two buttons. The fields are labeled "Constituency Name", "Number of Center", "Number of Parties", and "Division". The "Division" field is a dropdown menu. Below the fields are two buttons labeled "SAVE" and "EXIT".

Figure 3.2.4: Constituency Registration Module

name_of_constituencies	no_of_center	no_of_parties	division
Dhaka-1	12	21	Dhaka
Dhaka-2	13	4	Dhaka
Dhaka-3	34	8	Dhaka

Possible Divisions

- Dhaka
- Khulna
- Rajshahi
- Barishal
- Sylhet
- Chitagong

Figure 3.2.5: Constituency Registration Data

Constituency registration is also similar to party registration. In figure 3.2.4 you can see that the administrator is giving the input of Constituency name, number of centers where voting will take place, number of parties that is how many party will contest under an individual constituency and the division. We are taking division name, as we have to generate result according to the division also. In figure 3.2.5, it shows how the data are stored in the excel sheet. Here we did not give any constituency ID as every constituency name is like an ID. For example “Dahaka-1”, “Dhaka-2”, “Chittagong-1” etc, all of the constituencies’ names is unique. So here we don not need any other ID.

Thus I gained knowledge about how to make the flow of data and handled those in my input module.

The screenshot shows a window titled 'UserForm1' with a light gray background. It contains three input fields: 'Candidate Name' (a text box), 'Party Number' (a dropdown menu), and 'Constituency Name' (a dropdown menu). To the right of the 'Party Number' dropdown is a 'Sex' dropdown menu. At the bottom of the form are two buttons: 'SAVE' and 'EXIT'.

Figure 3.2.6: Candidate Registration Module

The screenshot shows an Excel spreadsheet with a red header row containing the text 'HYBRID SOLUTION FOR ELECTION SYSTEM BANGLADESH'. Below the header is a table with the following data:

candidate_name	party_no	name_of_constituencies	sex
Naim	1	Dhaka-1	M
Biplu	2	Dhaka-1	M
Eshita	3	Dhaka-1	F
Korim	1	Dhaka-2	M
Rohim	2	Dhaka-2	M
Akmol	3	Dhaka-3	M
Fatema	1	Dhaka-3	F

To the right of the table, there is a button labeled 'GO TO MAIN MENU' and a dropdown menu labeled 'Possible Sex' with options 'M' and 'F'.

Figure 3.2.7: Candidate Registration Data

Candidate registration is also similar to party registration in figure 3.2.6 you can see that the administrator is giving the input of candidate name, party name for

which he/she is contesting, constituency name from where he/she is contesting and sex whether he/she is male or female. In figure 3.2.7, it shows how the data are stored in the excel sheet. Here we could use the party name instead of party number. But we used party number to make the query easier.

3.2.2 Review and Suggestions from Advisor

During our presentation of the prototype, our supervisor and other respective teachers were keen about the proper input and checking. They asked about the data flow and showed some techniques to handle data properly. Regarding my module they pointed out some key issues:

- How to store data in smart way
- How the voting data can be secured
- How to pass party, candidate, constituency information to other working module
- How to deal if there are same names of two candidate in the same constituency
- How to deal with the Independent candidates
- What else information I may need for the candidates, parties and constituencies
- How to check duplicate party name except “Independent” and also constituency name
- Searching

Now again they advised me to find out some solutions to these issues and asked me to modify the prototype. After modifying the prototype my supervisor asked to formulate a real working database. Because after the excel prototype I gathered ideas about the data flow and I had a clear visualization of what are the things to do next.

3.2.3 Identifying Improvements

3.2.3.1 Informal Benchmarking

The first step in the strategy was to informally benchmark existing polling system scenario of some polling center. Our aim was to identify those techniques and features that usually make a polling center ideal polling environment.

3.2.3.2 Problem Analysis

Since the National Election Commission has the best idea about the whole polling system. So we went there and interviewed the external relation officer to understand the whole system. We tried out the problems with the existing system and the solutions. They told us where they face major problems and what can be better for them. Thus I carried out the problem analysis.

3.2.3.3 Technology Analysis

The next step was to analysis the technology. Firstly, I decided to take a look of there system, how they maintain the data. Then I took help from the internet. I looked for how in abroad these data are handled. I also gathered some knowledge about the interface from the existing ERP. We were concern about the proper and necessary input and out.

3.2.3.4 Outcome Analysis

The goal of outcome analysis is to promote creative thinking to develop other ways of create business value of our system. Our whole team finally integrates the improvement ideas and develops as outline of the final system. After some

refine in it into more details through the prototype, our final system will be used as Pilot project for testing and at the end will be used as full working system.

3.2.4 Designing the Data Flow Diagram

The data flow methods center around modeling both the system and the subjects' worlds, although they use mainly system world terms. Consequently, they require analysis to have particular skills in expressing subject world requirements in system world terms. Models in structured systems analysis are made up of three components: the process, the data and the system functions. Data flow diagrams model system processes and are one of the most important modeling tools used by the system analysts.

Although the data flow diagram implies a focus on data, this is not the case. The focus is mainly on the process or activities that are performed [2]. Data modeling, we will prepare from data flow, presents how the data created and used by processes are organized. I will try to present a combination of logical DFD and physical DFD so that I can easily convert them to entity relationship diagram and then finally able to find data modeling.

I will first describe how I modeled the systems using data flow symbols. A common way to begin is to model the whole system by one process. The DFD that does this is known as the context diagram. It shows all the external entities that interact with the system and the data flows between these external entities and the system.

The figure below shows the data flow in respect of context view. It models the "Hybrid Solution for National Election System". This system interacts with three external entities: Party Registration, Constituency Registration and Candidate Registration, Voting Data Security.

