Project Report on

E-Voting Using Secret Sharing Scheme

In the partial fulfillment of
6th semester of
MCA

By
MANISH KUMAR
(Roll no- 095580022)

DEPARTMENT OF COMPUTER APPLICATIONS
This is to certify that the project report entitled “E-Voting Using Secret Sharing Scheme” is a bonafide record of the work done by MANISH KUMAR (Reg_no.95580022) as the M.C.A. 6TH semester Major project.

APRIL 2011

_________________________  ____________________________
Internal Examiner                     Head of the Department

Submitted on: _____________________
CONTENTS

- ACKNOWLEDGEMENT
- SYNOPSIS

1. INTRODUCTION
   1.1. ORGANIZATION PROFILE
   1.2. PROJECT ORGANISATION
   1.3. PROJECT PROFILE & ALGORITHM
   1.4. SYSTEM ENVIRONMENT

2. SOFTWARE QUALITY ASSURANCE PLAN
   2.1. PURPOSE
   2.2. SCOPE
   2.3. DOCUMENT OVERVIEW
   2.4. TASKS
   2.5. IMPLEMENTATION
   2.6. DOCUMENTATION
   2.7. AUDIT
   2.8. SOFTWARE DEVELOPMENT PROCESS
   2.9. DOCUMENT REVIEW
   2.10. TESTING
3. SYSTEM ANALYSIS

3.1 SYSTEM STUDY

3.2 FEASIBILITY STUDY

4. SOFTWARE REQUIREMENTS SPECIFICATION

4.1 INTRODUCTION

4.2 PURPOSE

4.3 SCOPE

4.4 DEFINITION, ACRONYM AND ABBREVIATION

4.5 THE OVERALL DESCRIPTION

4.5.1 PRODUCT FEATURE

4.5.2 USER CHARACTERISTIC

4.6 SYSTEM REQUIREMENT SPECIFICATION

4.6.1 USER INTERFACE REQUIREMENT

4.6.2 DATABASE REQUIREMENT

4.6.3 FUNCTIONAL REQUIREMENTS

4.6.4 NON-FUNCTIONAL REQUIREMENTS

4.6.5 SYSTEM REQUIREMENT

4.6.6 TOOLS TECHNIQUE AND MECHANISM

5. SYSTEM DESIGN

5.1 INPUT DESIGN

5.2 OUTPUT DESIGN

5.3 PROCESS DESIGN

5.4 PROBLEM PARTITION

5.5 ARCHITECTURAL DESIGN
5.6 USER CASE DIAGRAM
5.7 ER-DIAGRAMS

6. DATA DESIGN

6.1.1. DATA FLOW DIAGRAMS
6.1.2. DATABASE DESIGN

7. SYSTEM TESTING

7.1. LEVELS OF TESTING AND TEST CASES
7.2. VALIDATION CHECKS

8. SYSTEM IMPLEMENTATION

9. SYSTEM MAINTENANCE

10. CONCLUSION

• APPENDIX

BIBLIOGRAPHY
Acknowledgement

This project would not have taken shape, but for the guidance provided by Dr. A. Sreekumar sir, senior faculty member of DCA CUSAT has helped me so much. Dr. A. Sreekumar had given me great support to make grip over algorithm and fundamental of C which provide the great concept and tool to me to develop this project. I profusely thank them for the support.

I express my profound gratitude to Dr. K. V. Pramod [HOD, DCA], Dr B.Kanan, S. Malathi and all faculty and staff members of the Department of Computer Applications for their endless help and support.

The guidance and support received from all the members who contributed and who are contributing to this project, was vital for the success of the project. I am grateful for their constant support and help.

Above all, I wish to express my heartfelt gratitude to my family & God, who has always been the singular source of inspiration in all my ventures I have undertaken.

Manish Kumar
Synopsis

We live in a democracy and voting is one of our fundamental duties as responsible citizens of the country, but no-where around the country a 100% people come to vote during the elections in their territory. There have been many reasons for that some of them are:

- In the rural areas the influential people keep their men at the polling booths to threaten the common man to vote for them.
- There are many portions of the country like the North East where there is locally sponsored terrorism, at such places the security conditions are also not very bright, so naturally people feel afraid to come out of their houses and go to vote.
- Net savvy new generation want hassle free voting system. Also the people in metros want a system through which they can vote for their territory without traveling.

Keeping in mind these situations and to improve the state of democracy in the country Online Polling System can be thought as a solution, in conjunction with the ongoing current manual voting system.

Our focus is to build a secure, flexible, easy to maintain environment for creating and maintaining the useful website for user who can vote through internet, irrespective of their current position. In the mean of this goal services for Administrator, polling officer and Public along with Candidates will be improved and the new environment will be created. When new public will register by filling his detail in a form for to caste his vote its record will be saved in databases and administrator can verify and updates latest change if there will be, One & most important objective is to make the system platform independent.

Public activities
E-Voting Using Secret Sharing Scheme [E.C.I.]

- Register yourself.
- Send feedback.
- Caste the vote.
- Change the password.
- View the candidate detail.
- See the result.

**Candidate activities**
- Register yourself.
- Change the password.
- Caste the vote.
- View the other candidate detail.
- See the result.

**Pooling Officer Activities**
- Verify User (after manually).
- Change Password.
- Can update any other detail of Public.

**Administrator activities**
- Approve the candidates.
- Change the password.
- Publish the Result.
- Add the new party.

These activities were all being performed manually prior to the implementation of this system. A need for the automation of all these activities was felt. To this effect the front end was deemed to be an internet browser and the data store backend was MySQL.
The Java programming language with jsp has been selected to be the go between the data store and the application. The Java programs will be accessed by the browser using the JSP technology.

1. Introduction

1.1 ORGANISATIONAL PROFILE

Department of Computer Applications::CUSAT

The Department of Computer Applications offers Master's programme in Computer Applications and research programmes leading to Ph.D., sanctioned to the University jointly by U.G.C, and Department of Electronics, Government of India. Guest lectures, seminars by experts in IT, workshops and symposia are organized in the department.

Computer Applications is one of the thrust areas in science and technology. In appreciation of its growing importance in business and visualizing the career prospects, the University established the Department of Computer Applications to facilitate research and human resource development in the subject. The M.C.A. programme was started (1994) with a model curriculum prepared jointly by ISTE and the Department of Electronics with minor modifications. The Syllabus is updated periodically, based on the current trends and requirements of the industry. The Research activities of the Department include the subject areas Fuzzy sets and Logic Applications in Artificial Intelligence, Simulation, Cryptography & Coding Theory, Algorithm, Pattern recognition, Internet-Marketing, E-commerce and Internet Technology, Networking and Mobile Communication and Software Engineering. Apart from this, the Department has taken up a challenging research project funded by AICTE, Computer Assisted Classical Music. The
Department of Computer Applications is also doing consultancy work for public and private sector undertakings. The Department has an excellent library with more than 3000 books and various national and international journals. The Department has a well-equipped laboratory, which is being constantly updated with the latest computers.

1.2 Project Organization

1.2.1 Process Model

1.2.2 Organizational Structure
2.2.3 Project Responsibilities

The table below identifies the major activities that must be carried out to ensure a successful project. The person(s) responsible for each activity is identified in the table as well.