3.2.5 Context Diagram

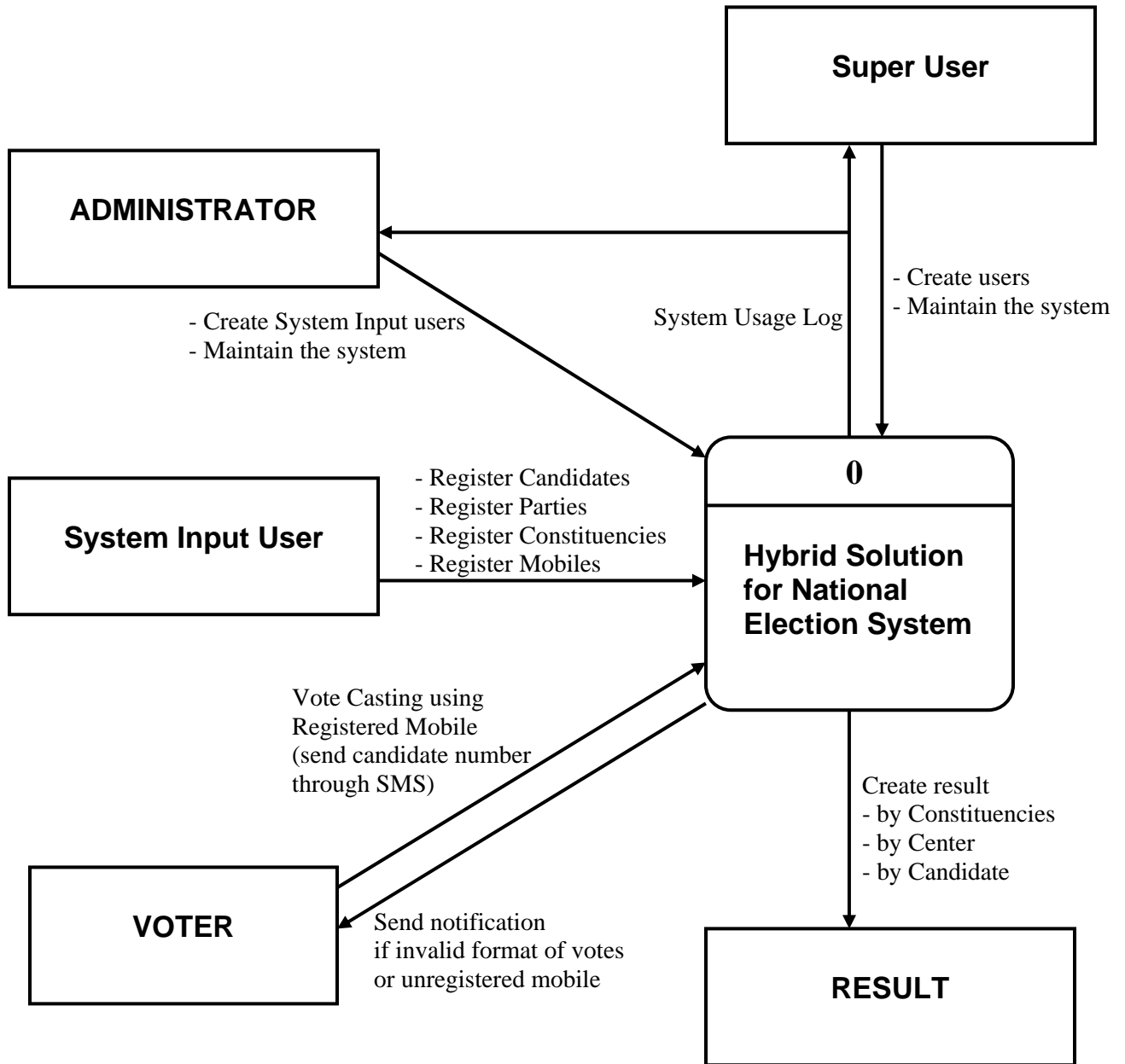


Figure 3.2.8: Context Diagram for Hybrid Solution for National Election System

3.2.6 Data Flow Diagram: Level - 0

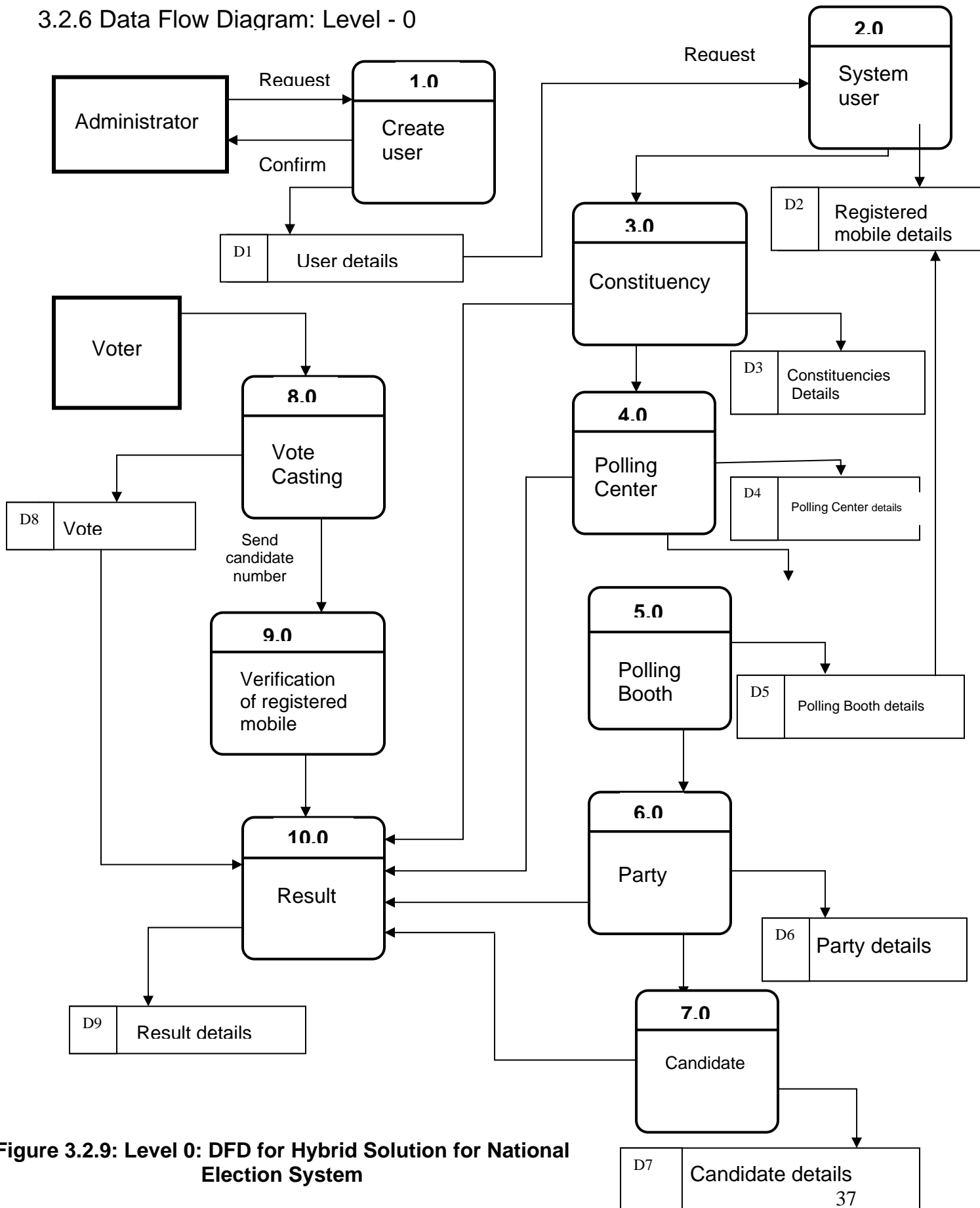


Figure 3.2.9: Level 0: DFD for Hybrid Solution for National Election System

Level -1 DFD

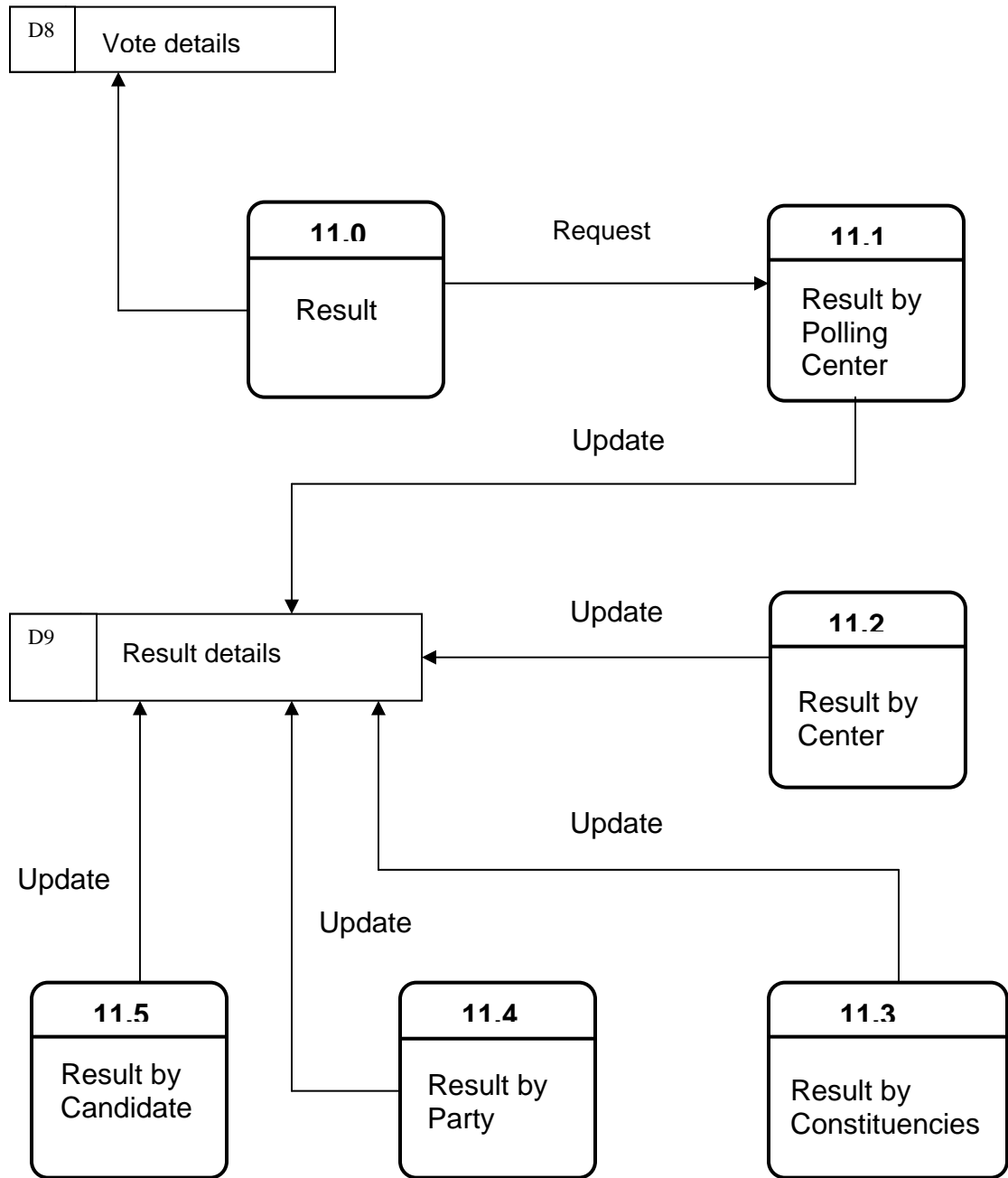


Figure 3.2.10: Level 1 DFD for Hybrid Solution for National Election System

3.3 Design

The design phase of the systems development life cycle used the requirements that were gathered during analysis to create a blueprint for the proposed system. A successful design builds on what was learned in earlier phases and leads to a smooth implementation by creating a clear, accurate plan of what needs to be done. The objectives are:

- Understand the initial transaction from analysis to design
- Be able to create physical data flow diagrams and entity relationship diagram
- Be familiar with the custom, package, and outsource design alternatives [2]

Throughout the design phase, I carefully considered the new system with respect to the current environment and systems that exist within current infrastructure. Major considerations of the “how” of a system are environmental factors, such as integrating with existing systems, converting data from legacy systems and leveraging skills that exist in-house [2]. Although planning and analysis phases are taken with prototype, the goal of my design phase is to create a final blueprint for my system that makes sense to easily implement.

I have divided the design phase into four sub-phases:

1. Data Modeling
2. Architecture Design
3. User Interface Design
4. Data Storage Design

3.3.1 Data Modeling

A data model is a formal way of representing the data that are used and created by a business system. It illustrates people, places or things about which information is captured and how they are related to each other [2]. A data model describes the data that support the whole system processes in a proposed system. During the analysis phase, all models represent the logical organization of data without indicating how the data are stored, created, or manipulated so that we can focus on requirement without being distracted by technical details. In the design phase, analyst draw data model to reflect how the data will physically be stored in databases and files. So in this sub-phase my main objective is to be able to create an entity relationship diagram. In between we must understand how to balance between entity relationship diagrams and data flow diagrams.