<table>
<thead>
<tr>
<th>Activity</th>
<th>Person(s) responsible</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overall Project Coordination</td>
<td>Mithilesh and Manish</td>
</tr>
<tr>
<td>Requirements Development</td>
<td>Mithilesh</td>
</tr>
<tr>
<td>Software Design and</td>
<td>Manish and Mithilesh</td>
</tr>
</tbody>
</table>
1.3 PROJECT PROFILE & ALGORITHM

Our intention is to implement a secret sharing scheme in our website of election commission of India so that we can implement security in e-voting to ensure a fool proof secure voting system using following algorithm.

Shamir’s Secret Sharing

**Shamir’s Secret Sharing** is an algorithm in cryptography. It is a form of secret sharing, where a secret is divided into parts, giving each participant its own unique part, where some of the parts or all of them are needed in order to reconstruct the secret.

Counting on all participants to combine together the secret might be impractical, and therefore we sometimes use the *threshold scheme* where any $k$ of the parts are sufficient to reconstruct the original secret.

Mathematical definition

Formally, our goal is to divide some data $D$ (e.g., the safe combination) into $n$ pieces $D_1, \ldots, D_n$ in such a way that:
1. Knowledge of any $k$ or more $D_i$ pieces makes $D$ easily computable.
2. Knowledge of any $k - 1$ or fewer $D_i$ pieces leaves $D$ completely undetermined (in the sense that all its possible values are equally likely).

This scheme is called $(k, n)$ threshold scheme. If $k \equiv n$ then all participants are required to reconstruct the secret.

Shamir’s secret-sharing scheme

One can draw an infinite number of polynomials of degree 2 through 2 points. 3 points are required to define a unique polynomial of degree 2. This image is for illustration purposes only — Shamir’s scheme uses polynomials over a finite field, not representable on a 2-dimensional plane.

The essential idea of Adi Shamir’s threshold scheme is that 2 points are sufficient to define a line, 3 points are sufficient to define a parabola, 4 points to define a cubic curve and so forth. That is, it takes $k$ points to define a polynomial of degree $k - 1$.

Suppose we want to use $(k, n)$ threshold scheme to share our secret $S$, without loss of generality assumed to be an element in a finite field $F$.

Choose at random $k - 1$ coefficients $a_1, \cdots, a_{k-1}$ in $F$, and let $a_0 = S$. Build the polynomial

$$f(x) = a_0 + a_1 x + a_2 x^2 + a_3 x^3 + \cdots + a_{k-1} x^{k-1}.$$
Let us construct any \( n \) points out of it, for instance set \( i = 1, \ldots, n \) to retrieve \((\hat{z}, f(\hat{z}))\).

Every participant is given a point (a pair of input to the polynomial and output). Given any subset of \( k \) of these pairs, we can find the coefficients of the polynomial using interpolation and the secret is the constant term \( u_0 \).

**Example**

The following example illustrates the basic idea. Note, however, that calculations in the example are done using integer arithmetic rather than using finite field arithmetic.

**Preparation**

Suppose that our secret is \( 1234 \) \((S = 1234)\).

We wish to divide the secret into 6 parts \((n = 6)\), where any subset of 3 parts \((k = 3)\) is sufficient to reconstruct the secret.

At random we obtain 2 numbers: 166, 94.

\[
(a_1 = 166; a_2 = 94)
\]

Our polynomial to produce secret shares (points) is therefore:

\[
f(x) = 1234 + 166x + 94x^2
\]

We construct 6 points from the polynomial:

\[
(1, 1494); (2, 1942); (3, 2578); (4, 3402); (5, 4414); (6, 5614)
\]

We give each participant a different single point (both \(x\) and \(f(x)\)).

**Reconstruction**

In order to reconstruct the secret any 3 points will be enough.

Let us consider \((x_0, y_0) = (2, 1942); (x_1, y_1) = (4, 3402); (x_2, y_2) = (5, 4414)\).

We will compute Lagrange basis polynomials:

\[
\ell_0 = \frac{x - x_1}{x_0 - x_1} \cdot \frac{x - x_2}{x_0 - x_2} = \frac{x - 4}{2 - 4} \cdot \frac{x - 5}{2 - 5} = \frac{1}{6}x^2 - \frac{1}{2}x + \frac{3}{2}
\]

\[
\ell_1 = \frac{x - x_0}{x_1 - x_0} \cdot \frac{x - x_2}{x_1 - x_2} = \frac{x - 2}{4 - 2} \cdot \frac{x - 5}{4 - 5} = -\frac{1}{2}x^2 + 3\frac{1}{2}x - 5
\]
Therefore

\[ f(x) = \sum_{j=0}^{2} y_j \cdot \ell_j(x) \]

\[ = 1942 \cdot \left( \frac{1}{6} x^2 - \frac{1}{2} x + 3 \frac{1}{3} \right) + 3402 \cdot \left( -\frac{1}{2} x^2 + \frac{3}{2} x - 5 \right) + 4414 \cdot \left( \frac{1}{3} x^2 - 2x + 2 \frac{2}{3} \right) \]

\[ = 1234 + 166x + 94x^2 \]

Recall that the secret is the free coefficient, which means that \( S = 1234 \), and we are done.

Properties

Some of the useful properties of Shamir’s \((k, n)\) threshold scheme are:

1. **Secure**: Information theoretic security.
2. **Minimal**: The size of each piece does not exceed the size of the original data.
3. **Extensible**: When \( k \) is kept fixed, \( D_i \) pieces can be dynamically added or deleted without affecting the other pieces.
4. **Dynamic**: Security can be easily enhanced without changing the secret, but by changing the polynomial occasionally (keeping the same free term) and constructing new shares to the participants.
5. **Flexible**: In organizations where hierarchy is important, we can supply each participant different number of pieces according to his importance inside the organization. For instance, the president can unlock the safe alone, whereas 3 secretaries are required together to unlock it.
1.4 SYSTEM ENVIRONMENT

Hardware Requirements

- Processor: Pentium III or higher.
- RAM: 512 Mb or more.
- Database: MySQL.
- Application: JSP.

Software Requirements

- Web Server: Apache Tomcat 5.5.
- MySQL 5.5
- Operating System: Windows or Linux
- Net beans IDE building tool

THEORITICAL FRAMEWORK

About Java

HISTORY OF JAVA

Java is a programming language originally developed by James Gosling at Sun Microsystems and released in 1995 as a core component of Sun Microsystems' Java platform. The language derives much of its syntax from C and C++ but has a simpler object model and fewer low-level facilities. Java applications are typically compiled to bytecode (class file) that can run on any Java virtual machine (JVM) regardless of computer architecture.

The original and reference implementation Java compilers, virtual machines, and class libraries were developed by Sun from 1995. As of May 2007, in compliance with the specifications of the Java Community Process, Sun made available most of their
Overview of Java

Java is loosely based on C++ syntax, and is meant to be Object-Oriented Structure of Java is midway between an interpreted and a compiled language. The Java compiler into Byte Codes, which are secure and portable across different platforms, compiles Java programs. These byte codes are essentially instructions encapsulated in single type, to what is known as a Java virtual machine (JVM), which resides in standard browser.

*JVM verifies these byte codes when downloaded by the browser for integrity. JVM available for almost all OS. JVM converts these byte codes into machine specific instructions at runtime.*

FEATURES OF JAVA

- Java is object-oriented language and supports encapsulation, inheritance, polymorphism and dynamic binding, but does not support multiple inheritances. Everything in Java is an object except some primitive data types.
- Java is portable architecture neutral that is Java programs once compiled can be executed on any machine that is enabled.
- Java is distributed in its approach and used for Internet programming.
- Java is robust, secured, high performing and dynamic in nature.
- Java supports multithreading. Therefore different parts of the program can be executed at the same time.

About JSP

Overview of JSP
The JSP technology will be used to interface HTML with Java. The JSP technology provides a seamless connection with Java and presents an easy to use, Java-like programming constructs that can be scripted within HTML files. Java Server Pages is a technology for developing web pages that include dynamic content. A JSP page contains standard markup language elements, such as HTML tags, just like a regular web page. A JSP page also contains special JSP elements that allow the server to insert dynamic content in the web page.

**ADVANTAGES OF JSP**

- JSP supports both scripting and element-based dynamic content.
- Allows developing custom tag libraries.
- JSP pages are precompiled for efficient server processing.
- JSP pages can be used in combination with servlets that handle the business logic.
- High Security.
- Can run on any J2EE compatible web Server.
- It can run on any OS that have J2EE compatible web server.
- JSP separates the dynamic and static parts.
- High Quality tool supports.
- JSP supports N tier Application.
- Write Once, Run Everywhere.
- JSP is vendor Neutral.

**Overview of Java Script**

*Java script is a general purpose, prototype based, object oriented scripting language developed jointly by sun and Netscape and is meant for the WWW. Java script*
borrows most of its syntax from java but also inherits from awk and perl, with some indirect influence from self in its object prototype system.

Java Script is almost as easy to learn as HTML and it can be included directly in HTML documents. Java Script was developed independently of java. Java script is a high level scripting language that does not depend on or expose particular machine representations or operating system services.

FEATURES:

- Java script is embedded into HTML documents and is executed with in them.
- Java script is browser dependent.
- JavaScript is an interpreted language that can be interpreted by the browser at run time.
- Java script is loosely typed language
- Java script is an object-based language.
- Java script is an Event-Driven language and supports event handlers to specify the functionality of a button.

The Struts framework provides the flexibility to develop the much less coupled applications. It generalizes and strictly implements MVC-model View Controller Architecture. That is the basic need of our architecture.

About Apache Tomcat

Overview of Apache Tomcat

Apache Tomcat is a servlet container developed by the Apache Software Foundation (ASF). Tomcat implements the Java Servlet and the JavaServer Pages (JSP) specifications from Sun Microsystems, and provides a "pure Java" HTTP web server environment for Java code to run.
Tomcat should not be confused with the Apache web server, which is a C implementation of an HTTP web server; these two web servers are not bundled together. Apache Tomcat includes tools for configuration and management, but can also be configured by editing XML configuration files.

**Components**

Tomcat version 4.x was released with Jasper (a redesigned JSP engine), Catalina (a redesigned servlet container) and Coyote (an HTTP connector).

**Catalina**

Catalina is Tomcat's servlet container. Catalina implements Sun Microsystems' specifications for servlet and JavaServer Pages (JSP). The architect for Catalina was Craig McClanahan.

---

### 2. SOFTWARE QUALITY ASSURANCE PLAN

#### 2.1 PURPOSE

The purpose of this plan is to define the “Customer Relationship Management” Software Quality Assurance (SQA) organization, SQA tasks and responsibilities; provide reference documents and guidelines to perform the SQA activities; provide the standards, practices and conventions used in carrying out SQA activities; and provide the tools, techniques, and methodologies to support SQA activities, and SQA reporting.

#### 2.2 SCOPE

The scope of this document is to outline all procedures, techniques and tools to be used for Quality Assurance of this project. This plan:

- Identifies the SQA responsibilities of the project developer and the SQA consultant
E-Voting Using Secret Sharing Scheme [E.C.I.]

- Lists the activities, processes, and work products that the SQA consultant will review and audit
- Identifies the SQA work products

2.3 DOCUMENT OVERVIEW:

The rest of the document is organized as follows:

Management: A description of each major element of the organization and a description of the SQA tasks and their relationships

Documentation: Identification of the documents related to development, verification, validation, use and maintenance of the software.

SQAP Requirements: This section defines the SQA review, reporting, and auditing procedures used to ensure that software deliverables are developed in accordance with this plan and the project’s requirements.

2.3.1 Management

This section describes the management organizational structure, its roles and responsibilities, and the software quality tasks to be performed.

2.3.2 Organization

Efforts for this project are supported by numerous entities, organizations and personnel. This tool is developed as part of fulfilment of requirements for Masters in Computer Applications degree. It will be the sole responsibility of the developer to review the product’s usability, efficiency, reliability, and accuracy. The client will however conduct inspections, reviews, and walk-through on a regular basis. Client’s specifications and suggestions will be used in places where quality decisions need to out-weigh development schedule decisions.

2.4 TASKS

- Develop requirement specification and cost estimation for the project.
- Develop the design plan and test plan for testing the tool.
- Implement and test the application and deliver the application along with the necessary documentation.
• Give a formal presentation to the client on completion of the analysis, design and testing phases. The client reviews the work and provides feedback/suggestions.

• Planning, coordinating, testing and assessing all aspects of quality issues.

The responsibilities of the client are to:

• Review the work performed.

• Provide feedback and advice.

2.5 SQA IMPLEMENTATION

Quality assurance will be implemented through all the software life cycles of the tool’s development process, until the release of the software product. The following are the quality assurance tasks for each phase of the software development:

Requirements phase: When the SRS is being developed, it has to be ensured that it elucidates the proposed functionality of the product and to keep refining the SRS until the requirements are clearly stated and understood.

Specification and Design phase: Due to the great importance for accuracy and completeness in these documents, weekly reviews shall be conducted between the developer and the client to identify any defects and rectify them.

Implementation phase: The developer shall do code reviews when the construction phase of the Tool begins.

Software testing phase: The developer shall test each case. The final product shall be verified with the functionality of the software as specified in the Software Requirements Specification (SRS) for the Tool.

2.6 DOCUMENTATION

In addition to this document, the essential documentation will include:

The Software Requirements Specification (SRS), which

• Prescribes each of the essential requirements of the software

• Objectively verifies achievement of each requirement by a prescribed method.

• Facilitates traceability of requirements specification to product delivery.
E-Voting Using Secret Sharing Scheme [E.C.I.]

- Gives estimates of the cost/effort for developing the product including a project plan.

The Software Design Document (SDD)

- Depicts how the software will be structured
- Describes the components and sub-components of the software design, including various packages and frameworks, if any.
- Gives an object model the essential classes that would make up the product.
- Gives a sample interaction diagram, showing the key interactions in the application.

Software Test Plan: Describes the test cases that will be employed to test the product.

2.7 DOCUMENT AUDIT

Quality Assurance for this project will include at least one review of all current work products in each stage of development (Requirement, Design, and Implementation). The reviews will assure that the established project processes and procedures are being followed effectively, and exposures and risks to the current project plan are identified and addressed. The review process includes:

- A formal presentation at the end of each development phase (Requirement, Design and Implementation).
- A managerial review by the client periodically to ensure the work generated is in compliance with project requirements.
- Reviews by the client after each presentation.

2.8 SOFTWARE DEVELOPMENT PROCESS

The software development process involves three stages: 1) Requirements phase, 2) Design phase 3) Implementation and testing phase. During each phase, the client will review the deliverable documents. The developer would incorporate modifications suggested by the committee. This would ensure quality of the software product.

2.9 PROJECT REVIEWS

The client will perform a review at the 3 stages of the project as described in the section above. This review will determine whether the requirements have been met for the deliverable, check that the product meets the requirements, ensure that the SQA plan
has been adhered to, verify the performance of the software and ensure that acceptance testing is carried out. A design checklist will be used and the developer will check to see whether the design meets the checklist criteria.