Entity Relationship Diagram

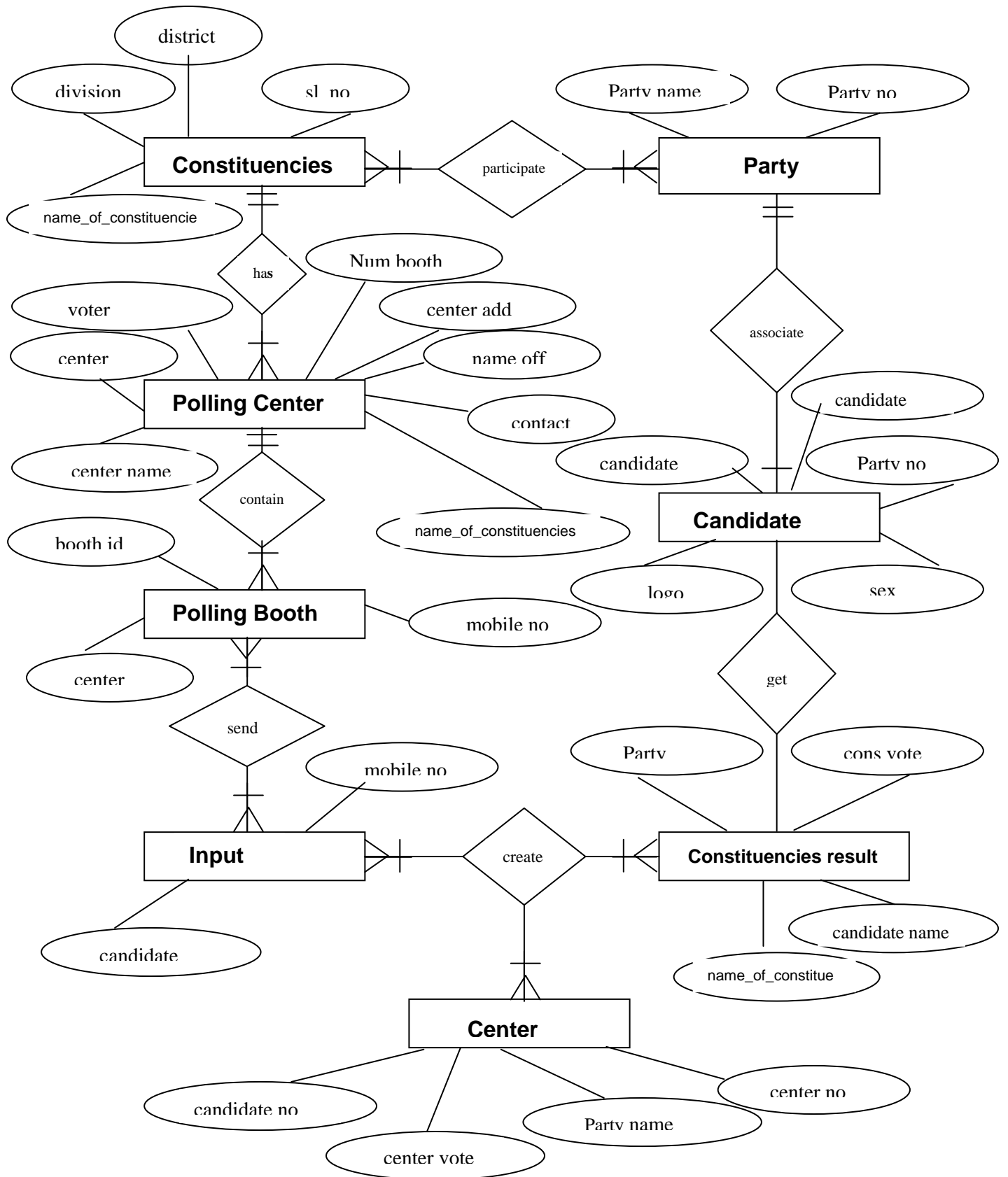


Figure 3.2.10: ER Diagram for Hybrid Solution for National Election System

3.3.2 Architecture Design

An important component of the design phase is the architecture design, which describes the proposed technical environment for the new system. The technical environment contains the hardware, software and communications infrastructure on which the new system will be created and the methods for supporting the system's security need and global requirements. The deliverable from the architecture design contains the network model, the hardware and software specification, and the plan for security and global support [2].

Computer Architecture: There are three fundamental computing architectures. In server-based computing, the server performs virtually all of the work. In client-based computing, the client computers are responsible for most of the application functions. In client-server computing, the work is shared between the servers and clients.

We have used the client server architecture with attempting to balance the processing between the client and the server by having both do some of the application functions. In this design the client computer will have our software, whereas the server is responsible for the data access logic and data storage. The application in resides on the client fully.

As we have mobile functionality, we have connected the mobile with our client machine. Now days we know mobile have operating system like computers. So we can describe our architecture as three-tiered architecture by definition. Votes are going to database server from mobile through client server. Here client server is acting like an application server. Other inputs like party, constituency and candidate inputs are going to database server from the application server. We have used both windows based server and client. We used ORACLE as database server and Visual Basic for application server

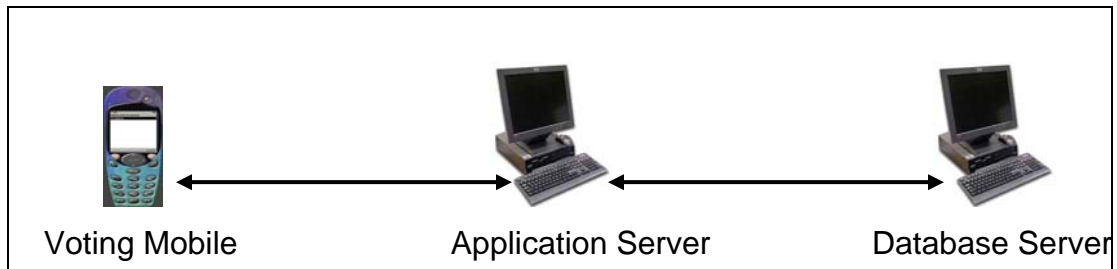


Figure: 3.3.2 Computer Architecture

3.3.2.1 Advantage of such Architecture

Cost of infrastructure: one of the strongest driving forces toward client-server architectures is the cost of infrastructure [4]. Earlier we thought of server and the cost increases surprisingly. Simply putting the personal computers are ten times cheaper than the server.

Control and Security: our core database server is far away from the input device. It needs access right and security code to access and run a query. The software has the password protection so that only authorized user can handle the application server.

Scalability: scalability refers to the ability to increase or decrease the capacity of the computing infrastructure in response to the changing capacity needs [2]. We were pretty concern about the SMS load and we designed in such a way that if we need to increase the receiving power in future, we can only add a mobile to the application server. If we need further, we can simply add another application server along a mobile with the database server. Such our designed is scalable in respect with time.

3.3.2.2 Infrastructure

In our cases, we built a system that has hardware, software and communication infrastructure already in place. As we do not have any technological infrastructure in our rural areas and that is the target market of our system. Further, the coordination of infrastructure components was our main issue during design. Below I tried to summarize some of the key elements of infrastructure design to give a clear view:

Network Model: The network model is a diagram that shows the major components of the information system (IS), such as servers, communication lines, and networks [2]. As we are using the mobile phone, so our network model is the existing mobile network in our country except the server portion. Creating the network model is a top-down exercise whereby we first graphically depict all of the locations where the application will reside [4]. But our aim to spread out our solution through out the country with the help of mobile network. So we will consider an area and show the network model of that particular part.

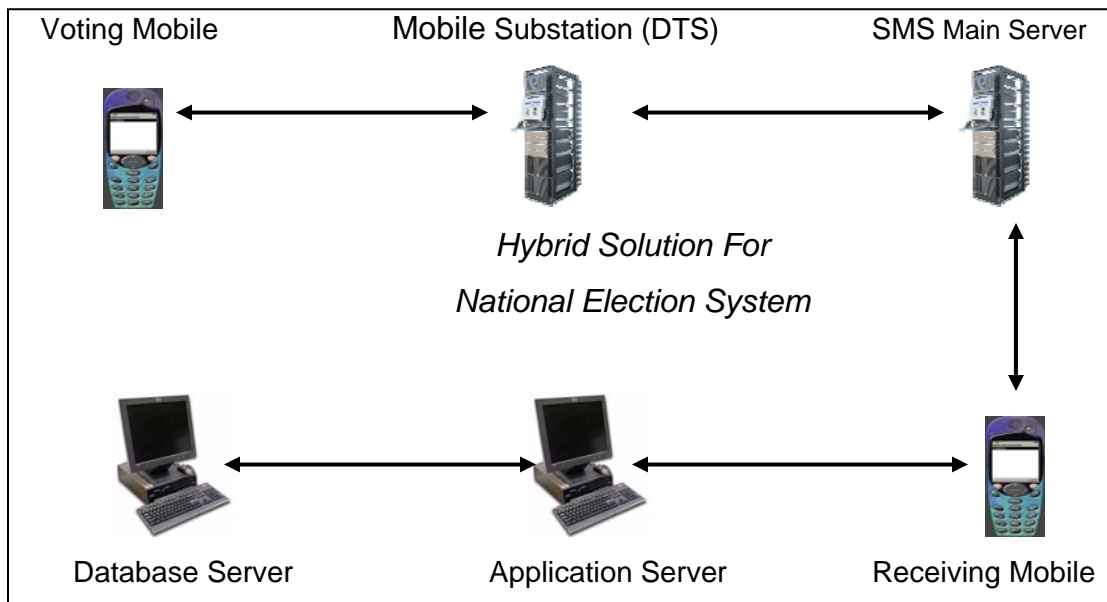


Figure: 3.3.3 Network Design

Hardware and software Specification: the design phase is the time to begin acquiring the hardware and software that will be needed for the future system. First, I have created a list of the hardware that is required to support my system. The network model provides a good starting point for recording the hardware needs because each of the components on the diagram correspond to an item on hardware requirement list. Second step is to find out the minimum requirements for each piece of hardware. I conveyed such requirements as the amount of processing capacity, the amount of storage space, and the receiving capacity of SMS. Finally, we considered the factors that affect hardware performance, such as response time with SMS, data volumes and memory requirements for the request query etc. the figure presents the specification for my system:

HARDWARE

Minimum Requirements:

Processors:	6-128 (128-way HP-UX 11i v2)
Microprocessor type:	Intel Itanium 2 (1.6 GHz) or mx2 dual-processor modules
Memory:	1TB
PCI slots:	192 (w/ I/O expander)
Operating systems:	HP-UX 11i v2; Microsoft® Windows® Server 2003, Data center Edition for 64-bit Itanium-based systems; Linux® (Red Hat Enterprise Linux AS 3, SUSE SLES 9); OpenVMS (1H2006)
Dimensions:	48"D

60"W
77.2"H

SOFTWARE

- OS: Windows Server 2003(SP1)
- Oracle9i
- Visual Studio.Net
- SMS Server Control
- J2ME v2.0
- CLDC v1.0

Another piece to include in architecture design is a security plan that addresses how to keep the application and its data secure. Some people will try to gain unauthorized access to the system, some will do no hard; others attempt to access a system for personal gain or to do sabotage the system in some way [2]. Several techniques are available to increase security. The use of password and encryption are central to any type of secure system. I had used this technique to protect the system.

3.3.3 User Interface Design

A user interface is the part of the system with which the users interact in our system. I have to design the user interface component such as registration of parties, constituencies, candidates and interface of voting. In addition I designed some user interface form for the operator of the system and also for the voters.

The first element of the user interface is the layout of the screen form, which is usually rectangular shapes with navigation, and a center area of the form for inputs.

The screenshot shows a web application window titled "Admin Module/Party". The interface features a navigation bar with buttons for "Mobile Number", "Candidate Details", "Party", "Logo", and "Search". The main content area is titled "Party Information" and contains two text input fields: "Enter Party Name :" and "Enter Party Id :", both of which are circled in red. Below these fields are three buttons: "Submit", "Cancel", and "Show Details". At the bottom, there is a section titled "Party details" containing a table with two rows and three columns.

Figure 3.3.3.1: Party Registration

The above in the interface form of party registration through which the system input user will register the parties who will contest in the National Election. I tried to include significant white space, perfect color and be consistent with fonts. Most of all I tried to design to support both novice/first-time users and experienced users. In the red circled text fields user have to give the inputs of party name and

party Id and have to press the submit button to be done with the registration for one party.

The screenshot shows a web application window titled "Admin Module/Party". At the top, there are five tabs: "Mobile Number", "Candidate Details", "Party", "Logo", and "Search". The "Party" tab is active. Below the tabs, there is a "Party Information" section with two input fields: "Enter Party Name :" and "Enter Party Id :". Below these fields are three buttons: "Submit", "Cancel", and "Show Details". The "Show Details" button is circled in red. Below the buttons is a "Party details" section containing a table with the following data:

	PARTY NAME	PARTY NO
▶	BNP	1
	BAL	2
	JIP	3
	INDEPENDENT	100
	CONGRESS	5

Figure 3.3.3.2: Party Registration: Party Details

The above interface form shows the details of parties. By pressing, "show details" button the user will be able to see the detail list of registered parties. I have showed the details just after the input section so that the user can easily get the knowledge of which parties are already registered. It helps the user to the do work efficiently.

The below in the interface form of constituency registration through which the system input user will register the constituencies where the election will take place in the National Election. In the text fields the user have to give the necessary inputs to do the registration procedure of a constituency and then have to press the “Add” button to be done with the registration for one constituency.

The screenshot shows a software window titled "Input Module" with a blue title bar. Inside the window, there are five buttons at the top: "Constituencies", "Polling Center", "Candidate", "Party", and "Logo". Below these is a section titled "Constituencies Information" which contains a form with four input fields: "Constituencies Name:", "Serial Number:", "Select District:", and "Select Division:". The "Select Division:" field is a dropdown menu. A red rectangle highlights these four input fields. Below the form are three buttons: "Add", "Clear", and "Show Details". At the bottom of the window is a table with the following headers: "Serial Number", "Constituency Name", "Districts", and "Division". The table body is currently empty.

Figure 3.3.3.3: Constituency Registration

The screenshot shows a software window titled "Input Module" with a blue title bar. Inside the window, there are five buttons at the top: "Constituencies", "Polling Center", "Candidate", "Party", and "Logo". Below these is a section titled "Constituencies Information" containing four input fields: "Constituencies Name:" (text box), "Serial Number:" (text box), "Select District:" (text box), and "Select Division:" (dropdown menu). At the bottom of this section are three buttons: "Add", "Clear", and "Show Details". Below the form is a table with the following data:

Serial Number	Constituency Name	Districts	Division
5	Dhaka-5	Dhaka	Dhaka
1	Dhaka-1	Dhaka	Dhaka
2	Dhaka-2	Dhaka	Dhaka
3	Dhaka-3	Dhaka	Dhaka
4	Dhaka-4	Dhaka	Dhaka
7	Dhaka-7	Dhaka	Dhaka
6	Dhaka-6	Dhaka	Dhaka

Figure 3.3.3.4: Constituency Registration: Constituency Details

The above interface form shows the details of registered constituencies. By pressing, “show details” button the user will be able to see the detail list of registered constituencies. I have showed the details just after the input section so that the user can easily get the knowledge of which constituencies are already registered. It helps the user to do the work efficiently.

The image shows a web-based form for candidate registration. At the top, there are five buttons: "Mobile Number", "Candidate Details", "Party", "Logo", and "Search". Below these is a section titled "Enter Candidate Details For Constituencies :" with a dropdown menu showing "Dhaka-3". The main form area contains several input fields: "Candidate Name :" with the text "NAIM", "Candidate Identification Number :" with the text "3001", "Sex :" with a dropdown menu showing "M", "Party Name :" with a dropdown menu showing "INDEPENDENT", and "Symbol :" with the text "CLOCK". A red circle is drawn around the "Candidate Identification Number" field. At the bottom of the form, there are three buttons: "Submit", "Cancel", and "Show Details".

Figure 3.3.3.5: Candidate Registration

The above in the interface form of constituency registration through which the system input user will register the candidates who will contest for a party from a constituency in the National Election. In the text fields the user will have to give the necessary inputs to do the registration procedure of a constituency and then have to press the “submit” button to be done with the registration for one

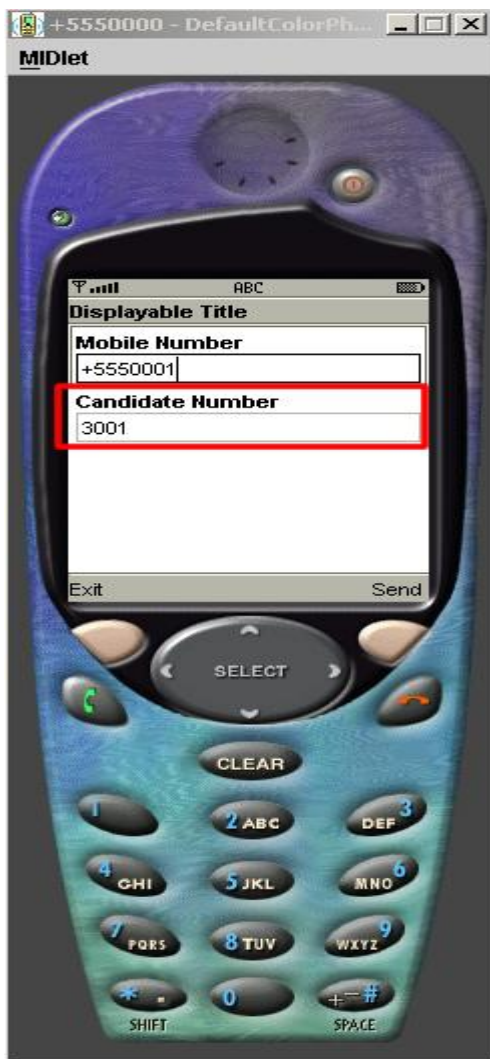
constituency. The red-circled text field shows the candidate ID number, which will be used as the input from the voters as their votes, and it is unique.

CANDIDATE NAME	PARTY NAME	LOGO	SEX	NAME OF CONSTITUENCIES
Farhad Bari	BNP	Paddy	M	Dhaka-1
Shamima Yeasmin	BAL	Boat	F	Dhaka-1
Abdul Bari	JIP	Plough	M	Dhaka-1
Hasanul bari	BAL	BOAT	M	Dhaka-1
Moklasur Rahman	JIP	String	M	Dhaka-1

Figure 3.3.3.6: Candidate Registration: Candidate Searching

The above interface form shows the details of registered candidates. Here the user can get details of a particular candidate or details of all candidates of a particular constituency. I have kept three types of searching options. One is searching by candidate name, second is searching is by candidate ID number and third one is searching by constituencies. By pressing “search” button the user will be able to see the detail list of registered candidates.