2.10 TESTING AND QUALITY CHECK

Testing will be carried out in accordance with the Software Testing Plan (STP). Testing documentation will be sufficient to demonstrate that testing objectives and software requirements have been met. Test results will be documented and discussed in the final phase of the project.

3. SYSTEM ANALYSIS

SYSTEM ANALYSIS

System analysis is the process of gathering and interpreting facts, diagnosing problems and using the facts to improve the system. System specifies what system should do. A system is a set of components that interact to accomplish some purpose.

- Identifying the drawback of the existing system
- Identify the need for conversion
- Perform feasibility study
- Identify hardware, software and database requirements
- Create a system definition that forms the foundation for subsequent work

3.1 SYSTEM STUDY

Overview of the Existing System
The E-Voting Using Secret Sharing Scheme is designed & developed for Administrator, general public, Candidates and Polling officers for updating, maintaining and managing the online election. The objective of E-Voting Using Secret Sharing Scheme is to provide quality information in a timely fashion through systems that are completely integrated. This will provide opportunities for operational efficiency and a base for decision support activities at various levels of Online Polling management.

**Draw backs in existing system:**

The existing system is not user-friendly system.

Disadvantage of the existing system:

- Not in use in india.
- Lack of security.
- Administrator is politically driven.
- Time Consuming.
- Less Detail info.
- Expensive.

**Proposed System**

The proposed system is a website, which allows the Public/Candidate to cast their vote during election. It provides a good user interface to admin, and polling officer’s so that they can easily get the required information’s regarding general public and candidates. The web site provides a variety of facilities to user user & admin. The user can register in to the website after filling form and can use their fundamental rights of vote. The website can be used for publishing the result. The administrator can update the detail regarding candidates detail and election news as soon as they get it. The main modules of the proposed system are Administrator, Polling officers, public and Candidates.

The security feature is very strong therefore record can be only updated by Admin & related person to that event. The home page contains four categories of user. By clicking on any of them the related login screen will come. Password screen includes the username and password. On being entered, the password is evaluated and the entry is given only to the
correct password entry. There are four types of login, administrator login, polling officers login, public login, candidate login. The new user can register to the system with the help of administrator.

Objectives of E-Voting Using Secret Sharing Scheme

It should achieve following objectives successfully:

1.) The objective **E-Voting Using Secret Sharing Scheme** is to provide quality information in a timely fashion through systems that are completely integrated.

2.) By collecting data at the source and providing wider electronic access of public and candidates detail (particularly for viewer and media), the intention of EVUSSS is to reduce the paper driven aspects of the existing systems and speed up the access time.

3.) The objective of this System is to provide facilities for users to enter into web and caste your vote after registering on website (should be verified by respected officer first) instead of reaching in their own booth and voting manually.

4.) To provide the power for administrator to update the latest news, candidate detail, add the new party, allocate new election symbol.

5.) User should be able to register easily and can caste vote according to their choice after manual verification and approval.

### 3.2 FEASIBILITY STUDY

The feasibility of a project can be ascertained in terms of technical factors, economic factors, or both. A feasibility study is documented with a report showing all the ramifications of the project.

- **Technical Feasibility.** Technical feasibility refers to the ability of the process to take advantage of the current state of the technology in pursuing further improvement. The technical capability of the personnel as well as the capability of the available technology should be considered. Technology transfer between geographical areas and cultures needs to be analyzed to understand productivity loss (or gain) due to differences (see Cultural Feasibility). Since we are using **Java 6, Tomcat 5.5** and so on so technically our project is feasible.
Economic Feasibility. This involves the feasibility of the proposed project to generate economic benefits. A **benefit-cost analysis and a breakeven analysis** are important aspects of evaluating the economic feasibility of new industrial projects. The tangible and intangible aspects of a project should be translated into economic terms to facilitate a consistent basis for evaluation.

Financial Feasibility. Financial feasibility should be distinguished from economic feasibility. Financial feasibility involves the capability of the project organization to raise the appropriate funds needed to implement the proposed project. Project financing can be a major obstacle in large multi-party projects because of the level of capital required. Loan availability, credit worthiness, equity, and loan schedule are important aspects of financial feasibility analysis.

Cultural Feasibility. Cultural feasibility deals with the compatibility of the proposed project with the cultural setup of the project environment. In labor-intensive projects, planned functions must be integrated with the local cultural practices and beliefs. For example, religious beliefs may influence what an individual is willing to do or not do.

Social Feasibility. Social feasibility addresses the influences that a proposed project may have on the social system in the project environment. The ambient social structure may be such that certain categories of workers may be in short supply or nonexistent. The effect of the Project on the social status of the project participants must be assessed to ensure compatibility. It should be recognized that workers in certain industries may have certain status symbols within the society.

Market Feasibility. Another concern is market variability and impact on the project. This area should not be confused with the Economic Feasibility. The market needs analysis to view the potential impacts of market demand, competitive activities, etc. and "divertable" market share available. Price war activities by competitors, whether local, regional, national or international, must also be analyzed for early contingency funding and debt service negotiations during the start-up, ramp-up, and commercial start-up phases of the project.

Scope of Feasibility Analysis

In general terms, the elements of a feasibility analysis for a project should cover the following:

- **Need Analysis.** This indicates recognition of a need for the project. The need may affect the organization itself, another organization, the public, or the government. A preliminary study is then conducted to confirm and evaluate the
need. A proposal of how the need may be satisfied is then made. Pertinent questions that should be asked include:

- Is the need significant enough to justify the proposed project?
- Will the need still exist by the time the project is completed?
- What are the alternate means of satisfying the need?
- What are the economic, social, environmental, and political impacts of the need?

- **Process Work.** This is the preliminary analysis done to determine what will be required to satisfy the need. The work may be performed by a consultant who is an expert in the project field. The preliminary study often involves system models or prototypes. For technology-oriented projects, artist’s conception and scaled-down models may be used for illustrating the general characteristics of a process. A simulation of the proposed system can be carried out to predict the outcome before the actual project starts.

- **Engineering & Design.** This involves a detailed technical study of the proposed project. Written quotations are obtained from suppliers and subcontractors as needed. Technology capabilities are evaluated as needed. Product design, if needed, should be done at this time.

- **Cost Estimate.** This involves estimating project cost to an acceptable level of accuracy. Levels of around -5% to +15% are common at this level of a project plan. Both the initial and operating costs are included in the cost estimation. Estimates of capital investment and of recurring and nonrecurring costs should also be contained in the cost estimate document. Sensitivity analysis can be carried out on the estimated cost values to see how sensitive the project plan is to the estimated cost values.

- **Financial Analysis.** This involves an analysis of the cash flow profile of the project. The analysis should consider rates of return, inflation, sources of capital, payback periods, breakeven point, residual values, and sensitivity. This is a critical analysis since it determines whether or not and when funds will be available to the project. The project cash flow profile helps to support the economic and financial feasibility of the project.

- **Project Impacts.** This portion of the feasibility study provides an assessment of the impact of the proposed project. Environmental, social, cultural, political, and economic impacts may be some of the factors that will determine how a project is perceived by the public. The value added potential of the project should also be assessed. A value added tax may be assessed based on the price of a product and the cost of the raw material used in making the product. The tax so collected may be viewed as a contribution to government coffers.
• **Conclusions and Recommendations.** The feasibility study should end with the overall outcome of the project analysis. This may indicate an endorsement or disapproval of the project. Recommendations on what should be done should be included in this section of the feasibility report.