The following interface form shows how the voters will cast their votes and how the data will go to the database server securely. As the mobile number of the database server is fixed so we kept the mobile number fixed. So, the voters will not have to give the mobile number as input. They will just have to give the candidate ID as their votes in the text field and the vote will go to the database server as an encrypted data and before storing in the database server it will be decrypted.



In this figure we can see two text fields. First one is for mobile, which is kept fixed so the voters will not enter the mobile number and the second one is the candidate number, which is unique. Voters will only send the unique candidate number as their votes. After pressing the send button it will be encrypted.

Figure 3.3.3.7: Voting Data Encryption

Once the voter press the send button the vote will be encrypted and it will be sent to the database server. As I have mentioned earlier that though I did the encryption-decryption of the data, but have not yet been integrated this with the system. The following figure shows the encrypted data of the voting data. This encrypted data is again decrypted just before storing in to the database server.

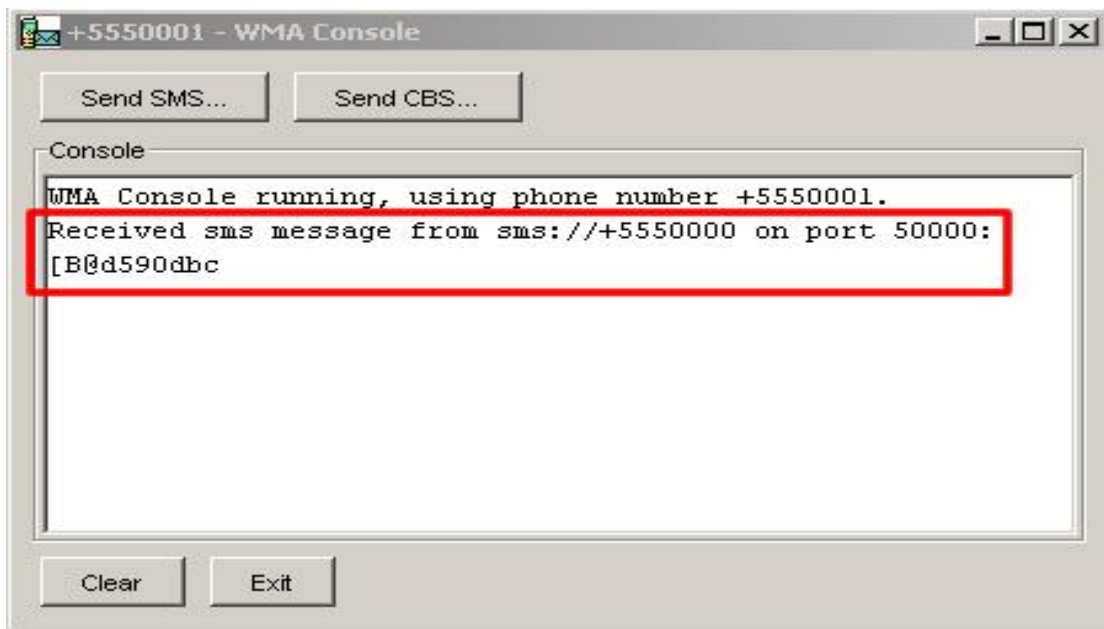


Figure 3.3.3.8: Encrypted Data

We used Bouncy Castle Cryptography Algorithm to do the Encryption-Decryption of the Voting Data. The Bouncy Castle Crypto package is a Java implementation of cryptographic algorithms. The package is organized so that it contains a lightweight API suitable for use in any environment (including the newly released J2ME) with the additional infrastructure to conform the algorithms to the JCE framework. Bouncy Castle uses private keys to do encryption-decryption, which is generated automatically inside the system. So, it is fully secured, as no one will get the access to the key.

3.3.3.1 Input Design

The goal of the input mechanism is to simply and easily capture accurate information for the system [2]. As we have used prototype so we have gathered the information of input earlier and changed that by the course of time with the appropriate requirement. So here we were concern about the validation by using some combination of completeness checks, format checks, range checks, check digits, consistency checks and database checks.

3.3.3.2 Output Design

The goal of the output mechanism is to present information to users so they can accurately understand it with the least effort [4]. I mainly was concern about the details showing and searching that I will show to the user according to their needs. I had some mistakes with prototype and my supervisor correct me with some suggestion.

3.3.4 Data Storage Design

My first step was to convert the E-R model to a relational model, which then be tested to see if it contains any redundancies. A number of criteria were pointed out and implemented for such test. They were defined in terms of functional dependencies and relation keys. Relations that satisfy the criteria are well known as normal relations. I tried to ensure that my data model contains only relations in the highest normal form.

3.3.4.1 Party Registration System

Table Name: PARTY

Purpose: Store Party Name and party ID

Name	Datatype	Size	Scale	Nulls?	Default Value
PARTY_NAME	CHAR	35			
PARTY_NO	NUMBER	5	0		

Table 3.3.4.1: PARTY

Description: I am saving party name and party ID in this table. This table also used for candidate table as there we used the party number.

3.3.4.2 Constituency Registration System

Table Name: CONSTITUENCIES

Purpose: Store Constituency Serial number, name, district name and the division

Columns					
Name	Datatype	Size	Scale	Nulls?	Default Value
SL_NO	NUMBER	10	0		
NAME_OF_CONSTITU...	CHAR	20			
DISTRICT	CHAR	20			
DIVISION	CHAR	20			

Table 3.3.4.2: CONSTITUENCY

Description: This table is used to do the registration of constituency. The constituency name is also used in the relation table of candidate and constituencies.

3.3.4.3 Candidate Registration System

Table Name: CANDIDATE

Purpose: Store Candidate ID, name, party number, logo and sex

Name	Datatype	Size	Scale	Nulls?	Default Val
CANDIDATE_NO	NUMBER	10	0		
CANDIDATE_NAME	CHAR	35			
PARTY_NO	NUMBER	5	0		
LOGO	CHAR	20			
SEX	CHAR	7			

Table 3.3.4.3: CANDIDATE

Description: This table keeps the records of candidates. From this table the candidate number is used in the relation table of the candidate and constituency.

Table Name: CONSTITUENCIES_CANDIDATE

Purpose: Store Candidate ID, name, party number, logo and sex

Columns					
Name	Datatype	Size	Scale	Nulls?	Default Value
NAME_OF_CONSTI...	CHAR	20			
CANDIDATE_NO	NUMBER	10	0		

Table 3.3.4.4: CONSTITUENCIES_CANDIDATE

Description: This is the relation table of candidates and constituencies to get the information that which candidate is under which constituency.

3.4 Implementation

3.4.1 Party Registration System

After all the analysis and design my party registration system functions like:

1. When a user will seek to register a party for the National Election, he/she will have to go to the party registration form by pressing "Party" button.
2. Then the user will have to enter the Party Name and Party ID. If Party Name or Party ID exists then it will give a notification message saying the Party Name or Party ID is already exist. On the other hand if the format of the input is wrong then it will ask for right input.
3. After pressing "Submit" button the data will be stored in to database server and the text fields will be empty.
4. Pressing "Show Details" a query will be run and will show all parties name with their IDs in the Party Details sheet.

3.4.1.1 Pseudo code for Showing Details of Parties

1. *Private Sub show_details_Click()*
2. *Set show_party = New ADODB.Recordset*
3. *show_party.Open "select party_name ,party_no from party", db, adOpenDynamic, adLockOptimistic*

4. *Set Adodc1.Recordset = show_party*
5. *Adodc1.Refresh*
6. *show_party.Close*
7. *End Sub*

3.4.2 Constituency Registration System

1. When a user will seek to register a constituency for the National Election, he/she will have to go to the constituency registration form by pressing “Constituencies” button.
2. Then the user will have to enter the Constituency Name, Serial Number, and District Name of the constituency and have to select the Division Name. If Constituency Name or Serial Number exists then it will give a notification message saying the Constituency Name or Serial Number is already exist. On the other hand if the format of the input is wrong then it will ask for right input.
3. After pressing “Add” button the data will be stored in to database server and the text fields will be empty.
4. Pressing “Show Details” a query will be run and will show all constituencies details in the second grid sheet.

3.4.2.1 Pseudo code for Showing Details of Constituencies

1. *Private Sub cmdShowDetails_Click()*
2. *Set rstTest = New ADODB.Recordset*
3. *rstTest.CursorLocation = adUseClient*

```

4. rstTest.Open "select * from constituencies", db, adOpenStatic,
   adLockOptimistic
5. Me.grdInfo.Rows = rstTest.RecordCount + 1
6. Dim i As Long
7. rstTest.MoveFirst
8. For i = 1 To rstTest.RecordCount
9. Me.grdInfo.TextMatrix(i, gridcols.serial) = rstTest("sl_no")
10. Me.grdInfo.TextMatrix(i, gridcols.constitName) =
    rstTest("NAME_OF_CONSTITUENCIES")
11. Me.grdInfo.TextMatrix(i, gridcols.Districts) = rstTest("district")
12. Me.grdInfo.TextMatrix(i, gridcols.Division) =rstTest("Division")
13. rstTest.MoveNext
14. Next i
15. Dim strMobNo As String
16. strMobNo = "0171173488"
17. db.Execute ("delete from input where mobile_no=" & strMobNo & "")
18. End Sub

```

3.4.3 Candidate Registration System

1. When a user will seek to register a candidate for the National Election, he/she will have to go to the candidate registration form by pressing "Candidate" button.
2. Now the user will have to select the Constituency Name. Then he/she will enter the Candidate Name, unique Candidate ID, Sex, and Party Name for which he/she is contesting and the Symbol. If Candidate ID exists then it will give a notification message saying the Candidate ID already exists. On

the other hand if the format of the input is wrong then it will ask for right input.