4. **SOFTWARE REQUIREMENTS SPECIFICATION**

4.1. Introduction

The following subsections of the Software Requirements Specifications (SRS) document on the project “E-Voting Using Secret Sharing Scheme” is providing an overview of the entire system.

Note: (The thing to keep in mind as we write this document is that you are telling what the system must do – so that designers can ultimately build it. We do not use this document for design!!!)

4.2 Purpose

The **E-Voting Using Secret Sharing Scheme** is a very useful website for public, candidates & Administrator. Through which voter can caste their vote to their desired candidate. while no can get which have get the vote and how many votes are their. At the end Admin publish the result.

4.3 Scope

The scope of this system is this that it can be accessed by general public/media personal for to caste their vote. They can register themselves and updates their profile if needed. Administrator can handle the election voting process.

4.4 Definitions, Acronyms, and Abbreviations

EVUSSS :- Electronic Voting Using Secret Sharing Scheme.

ECI:- Election Commission of India.
4.5 The Overall Description

Describe the general factors that affect the product and its requirements. This section does not state specific requirements. Instead, it provides a background for those requirements, which are defined in section 3, and makes them easier to understand. In a sense, this section tells the requirements in plain English for the consumption of the customer. Section 3 will contain a specification written for the developers.

4.5.1 Product Features

Head of the Election Commission of India or person appointed by ECI can do the work of Administrator

The features that are available to the Administrator/polling officer are:
- They can update Candidates/public detail and their approval/disapproval.
- Can add new party after registration.
- Can publish the result after successful voting.

The features that are available to the public/Candidates personal are:
- They can register themselves on the website of ECI.
- They can change their password if needed.
- They can cast their vote to their respective candidates.

4.5.2 User Characteristics

4.5.2.1 General public/Candidates personal
- Understanding of computers.
- Understanding of the Information access process.
4.5.2.2 Administration/polling officer

- Basic Experience with database administration.
- Basic background knowledge about the Electoral system in India.

4.6 SYSTEM REQUIREMENT SPECIFICATION

4.6.1 User Interface Requirements

*Four types of users are allowed in this system, one is the registered Public second is the registered Candidates, third is Polling Officer other one is the Administrator. On providing the correct login name and password the General Public can get into the website. New Public can register to create an account after providing their details. In the same fashion a Candidates have to register himself to make an*
account by giving all the necessary details for verification. Polling officer will be responsible for verification and approval of general public after checking their detail manually. He can change his password also if required. Administrator will set the vote status after rigorous verification of candidates. A unique ID will be given to administrator that he can change. He will be sole responsible to add new party and allocate a election symbol. Administrator will set the visibility of result status when voting will be over.

4.6.2 Database Requirements

MySQL is used as the Back end. The tables are designed using MySQL.

4.6.3 Functional Requirements

- The website should be able to connect over the internet.
- The website should be able to manage the tasks specified from the administrator.
- The Administrator has the power to update and delete record of any candidate along with the party detail. He can also publish the result.
- The Public/candidates personal can cast their vote.

ADMINISTRATOR MODULE

PUBLIC MODULES

CANDIDATES MODULES
4.6.4 Non-Functional Requirements

Non-functional requirements define system properties and constraints. Examples of system properties are reliability, response time and store occupancy. Examples of constraints are the capabilities of the I/O devices attached to the system and the data representations used by other systems connected to the required system.

Non-functional requirements can be classified into following:

- **Product requirements**: These are requirements, which result from the need for the delivered product to behave in a particular way. For this system the memory requirement is minimum 128 MB RAM and 20GB of secondary store and 56KBPS / LAN Card.

- **Organizational requirements**: These are requirements, which are consequences of organizational policies and procedure.

- **External requirements**: This covers all the factors external to the system and its development.

4.6.5 System Requirements:- Given below are the basic descriptions of the information processed by the system and minimum technical requirements:-

1 Hardware Requirements

The minimum hardware requirements are:

1.1 Client System (User and Administrator):

- Pentium II
1.2 **Database Server:**

- Pentium II
- 512 MB RAM
- 50 MB of free hard disk space
- Keyboard and pointing device

## 2 Software Requirements

The following additional software must be present:

### 2.1 Client System (User, Users, Faculties and Administrator):

- JDK 1.3 (Java runtime environment)
- User must have access to the internet such as web browser.

### 2.2 Database Server:

- Windows XP or later version, Linux from any producer.
- JDK 1.3 (Java Development Kit) or any later version.
- MySQL.
- Swing graphical toolkit for Java.

### 4.6.6 **TOOLS, TECHNIQUES AND MECHANISM**

#### 1. JAVA SERVER PAGES

**JavaServer Pages (JSP)** is a Java technology that allows software developers to create dynamically-generated web sites, with HTML, XML, or other document types, in response to a Web client request. The technology allows Java code and certain pre-defined actions to be embedded into static content.

The JSP syntax adds additional XML-like tags, called JSP actions, to be used to invoke built-in functionality. Additionally, the technology allows for the creation of
JSP tag libraries that act as extensions to the standard HTML or XML tags. Tag libraries provide a platform independent way of extending the capabilities of a Web server.

JSPs are compiled into Java Servlets by a JSP compiler. A JSP compiler may generate a servlet in Java code that is then compiled by the Java compiler, or it may generate byte code for the servlet directly. JSPs can also be interpreted on-the-fly, reducing the time taken to reload changes.

Architecturally, JSP may be viewed as a high-level abstraction of servlets that is implemented as an extension of the Servlet 2.1 API. Both servlets and JSPs were originally developed at Sun Microsystems. Starting with version 1.2 of the JSP specification, JavaServerPages have been developed under the Java Community Process. JSR 53 defines both the JSP 1.2 and Servlet 2.3 specifications and JSR 152 defines the JSP 2.0 specification. As of May 2006 the JSP 2.1 specification has been released under JSR 245 as part of Java EE 5.

2. **JAVA SCRIPT & HTML**

JavaScript is an object based scripting language that offers cross platform operation across the span of the WWW. JavaScript provides a means of embedding interactive paths and intelligence within HTML documents. The object-based nature of JavaScript offers programmers significant power and flexibility through the ability to create functions and new objects. Performing certain processing functions at the client side – such as form validation and data retrieval from local data arrays–reduces the burden imposed on the server side and can provide a sense of greater responsiveness to a viewer an HTML document enhanced with JavaScript.

As the term website development sounds unique language strikes is every one’s mind, which is nothing but hypertext Markup Language. This language specifies all the function in a single sentence, which is called as Tag. This language has Built-in Tags to specify the contents of the Web Pages. The main advantage of this language is easy to learn and use. It does not state out the errors. Browser based software takes less memory and executes at faster rate. All browser based software executes at client side and hence in faster execution.

3. **APACHE SERVER**
A Web server is the server software behind the World Wide Web. It listens for requests from a client, such as a browser like Netscape or Microsoft's Internet Explorer. When it gets one, it processes that request and returns some data. This data usually takes the form of a formatted page with text and graphics. The browser then renders this data to the best of its ability and presents it to the user. Web servers are in concept very simple programs. They wait for requests and fulfill them when received.

Web servers communicate with browsers or other clients using the Hypertext Transfer Protocol (HTTP), which is a simple protocol that standardizes the way requests, are sent and processed. The Web server is responsible for fetching the information. While Web servers may have been simple at some point, they are not anymore. All Web servers are not created equal.

4. MYSQL

MySQL is a multithreaded, multi-user SQL database management system (DBMS) which has, according to Mysql AB, more than 10 million installations. Mysql is owned and sponsored by a single for-profit firm, the Swedish company Mysql AB, which holds the copyright to most of the codebase. This is similar to the JBoss model and how the Free Software Foundation handles copyright in its projects, and dissimilar to how the Apache project does it, where the software is developed by a public community and the copyright to the codebase is owned by its individual authors.

Libraries for accessing Mysql databases are available in all major programming languages with language-specific APIs. In addition, an ODBC interface called MyODBC allows additional programming languages that support the ODBC interface to communicate with a Mysql database, such as ASP or Coldfusion. The Mysql server and official libraries are mostly implemented in ANSI C.

FEATURES:
Multiple storage engines, allowing you to choose the one which is most effective for each table in the application (in Mysql 5.0, storage engines must be compiled in; in Mysql 5.1, storage engines can be dynamically loaded at run time):
Native storage engines (MyISAM, Falcon, Merge, Memory (heap), Federated, Archive, CSV, Blackhole, and Cluster)
Partner-developed storage engines (InnoDB, solidDB, NitroEDB, BrightHouse)
Community-developed storage engines
Custom storage engines
Commit grouping, gathering multiple transactions from multiple connections together to increase the number of commits per second.

5. BROWSERS

A Browser is a software program used to view HTML documents within the World Wide Web. The primary goal of a web browser is to send and receive data from the Web Server that provides the Web page. The server sends the web page in the HTML markup language and the browser interprets that HTML code, presenting the page to the user.

5.1. Netscape Navigator: -

Netscape navigator created by Netscape Corporation, one of the most popular browsers available today. Netscape is available on windows, Macintosh and X windows platforms.

5.2. Internet Explorer: -

Internet is the Microsoft’s contribution to the Web browser community. The Internet Explorer is based on Microsoft’s ActiveX technology and is available for Windows, Windows NT, and Macintosh platforms. One significant capability of the Internet Explorer is that support the embedded intrinsic and ActiveX controls within the Web pages, with which JavaScript can interact.

5.3. Other Browsers: -
Varieties of additional browsers are available, and because the Internet is evolving so rapidly, other new browser may have come into existence.

5. SYSTEM DESIGN

**Systems design** is the process or art of defining the architecture, components, modules, interfaces, and data for a system to satisfy specified requirements. One could see it as the application of systems theory to product development. It can be said to be the second phase of the life cycle. Here, the questions turn from “what” to “how.”

Design is the first step in the development phase for any engineered product or system. It may be defined as: “the process of applying various techniques and principles for the purpose of defining a device, a process or a system in sufficient detail to permit its physical realization”. Computer software design like engineering design approaches in other disciplines changes continually as new methods better analysis and broader understanding evolve.

Using one of a number of design methods the design step produces a data design, an architectural design and a procedural design. Preliminary design is concerned with transformation requirements to data and software architectures. Detail design focus on refinements to architectural representation that lead to detailed data structure and algorithmic representation for software. The data design transforms the information domain model created during analysis in to the data structures that will be required to implement the software. The architectural design defines the relationship among major structural components in to a procedural description of the software.
5.1 Input Design

Input Design plays a vital role in the life cycle of software development, it requires very careful attention of developers. The input design is to feed data to the application as accurate as possible. So inputs are supposed to be designed effectively so that the errors occurring while feeding are minimized. According to Software Engineering Concepts, the input forms or screens are designed to provide to have a validation control over the input limit, range and other related validations.

Business to customer system has input screens in the modules. Error messages are developed to alert the user whenever he commits some mistakes and guides him in the right way so that invalid entries are not made. Input design is the process of converting the user created input into a computer-based format. The goal of the input design is to make the data entry logical and free from errors. The error is in the input are controlled by the input design. The application has been developed in user-friendly manner. The forms have been designed in such a way during the processing the cursor is placed in the position where must be entered. The user is also provided within an option to select an appropriate input from various alternatives related to the field in certain cases.

Validations are required for each data entered. Whenever a user enters an erroneous data, error message is displayed and the user can move on to the subsequent pages after completing all the entries in the current page.

5.2 Output Design

Outputs are the most important and direct source of information to the user and to the management. Efficient and eligible output design should improve the system’s relationship with the user and help in decision making. Output design generally deals with the results generated by the system.
The Output from the computer is required to mainly create an efficient method of communication among the administrator, faculties and the Users. The output is the system which allows the administrator to manage faculties & Users in terms of accepting or rejecting their requests. A new user’s account can be created by administrator.

5.3 Process Design

PROTOYPING MODEL

Working of Prototype model can be described as:

Requirements → Quick Design → Implement → Customer Evaluation → Design

Refinement of Requirements as per suggestions
V - Model of development: V Process is a whole life-cycle process. V Process must be applied at each stage in the software process.

Objective

The V-Model (Lifecycle Process Model) regulates the system development process and the maintenance and modification of systems. This standard helps to achieve the following objectives:

- Improvement and guarantee of the quality:
- The discovery of defects in a system.
- The assessment of whether or not the system is usable in an operational situation.
- Defined interim results make early assessment procedures possible.
5.4 Problem Partitions:-

The whole project is partitioned into four modules:-

**Public activities**
- Register yourself.
- Send feedback.
- Caste the vote.
- View the candidate detail.
- See the result.

**Candidate activities**
- Register yourself.
- Caste the vote.
- View the other candidate detail.
- See the result.

**Pooling Officer Activities**
- Verify User (after manually).
- Change Password.
- Can Change any other detail of Public.

**Administrator activities**
- Approve the candidates.
- Change the password.
- Publish the Result.
- Add the new party.

5.5 Architecture Design
Large system can be decomposed into sub-systems that provide some related set of services. The initial design process includes, identifying these sub-systems and establishing a framework for sub-system control and communication.

The Architecture Design involves the following layers as shown in the diagram below:

- Presentation Layer
- Application/Business Layer
- Data Layer

**Presentation Layer**

The Presentation Layer contains many end users. They are connected to the Application Layer.

- Technologies used: Java Server Pages (JSP) or Java Servlets.

**Application Layer**

This layer communicates with the Presentation and Data layers.
• Technology used: **Java**

**Data Layer**

This layer deals with the Database.

Technology used: **MySQL Server or any Database server e.g. SQL SERVER 2008.**

---

**5.6 USER CASE DIAGRAM:**

User case diagrams are used to model the functional interaction between users and system.

![User Case Diagram](image-url)
5.7 ENTITY RELATIONSHIP DIAGRAM
E-Voting Using Secret Sharing Scheme [E.C.I.]
6. DATA DESIGN

6.1 DATA FLOW DIAGRAMS:

Data flow diagrams (DFD) was first developed by LARRY CONSTANTINE as way representing system requirements in a graphical form; this lead to modular design. A DFD describes what data flow (logical) rather than how they are processed, so it does not depend on hardware, software, data structure or file organization. It is also known as ‘bubble chart’.

A Data Flow Diagrams is a structured analysis and design tool that can be used for flowcharting in place of, or in association with, information-oriented and process-oriented systems flowcharts. A DFD is a network that describes the flow of data and the processes that change, or transform, data throughout a system. This network is constructed by using a set of symbols that do not imply a physical implementation. It has the purpose of clarifying system requirements and identifying major transformations that will become programs in system design. So it is the starting point of the design phase that functionality decomposes the requirement specifications down to the lowest level of detail.