3. After pressing “Submit” button the data will be stored in to database server and the text fields will be empty.
4. Pressing “Show Details” another form will open where the use will be able to search a particular candidate details or all candidates’ details for a particular constituency.
5. The user will have to select whether he/she will do the search by Candidate Name or Candidate ID or Constituencies. Then by pressing “Search” it will show the report.

3.4.3.1 Pseudo code for Searching of Candidates

1. *Private Sub Command_search_Click()*
2. *If Text1.Text = "" And Combo1.Text = "" And Text2.Text = "" Then*
3. *MsgBox "Enter Search Items", vbInformation*
4. *Elseif Option3.Value = True Then*
5. *cand_name = Text1.Text*
6. *Set search_with_cons = New ADODB.Recordset*
7. *search_with_cons.Open* *"select*
candidate_name,party_name,logo,sex,name_of_constituencies *from*
Party,Candidate,constituencies_candidate *where*
party.party_no=candidate.party_no *and*
constituencies_candidate.candidate_no=candidate.candidate_no *and*
candidate_name ="" & cand_name & """, db, adOpenDynamic,
adLockOptimistic
8. *Set Adodc1.Recordset = search_with_cons*

```

9. Adodc1.Refresh
10. search_with_cons.Close
11. Elself Option1.Value = True Then
12. cand_no = Text2.Text
13. Set search_with_cons = New ADODB.Recordset
14. search_with_cons.Open                                "select
    candidate_name,party_name,logo,sex,name_of_constituencies    from
    Party,Candidate,constituencies_candidate                    where
    party.party_no=candidate.party_no                            and
    constituencies_candidate.candidate_no=candidate.candidate_no    and
    constituencies_candidate.candidate_no    ="    &    cand_no,    db,
    adOpenDynamic, adLockOptimistic
15. Set Adodc1.Recordset = search_with_cons
16. Adodc1.Refresh
17. search_with_cons.Close
18. Elself Option2.Value = True Then
19. cons_name = Combo1.Text
20. Set search_with_cons = New ADODB.Recordset
21. search_with_cons.Open                                "select
    candidate_name,party_name,logo,sex,name_of_constituencies    from
    party,candidate,constituencies_candidate                    where
    party.party_no=candidate.party_no                            and
    constituencies_candidate.candidate_no=candidate.candidate_no    and
    name_of_constituencies="" & cons_name & "", db, adOpenDynamic,
    adLockOptimistic
22. Set Adodc1.Recordset = search_with_cons
23. Adodc1.Refresh
24. search_with_cons.Close
25. End If
26. End Sub

```

3.4.4 Vote-data Security System

1. When a voter will seek to cast his/her vote then he/she will just have to enter the candidate number. Here the mobile number is kept fixed
2. After pressing the “Send” button the vote-data will be encrypted by the Bouncy Castle Cryptography Algorithm.
3. When it will get any data it will do the encryption using a private key. This private key will be automatically generated inside the system which will be even hidden from the system administrator.
4. After getting the encrypted data the client end will decrypt the vote-data using the same algorithm and finally it will store the vote to the database server.

3.4.4.1 Bouncy Castle Encryption Algorithm

```
1. public class Encryptor {
2. private BufferedBlockCipher cipher;
3. private KeyParameter key;
4. public Encryptor( byte[] key ){
5. cipher = new PaddedBlockCipher(
6. new CBCBlockCipher(
7. new DESEngine() ) );
8. this.key = new KeyParameter( key );
9. }
10. public Encryptor( String key ){
11. this( key.getBytes() );
12. }
```

```

13. private byte[] callCipher( byte[] data )
14. throws CryptoException {
15. int size =
16. cipher.getOutputSize( data.length );
17. byte[] result = new byte[ size ];
18. int olen = cipher.processBytes( data, 0,
19. data.length, result, 0 );
20. olen += cipher.doFinal( result, olen );
21. if( olen < size ){
22. byte[] tmp = new byte[ olen ];
23. System.arraycopy(
24. result, 0, tmp, 0, olen );
25. result = tmp;
26. }
27. return result;
28. }
29. public synchronized byte[] encrypt( byte[] data )
30. throws CryptoException {
31. if( data == null || data.length == 0 ){
32. return new byte[0];
33. }
34. cipher.init( true, key );
35. return callCipher( data );
36. }
37. public byte[] encryptString( String data )
38. throws CryptoException {
39. if( data == null || data.length() == 0 ){
40. return new byte[0];
41. }
42. return encrypt( data.getBytes() );

```

```

43.}
44.public synchronized byte[] decrypt( byte[] data )
45.throws CryptoException {
46.if( data == null || data.length == 0 ){
47.return new byte[0];
48.}
49.cipher.init( false, key );
50.return callCipher( data );
51.}
52.public String decryptString( byte[] data )
53.throws CryptoException {
54.if( data == null || data.length == 0 ){
55.return "";
56.}
57.return new String( decrypt( data ) );
58.}}

```

3.4.4.2 Bouncy Castle Decryption Algorithm

```

1. public synchronized byte[] decrypt( byte[] data )
2. throws CryptoException {
3. if( data == null || data.length == 0 ){
4. return new byte[0];
5. }
6. cipher.init( false, key );
7. return callCipher( data );
8. }
9. public String decryptString( byte[] data )
10.throws CryptoException {
11.if( data == null || data.length == 0 ){

```



```
12. return "";  
13.}  
14. return new String( decrypt( data ) );  
15.}
```

CHAPTER 4

SYSTEM TESTING

4.1 Unit testing and Integration Testing

As I have put four systems: Party input system, Candidate input system, Constituency input system and sending the voting data securely that is security, my modules are inter-related. Party, candidate and constituency input system works based on the output information of each other. If any party input failed then that party will not be able to do the election. According to my modules, if party input and constituency input is not done first then candidate input is not possible. So, I prove that given sample data, if all systems individually work properly then integration testing is successful.

Testing For Party Registration System

Tester: Md. Naimuzzaman

Date: 22.07.2005

Objective

Ensure that the information provided by the administrator is correct and rightly used by the system.

Data Field	Value
1. Party Name, Party ID	BNP, 1
2. Party Name, Party ID	2, BAL
3. Party Name, Party ID	BAL, 2
4. Party Name, Party ID	BAL, 3
5. Party Name, Party ID	JAMAT, 3
6. Party Name, Party ID	ind, 3
7. Party Name, Party ID	IND, 4
8. Party Name, Party ID	IND, 5

Table 4.1: Testing For Party Registration

Expected Result Notes

Test 1, 3, 5, 7 and 8 are valid because they have right format. 2 is invalid due the wrong format, 4 is invalid as party name “BAL” is already inserted with ID no. 2. 6 are invalid as it took the same party ID like 5. So, it is not valid. 6 is also invalid as the system is case sensitive. Here there is an exception between 7, 8. Though both are same party name but they are valid because there are lots of independent candidates. So, only multiple “IND” is valid with unique ID no.

Actual Result Notes

Test 1, 3, 5, 7 and 8 are accepted. Test 2, 4 and 6 were rejected with correct error.

Testing For Constituency Registration System

Tester: Md. Naimuzzaman

Date: 23.07.2005

Objective

Ensure that the information provided by the administrator is correct and rightly used by the system.

Data Field	Value
1. Constituency Name, serial no, District, Division	Dhaka-1,1, Dhaka, Dhaka
2. Constituency Name, serial no, District, Division	Dhaka -1,1, Dhaka, Dhaka
3. Constituency Name, serial no, District, Division	2, Dhaka -2, Dhaka, Dhaka
4. Constituency Name, serial no, District, Division	Gazipur -2,3, Gazipur, Dhaka
5. Constituency Name, serial no, District, Division	Gazipur-3,4,Gazipur,Dhaka

Table 4.2: Testing For Constituency Registration

Expected Result Notes

Test 1, 4 and 5 are valid because they have right format. 3 is invalid due the wrong format. 2 are invalid for duplicate insertion.

Actual Result Notes

Test 1, 4 and 5 are accepted. Test 2 and 3 were rejected with correct error.

Testing For Candidate Registration System

Tester: Md. Naimuzzaman

Date: 24.07.2005

Objective

Ensure that the information provided by the administrator is correct and rightly used by the system.

Data Field	Value
1. Constituency Name, Candidate name, ID, Sex, Party Name, Symbol	Dhaka -1, Naim, 1001, M, BNP, SOP
2. Constituency Name, Candidate name, ID, Sex, Party Name, Symbol	Dhaka -1, Naim, 1002, M, BAL, BOAT
3. Constituency Name, Candidate name, ID, Sex, Party Name, Symbol	Dhaka -1, Naim, 2003, M, JAMAT, KULA
4. Constituency Name, Candidate name, ID, Sex, Party Name, Symbol	Dhaka -2, Naim, 2001, M, BNP, SOP
5. Constituency Name, Candidate name, ID, Sex, Party Name, Symbol	5005, Dhaka -5, Aklima, F, IND, CLOCK
6. Constituency Name, Candidate name, ID, Sex, Party Name, Symbol	Dhaka-5, Aklima, 5005, F, IND, CLOCK
7. Constituency Name, Candidate name, ID, Sex, Party Name, Symbol	_____, Faria, 5006, F, IND, CLOCK

Table 4.3: Testing For Candidate Registration

Expected Result Notes

Test 1, 2, 4 and 6 are valid because they have right format. 3 is not valid due to wrong format of ID. For Dhaka-1 it has to be in 1000 series, for Dhaka-2 it will be 2000 series and so on. 5 is not valid due to misplacement of input. 7 is not valid because no field cannot be kept empty

Actual Result Notes

Test 1, 2, 4 and 6 are accepted. Test 3, 5 and 7 were rejected with correct error.