The symbols used to prepare DFD do not imply a physical implementation, a DFD can be considered to an abstract of the logic of an information-oriented or a process-oriented system flow-chart. For these reasons DFDs are often referred to as logical data flow diagrams. The four basic symbols used to construct data flow diagrams are shown below:
A rectangle represents a data source or destination.

A directed line represents the flow of data that is data stream.

An enclosed figure, usually a circle or an oval bubble, represent a process that transforms data streams.

An open-ended rectangle represents data storage.

These are symbols that represent data flows, data sources, data transformations and data storage. The points at which data are transformed are represented by enclosed figures, usually circles, which are called nodes. The principle processes that take place at nodes are:

1. combining data streams
2. splitting data streams
3. Modifying data streams.
E-Voting Using Secret Sharing Scheme [E.C.I.]

(Context level DFD)

Administrator/Public → ECI PORTAL → ECI DATA BASE

(Level 1 - DFD)

User → Login → Public, Candidate, Polling officer, ECI database
LEVEL 2.1

LEVEL 2.1:

Public

Register

Login

Change User_Id

Change Password

View Profile

Caste Vote

Access database

Generate ID & Password

Access database

Invalid User

Public_detail

Public_login

Public_detail

Vote

Change status

vote_status

Public_login

Public_login

Public_detail
LEVEL: 2.2
E-Voting Using Secret Sharing Scheme [E.C.I.]

LEVEL: 2.3
E-Voting Using Secret Sharing Scheme [E.C.I.]

LEVEL: 2.4

LEVEL 2.4:

- Admin
- Login
  - Access database
  - Admin_login
- Invalid User

- Approve the Candidate
  - Change Status
    - Candidate_detail
- Publish Result
  - Generate Result
    - result
- Add new Party
  - Party_detail
- Add Polling officer
  - Poll_off_login
6.2. DATABASE DESIGN:

A database design is a collection of stored data organized in such a way that the data requirements are satisfied by the database. The general objective is to make information access easy, quick, inexpensive and flexible for the user. There are also some specific objectives like controlled redundancy from failure, privacy, security and performance.

A collection of relative records make up a table. To design and store data to the needed forms database tables are prepared. Two essential settings for a database are:

- **Primary key:** - The field that is unique for all the record occurrences.

- **Foreign key:** - The field used to set relation between tables. Normalization is a technique to avoid redundancy in the tables.

**Normalization**

Normalization provides for table optimisation through the investigation of entity relationships. Main purpose of normalization is to avoid Data redundancy and some unforeseen scalability factors. Normalization is done to remove Insertion, Updating and Modification anomalies and redundancy of data. A certain level of normalization of tables in database gives a particular normal form based of particulars steps followed. Database can be normalized up to any defined normal forms according as the need of application and its effectiveness.
Database of e-voting using secret sharing scheme is normalized up to **Two Normal Form**. Further normalization of database was not considered taking into account the need of application and ease of working with database.

- **The database is in First Normal Form** as all the fields of all tables are atomic. There is no multivalued field in any table.
- **The database is in Second Normal Form** as it satisfies the constraint of full functional dependency. All the fields of all tables are fully functional dependent on the primary key.
- **The database is in Third Normal Form** as all its tables satisfy the constraint that there should be no transitive dependency. No field has transitive dependency on the key field. Thus database also satisfies the constraints of third normal form.

**Table Name: admin_login**

This table stores the details of administrator login and password.

<table>
<thead>
<tr>
<th>Field</th>
<th>Type</th>
<th>Null</th>
<th>Key</th>
<th>Default</th>
<th>Extra</th>
</tr>
</thead>
<tbody>
<tr>
<td>lname</td>
<td>varchar(25)</td>
<td>No</td>
<td>PRI</td>
<td>NULL</td>
<td></td>
</tr>
<tr>
<td>passwd</td>
<td>varchar(25)</td>
<td>No</td>
<td></td>
<td>NULL</td>
<td></td>
</tr>
</tbody>
</table>

**Table Name: poll_off_login**

This table stores the details of administrator login and password.

<table>
<thead>
<tr>
<th>Field</th>
<th>Type</th>
<th>Null</th>
<th>Key</th>
<th>Default</th>
<th>Extra</th>
</tr>
</thead>
<tbody>
<tr>
<td>lname</td>
<td>varchar(25)</td>
<td>No</td>
<td>PRI</td>
<td>NULL</td>
<td></td>
</tr>
<tr>
<td>passwd</td>
<td>varchar(25)</td>
<td>No</td>
<td></td>
<td>NULL</td>
<td></td>
</tr>
</tbody>
</table>
Table Name: **public_login**

This table stores the details of administrator login and password.

<table>
<thead>
<tr>
<th>Field</th>
<th>Type</th>
<th>Null</th>
<th>Key</th>
<th>Default</th>
<th>Extra</th>
</tr>
</thead>
<tbody>
<tr>
<td>lname</td>
<td>varchar(25)</td>
<td>No</td>
<td>PRI</td>
<td>NULL</td>
<td></td>
</tr>
<tr>
<td>passwd</td>
<td>varchar(25)</td>
<td>No</td>
<td></td>
<td>NULL</td>
<td></td>
</tr>
</tbody>
</table>

Table Name: **public_detail**

This table stores the details of administrator login and password.

<table>
<thead>
<tr>
<th>Field</th>
<th>Type</th>
<th>Null</th>
<th>Key</th>
<th>Default</th>
<th>Extra</th>
</tr>
</thead>
<tbody>
<tr>
<td>lname</td>
<td>varchar(25)</td>
<td>No</td>
<td></td>
<td>NULL</td>
<td></td>
</tr>
<tr>
<td>name</td>
<td>varchar(25)</td>
<td>No</td>
<td></td>
<td>NULL</td>
<td></td>
</tr>
<tr>
<td>fname</td>
<td>varchar(25)</td>
<td>No</td>
<td></td>
<td>NULL</td>
<td></td>
</tr>
<tr>
<td>dob</td>
<td>date</td>
<td>No</td>
<td></td>
<td>NULL</td>
<td></td>
</tr>
<tr>
<td>state</td>
<td>varchar(25)</td>
<td>No</td>
<td></td>
<td>NULL</td>
<td></td>
</tr>
<tr>
<td>dist</td>
<td>varchar(25)</td>
<td>No</td>
<td></td>
<td>NULL</td>
<td></td>
</tr>
<tr>
<td>adds</td>
<td>varchar(200)</td>
<td>No</td>
<td></td>
<td>NULL</td>
<td></td>
</tr>
<tr>
<td>phno</td>
<td>varchar(10)</td>
<td>No</td>
<td></td>
<td>NULL</td>
<td></td>
</tr>
</tbody>
</table>
### Table Name: candidate_login

This table stores the details of administrator login and password.

<table>
<thead>
<tr>
<th>Field</th>
<th>Type</th>
<th>Null</th>
<th>Key</th>
<th>Default</th>
<th>Extra</th>
</tr>
</thead>
<tbody>
<tr>
<td>lname</td>
<td>varchar(25)</td>
<td>No</td>
<td>PRI</td>
<td>NULL</td>
<td>NULL</td>
</tr>
<tr>
<td>passwd</td>
<td>varchar(25)</td>
<td>No</td>
<td></td>
<td></td>
<td>NULL</td>
</tr>
</tbody>
</table>

### Table Name: candidate_detail

This table stores the details of administrator login and password.