Testing For Candidate Searching System

Tester: Md. Naimuzzaman

Date: 24.07.2005

Objective

Ensure that the information provided by the administrator is correct and rightly used by the system.

Data Field	Value
1. Candidate name / Candidate ID / Constituency Name	Naim / 1001 / Dhaka-1
2. Candidate name / Candidate ID / Constituency Name	1001/ Naim / Dhaka-1

Table 4.4: Testing For Candidate Search

Expected Result Notes

For searching we have to search by using any of the data field rather than all of three. So, test 1 is valid because it has right format. 2 is not valid due to wrong input. By using first two data field of test 1 I expected to get the information about that candidate if he/she exists. By using last data field I expected to get details of all candidates under that constituency.

Actual Result Notes

Test 1, worked properly by using all three data fields separately. Test 2 was rejected with correct error.

Testing For Encryption-Decryption of Voting Data

Tester: Md. Naimuzzaman

Date: 25.07.2005

Objective

Ensure that the votes given by the voters go to the server end surely

	Data Field	Value	Encrypted	Decrypted
1.	Candidate number	1001	didn't	1001
2.	Candidate number	1001	done	didn't
3.	Candidate number	1001	f35[-709_)]@3	1001
4.	Candidate number	2001	^#832&^(09e	2001
5.	Candidate number	BNP	JHS*(*)ć	BNP

Table 4.5: Testing for Encryption-Decryption of Voting Data

Expected Result Notes

Test 1 and 2 are invalid because in 1 the encryption could not be done and in 2, encryption was successful but decryption did not work. 3 and 4 is valid as the input is correct and the encryption-decryption works properly. 5 is not valid as the input format is not ok. It has to be only candidate number.

Actual Result Notes

Test 3 and 4 worked properly. Test 1, 2 and 5 were rejected with correct error.

4.2 System Testing

We tested our system by our selves. Following is the manual of input/output done by ourselves

4.2.1 Manual of Input/output

Party Input System: It has one input and five either output according to the situation.

Input: BNP, 1

Output: "Input is done successfully"

Output: "X Field is empty"

Output: "Party name is already exist"

Output: "Input format is wrong"

Output: "Party ID is already exist"

Constituency Input System: It has one input and five either output according to the situation.

Input: Gazipur -1, 1, Gazipur , Dhaka

Output: "Input is done successfully"

Output: "X Field is empty"

Output: "Constituency name is already exist"

Output: "Constituency ID is already exist"

Output: "Input format is wrong"

Candidate Input System: It has one input and seven either output according to the situation.

Input: Gazipur -1, Naim, 1001, M, BNP, SOP

Output: "Input is done successfully"

Output: "X Field is empty"

Output: "Candidate ID is already exist"

Output: "Candidate ID format does not match with Constituency Name"

Output: "Input format is wrong"

Output: "You did not select the Constituency Name"

Output: "You did not select the Party Name"

Candidate search System: It has one input and five either output according to the situation.

Input: Naim/ 1001 / Gazipur -1

Output: "X Field is empty"

Output: "Candidate name does not exist"

Output: "Candidate ID does not exist"

Output: if search is done by Constituency then it will show details of all candidates under that constituency

Output: if search is done by candidate name or DI then it will show details of that particular candidate

Encrypted-Decrypted Voting Data: It has one input and four either output according to the situation.

Input: 1001

Output: "Format Error"

Output: "Invalid Input"

Output: "[B@d590dbc" (this is an example. It will change for each time encryption of each data. That means, next time if the input is again 1001 the output will be different)

Output: 1001 (here shows the data after decrypting from encrypted format)

4.2.2 Actual Input Output

Party Input System:

Constituency Input System:

Candidate Input System:

Encryption-Decryption of Voting Data:

Input:

Server Mobile Number

0172123691

15002

Exit Send

Figure 4.2.1: Vote Data Input

Output:

CANDIDATE_NO	MOBILE_NO
15002	171327701
15001	152377860
15002	171327723
15002	152377860
15001	171327723
15001	171327701
15002	152377860

Storing in Database Server after Decryption

Figure 4.2.2: Decrypted Vote Data Stored in database server

4.3 Acceptance Testing

On 30th July, we tested the system at a software development firm in Dhanmondi. There we prearranged a room as the polling center to simulate our complete system. We, all three-group members mutually tested the system over there. The office stuffs participated in the testing session. They were provided three mobile phones to interact with the system and we also gave them proper instruction how to do the proper inputs. Thus we had our system testing and from there we have gathered ideas how organize the sequence of our entire Electronic Election System.

Doing so, we separated office stuffs who voted. We selected our Supervisor Dr. Yousuf Islam and another respective teacher Mr. Zillur Rahman as the candidate and we registered them. We also registered three mobile numbers from which all

votes sent. We assigned two parties, one constituency and other necessary information against two candidates. Then all the votes had done.

4.4 Test Data

As I have discussed earlier, our acceptance testing will be theoretically a beta testing and all the data we will use here will be real life user data.

CONSTITUENCIES

For testing purpose we registered one constituency under which all the voting were done:

SL_NO	NAME_OF_CONSTITUENCY	DISTRICT	DIVISION
15	Dhaka-15	Dhaka	Dhaka

POLLING_CENTER

For testing purpose we registered one polling center under which all the voting was done:

CENTER_NAME	CENTER_NO	NAME_OF_CONSTITUENCIES	VOTER	NUM_BOOTH
SoftEd	15-Dhaka-1	Dhaka-15	50	3

POLLING_BOOTH

For testing purpose we registered one polling center under which all the voting was done:

CENTER_NO	BOOTH_ID	MOBILE_NO
15-Dhaka-1	1	+880171327701
15-Dhaka-1	2	+880171327723
15-Dhaka-1	3	+880172377860

PARTY

For testing purpose we registered two parties as follows:

PARTY_NAME	PARTY_NO
BNP	1
BAL	2

CANDIDATE

We registered two candidates who contested for election during our testing time

CANDIDATE_NO	CANDIDATE_NAME	PARTY_NO	LOGO	SEX
15001	YMI	1	SOP	M
15002	ZRA	2	BOAT	M

CONSTITUENCIES_CANDIDATE

This table shows which candidate is contesting from which constituency

CANDIDATE_NO	NAME_OF_CONSTITUENCIES
15001	Dhaka-15
15002	Dhaka-15

INPUT

During testing we got the following inputs from the registered mobile as votes:

CANDIDATE_NO	MOBILE_NO
15001	+880171327701
15001	+880171327723
15002	+880171327701
15001	+880172377860
15002	+880171327723
15001	+880171327701
15001	+880172377860
15002	+880171327723
15002	+880171327701
15001	+880172377860
15002	+880171327701
15001	+880171327723
15002	+880171327701
15001	+880172377860
15002	+880171327723
15002	+880172377860
15001	+880171327723
15001	+880171327701
15002	+880172377860
15001	+880171327701
15001	+880171327723
15001	+880172377860
15002	+880171327701

4.5 Results:

We have tested our system in a Software Development firm using two registered mobile phones. In the following there are few screen shots of the results that we generated after the voting by the participants:

Show result for constituencies				
Dhaka-15		Go	Who Is Winner???	
Details results in constituencies				
CANDIDATE NO	CANDIDATE NAME	PARTY NAME	NAME OF CONSTITUENCIES	CONS VOTE
15002	ZRA	BAL	Dhaka-15	10
15001	YMI	BNP	Dhaka-15	13

Total Reg. Voter : 20 Vote Casted : 23 Percent : 115.00%

Figure 4.5.1: Result by Constituency



Figure 4.5.2: Winning Candidate

CHAPTER 5
USER MANUAL

5.1 User Instructions for Administrators

5.1.1 Party Registration System

This module keeps information of parties. So, administrators have to give inputs of information about parties. If an administrator or authority wants to know about any particular party, he/she has to just search it as like:

BNP
Party name

He/she just has to search by using any of the above field. It will show the list of parties according to the input.

5.1.2 Constituency Registration System

This module keeps information of constituencies. So, administrators have to give inputs of information about constituencies. If an administrator or authority wants to know about any particular constituency, he/she has to just search it as like:

Dhaka	Gazipur	Dhaka-1
Division name	District name	Constituency name

He/she just has to search by using any of the above field. It will show the list of constituencies according to the input.

5.1.3 Candidate Registration System

This module keeps information of candidates. So, administrators have to give inputs of information about candidates. If an administrator or authority wants to know about any particular candidate, he/she has to just search it as like:

Naim	1001	Dhaka-1
Candidate name	Candidate number	Constituency name

He/she just has to search by using any of the above field. It will show the list of candidates according to the input.

5.2 User Instruction for Voter

This module just takes the votes securely from the voter through the mobile device. If a voter wants to cast his/her vote then he/she just has to send a SMS writing the candidate number only. It is as like:

2001
Candidate name

He/she just has to insert the candidate number and data will go to server end in encrypted format. After storing the vote in data base in decrypted mode it will send a confirmation message to the voter.

CHAPTER 6

CONCLUSION

The current Election System is done manually. In this system we found out some major problems. The system is fully paper based like printing ballot papers and distributing them, high risk of Ballot box hijacking in the remote areas, Ballot paper is manually counted which requires huge manpower. Counting errors occur and it needs recounting, compilation of result requires many stages, which is very time consuming. These problems as a whole put a big question mark on the reliability and transparency of the current election system. So we have come up with a hybrid solution, which automates and secures some of the sensitive modules of the system. This hybrid system has a simple voting interface for the voters. The counting and result generation is automated and requires short span of time. Since portions of the system is automated involvement of human workforce decreases. In addition, the system is more secured, more dependable and more efficient as most of the sensitive functions are implicit to the system and done automatically and securely. Our system may be initially installed in areas where the risk of hijacking of ballot box is high. In a word the Hybrid Solution for National Election System improves the overall efficiency of the current election system by providing an alternative for faster, feasible and secured processing of election results.

REFERENCES

- [1] Jeffrey A. Hoffer, Joey F. George, Modern System Analysis & Design. Pearson Education Asia.
- [2] Alan Debbis, Indiana University. Barbara Haley Wixom, University of Virginia, David Tegarden, Virginia Tech, System Analysis and Design
- [4] Mawdudur Rahman, Nishikant Sonwalkat, "Multidimensional Assesment of online learning A pilot study".
- [5] <http://www.bd-ec.org/>
- [6] <http://avirubin.com/vote/>
- [7] <http://www.bangladeshgov.org/ecs/>
- [8] <http://www.telsis.com/0281.htm>
- [9] <http://www.egov4dev.org/mgovapplic.htm>
- [10] <http://www.textually.org>
- [11] <http://www.itl.nist.gov/fipspubs/fip46-2.htm>
- [12] http://en.wikipedia.org/wiki/Triple_DES
- [13] <http://www.users.zetnet.co.uk/hopwood/crypto/scan/cs.html#DESede>
- [14] http://www.hotscripts.com/Java/Tips_and_Tutorials/Security/index.html
- [15] <http://forum.java.sun.com/thread.jspa?threadID=633881&tstart=105>
- [16] <http://www.finetuning.com/h/bouncycastle.html>
- [17] <http://www.javastaff.com/article.php?story=20050117121358746>
- [18] <http://www.blackboxvoting.org/>
- [19] http://franklinmint.fm/2004/09/27/mobile_atom.html
- [20] <http://www.pcworld.com/news/article/0,aid,116709,00.asp>
- [21] <http://www.washingtonpost.com/wp-dyn/articles/A59554-2004Oct24.html>
- [22] <http://www.winsms.com/>
- [23] <http://www.activexperts.com/activsms/>
- [24] http://www.freedownloadcenter.com/Programming/ActiveX/SMS_an_Pager_Toolkit.html

- [25] <http://www.elections.act.gov.au/EVACS.html>
- [26] <http://evm2003.sourceforge.net>
- [27] <http://www.ss.ca.gov/executive/ivote/>
- [28] <http://www.vote.caltech.edu/Reports/>
- [29] <http://www.sos.state.oh.us/sos/hava/files/compuware.pdf>
- [30] <http://users.actrix.co.nz/>
- [31] <http://www.verifiedvoting.org/drefaq.asp>
- [32] <http://fecweb1.fec.gov/>
- [33] <http://www.cs.uiowa.edu/jones/voting/dieboldftp.html>
- [34] <http://news.findlaw.com/cnn/docs/voting/nsfe-voterprt.pdf>
- [35] http://www.raba.com/press/TA_Report_AccuVote.pdf
- [36] <http://avirubin.com/e-voting.security.html>
- [37] <http://www.banglalinkgsm.com/php/mobilemela/gsm.pdf>
- [38] http://www.banglalinkgsm.com/php/mobilemela/SS7_pocket1.pdf
- [39] http://www.banglalinkgsm.com/php/mobilemela/MELA_SESSION_website.pdf

APENDICES

Voting Message Log

The following table contains the voting messages, which are sent by the participants when we did the test in the software development firm.

MESSAGES	MOBILE NUMBER
15001	+880171327701
15001	+880171327723
15002	+880171327701
15001	+880172377860
15002	+880171327723
15001	+880171327701
15001	+880172377860
15002	+880171327723
15002	+880171327701
15001	+880172377860
15002	+880171327701
15001	+880171327723
15002	+880171327701
15001	+880172377860
15002	+880171327723
15002	+880172377860
15001	+880171327723
15001	+880171327701
15002	+880172377860
15001	+880171327701
15001	+880171327723
15001	+880172377860
15002	+880171327701

The following table contains the voting messages, which are sent by the participants when we did the test by ourselves.

MESSAGE	MOBILE NUMBER
1000	+880171176488
1001	+880189111757
1002	+880171174835
1003	+880171176488
1004	+880171174835
1005	+880189111757
1006	+880171174835
1007	+880171176488
1008	+880189111757
1009	+880171174835
1010	+880171176488
1011	+880171174835
1004	+880189111757
1003	+880171174835
1003	+880189111757
1003	+880171176488
1002	+880170000001
1002	+880171174835
1006	+880171176488
1010	+880171174835
1001	+880189111757
1002	+880171174835
1003	+880171176488
1001	+880189111757
1004	+880171176488

1004	+880171174835
1005	+880171174835
1006	+880171176488
1007	+880171174835
1007	+880189111757
1005	+880171176488
1009	+880171174835
1011	+880189111757
1006	+880171176488
1004	+880189111757
1005	+880171174835
1007	+880189111757
1007	+880171174835
1008	+880171176488
1009	+880189111757
1010	+880171174835
1010	+880171176488
1011	+880171174835
1001	+880189111757
1002	+880171176488
1003	+880171174835
1004	+880189111757
1005	+880171176488
1002	+880171174835
1002	+880171176488
1006	+880171174835
1010	+880189111757
1001	+880171174835
1002	+880189111757

1003	+880171176488
1001	+880171174835
1004	+880189111757
1004	+880171176488
1005	+880171174835
1006	+880189111757
1007	+880171176488
1007	+880189111757
1004	+880171174835
1005	+880189111757
1006	+880171174835
1007	+880171176488
1008	+880189111757
1009	+880171174835
1010	+880171176488
1011	+880189111757
1004	+880171174835
1003	+880189111757
1003	+880171174835
1003	+880171176488
1002	+880189111757
1002	+880171176488
1006	+880171174835
1010	+880189111757
1001	+880171174835
1002	+880171176488
1003	+880189111757
1001	+880171176488
1004	+880171174835

1004	+880189111757
1005	+880171174835
1006	+880171176488
1004	+880189111757
1005	+880171176488
1002	+880189111757
1002	+880171174835
1006	+880171176488
1010	+880171174835
1001	+880189111757
1002	+880171176488
1003	+880171174835
1001	+880189111757
1004	+880171174835
1004	+880189111757
1005	+880171174835
1006	+880189111757
1007	+880171176488
1007	+880171174835
1004	+880189111757
1005	+880171176488
1006	+880171174835
1007	+880189111757
1008	+880171176488
1009	+880171174835
1010	+880189111757
1011	+880171176488
1004	+880171174835
1003	+880189111757

1003	+880171176488
1000	+880171174835
1001	+880189111757
1002	+880171174835
1003	+880189111757
1004	+880171176488
1005	+880171174835
1006	+880189111757
1007	+880171176488
1008	+880171174835
1009	+880189111757
1010	+880171174835
1011	+880189111757
1004	+880171174835
1003	+880171176488
1003	+880189111757
1003	+880171176488
1002	+880171174835
1002	+880189111757
1006	+880171174835
1010	+880171176488
1001	+880189111757
1002	+880171176488
1003	+880171174835
1001	+880189111757
1004	+880171174835
1004	+880171176488
1005	+880189111757
1006	+880171176488

1007	+880189111757
1007	+880171174835
1005	+880171176488
1009	+880171174835
1011	+880189111757
1006	+880171176488
1004	+880171174835
1005	+880171176488
1007	+880171174835
1007	+880189111757
1008	+880171174835
1009	+880189111757
1010	+880171176488
1010	+880171174835
1011	+880189111757
1001	+880171176488
1002	+880171174835
1003	+880189111757
1004	+880171176488
1005	+880189111757
1002	+880171174835
1002	+880189111757
1006	+880171174835
1010	+880171176488
1001	+880189111757
1002	+880171174835
1003	+880171176488
1001	+880171174835
1004	+880189111757

1004	+880171176488
1005	+880171174835
1006	+880189111757
1007	+880171176488
1007	+880171174835
1004	+880189111757
1005	+880171174835
1006	+880189111757
1007	+880171174835
1008	+880171176488
1009	+880189111757
1010	+880171176488
1011	+880171174835
1004	+880189111757
1003	+880171174835
1003	+880171176488
1003	+880189111757
1002	+880171176488
1002	+880171174835
1006	+880189111757
1010	+880171174835
1001	+880171176488
1002	+880189111757
1003	+880171176488
1001	+880189111757
1004	+880171174835
1004	+880171176488
1005	+880171174835
1006	+880189111757

1004	+880171176488
1005	+880171174835
1002	+880171176488
1002	+880171174835
1006	+880189111757
1010	+880171174835
1001	+880189111757
1002	+880171176488
1003	+880171174835
1001	+880171176488
1004	+880171174835
1004	+880189111757
1005	+880171176488
1006	+880171174835
1007	+880171176488
1007	+880171174835
1004	+880189111757
1005	+880171174835
1006	+880189111757
1007	+880171176488
1008	+880171174835
1009	+880189111757
1010	+880171176488
1011	+880171174835
1004	+880189111757
1003	+880171176488
1003	+880189111757
1000	+880171174835
1001	+880171176488

1002	+880171174835
1003	+880171176488