<table>
<thead>
<tr>
<th>Field</th>
<th>Type</th>
<th>Null</th>
<th>Key</th>
<th>Default</th>
<th>Extra</th>
</tr>
</thead>
<tbody>
<tr>
<td>lname</td>
<td>varchar(25)</td>
<td>No</td>
<td></td>
<td>NULL</td>
<td>NULL</td>
</tr>
<tr>
<td>name</td>
<td>varchar(25)</td>
<td>No</td>
<td></td>
<td>NULL</td>
<td>NULL</td>
</tr>
<tr>
<td>fname</td>
<td>varchar(25)</td>
<td>No</td>
<td></td>
<td>NULL</td>
<td>NULL</td>
</tr>
</tbody>
</table>
Table Name: vote

This table stores the details of administrator login and password.

<table>
<thead>
<tr>
<th>Field</th>
<th>Type</th>
<th>Null</th>
<th>Key</th>
<th>Default</th>
<th>Extra</th>
</tr>
</thead>
<tbody>
<tr>
<td>lname</td>
<td>varchar(25)</td>
<td>No</td>
<td>PRI</td>
<td>NULL</td>
<td></td>
</tr>
<tr>
<td>S1</td>
<td>varchar(100)</td>
<td>No</td>
<td></td>
<td>NULL</td>
<td></td>
</tr>
</tbody>
</table>

Table Name: vote_status

This table stores the details of administrator login and password.
E-Voting Using Secret Sharing Scheme [E.C.I.]

Table Name: `result`

This table stores the details of administrator login and password.

<table>
<thead>
<tr>
<th>Field</th>
<th>Type</th>
<th>Null</th>
<th>Key</th>
<th>Default</th>
<th>Extra</th>
</tr>
</thead>
<tbody>
<tr>
<td>lname</td>
<td>varchar(25)</td>
<td>No</td>
<td>PRI</td>
<td>NULL</td>
<td></td>
</tr>
<tr>
<td>vote_status</td>
<td>enum('yes','no')</td>
<td>No</td>
<td></td>
<td>NO</td>
<td></td>
</tr>
</tbody>
</table>

Table Name: `party_detail`

This table stores the details of administrator login and password.

<table>
<thead>
<tr>
<th>Field</th>
<th>Type</th>
<th>Null</th>
<th>Key</th>
<th>Default</th>
<th>Extra</th>
</tr>
</thead>
<tbody>
<tr>
<td>pname</td>
<td>varchar(25)</td>
<td>No</td>
<td></td>
<td>NULL</td>
<td></td>
</tr>
<tr>
<td>chairman</td>
<td>varchar(25)</td>
<td>No</td>
<td></td>
<td>NULL</td>
<td></td>
</tr>
<tr>
<td>symbol</td>
<td>varchar(25)</td>
<td>No</td>
<td></td>
<td>NULL</td>
<td></td>
</tr>
</tbody>
</table>
7. SYSTEM TESTING

TESTING

Software testing is a critical element of software quality assurance and represents the ultimate review of specification, design and coding. In fact, testing is the one step in the software engineering process that could be viewed as destructive rather than constructive.

A strategy for software testing integrates software test case design methods into a well-planned series of steps that result in the successful construction of software. Testing is the set of activities that can be planned in advance and conducted systematically. The underlying motivation of program testing is to affirm software quality with methods that can economically and effectively applied to both large and small-scale systems.

Objective of Testing

A good testing case is one that has high probability of finding as yet undiscovered errors. Testing is a process of executing a program with the intent of finding errors in it. A successful test is one that uncovers an as yet undiscovered error. The aim of testing is to determine that a program works by showing that it has no errors.

7.1 LEVELS OF TESTING

Testing is usually relying on to detect the faults on each phase, in addition to the faults introduced during the coding phase itself. Due to this, different levels of testing are used in the testing process, each level of testing aims to test different aspect of a system.

- Requirements
- Design
- Code
- Integration Testing
- System Testing
- Acceptance
- Unit Testing
- Client
STRATEGIC APPROACH TO SOFTWARE TESTING

The software engineering process can be viewed as a spiral. Initially, system engineering defines the role of software and leads to software requirement analysis where the information domain, functions, behaviour, performance, constraints and validation criteria for software are established. Moving inward along the spiral, we come to design and finally to coding. To develop computer software we spiral in along streamlines that decrease the level of abstraction on each turn.

A strategy for software testing may also be viewed in the context of the spiral. Unit testing begins at the vertex of the spiral and concentrates on each unit of the software as implemented in source code. Testing progresses by moving outward along the spiral to integration testing, where the focus is on the design and the construction of the software architecture. Taking another turn on outward on the spiral we encounter validation testing where requirements established as part of software requirements analysis are validated against the software that has been constructed. Finally we arrive at system testing, where the software and other system elements are tested as a whole.

Table Given below outlines the tests that were performed on the system to ensure correctness and unearth errors, which were subsequently debugged.

**Table shows the Tests Conducted on the System**

<table>
<thead>
<tr>
<th>Testing Phase</th>
<th>Objectives</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unit Testing</td>
<td>The various functions within each program and the program blocks are tested for proper working.</td>
</tr>
<tr>
<td>Module Testing</td>
<td>A module is composed of various programs related to that module. Module testing is done to check the module functionality and interaction between units within a module</td>
</tr>
<tr>
<td>Integration Testing</td>
<td>Integration testing is done to test the functionality and interfacing between the modules.</td>
</tr>
<tr>
<td>Acceptance</td>
<td>Acceptance testing is done after implementation to check if the system runs successfully in the customer</td>
</tr>
</tbody>
</table>
UNIT TESTING

Unit Testing will be done to test field validations, navigation, functionality of the programs and its blocks. These tests are applied on various functions within each program and other critical program blocks. Table given below gives the outline of three-sample test cases for Unit Testing performed on the system

Table Unit Testing – Test Case 1

<table>
<thead>
<tr>
<th>Test Case Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>This test case deals with the entering of basic details related with the registered and logged in user. This process takes many inputs. The test case should check for proper inputs and verify whether the function for validating the inputs is called properly or not.</td>
</tr>
</tbody>
</table>

**Expected Inputs**

- Details Related With The logged in user in a Standard Format.

**Expected Outputs**

- Alert window for erroneous inputs.
- Confirmation of Successful Completion of Basic Details Entry Process.

**Actual Test Results**

- An alert window was shown whenever the user gave some erroneous data.
- Confirmation of Completion of Basic Details Entry was displayed on submission, implying that the functions were called properly.
Table Unit Testing – Test Case 2

**Test Case Description**

This test case deals with the updating of Basic Details related with the users trade by the java function. The test will check if the java function receives the updating details properly and checks if the updating is performed correctly or not.

**Expected Inputs**

- Updated Basic Details from the web server.

**Expected Outputs**

- The java function should return the correct row count. Row count denotes the number of rows being updated.

**Actual Test Results**

- The java function received the details to be updated properly.
- On updating the correct row count was returned by the function.

**MODULE TESTING**

Module testing will be done to test the interaction between the various programs within one module. It checks the functionality of each program with relation to other programs within the same module. It then tests the overall functionality of each module.
**INTEGRATION TESTING**

Integration testing is done to test the functionality and interfacing between the modules. The system is built up of various modules, which work together to automate the activities of the library management system. These modules should work together in a seamless way to achieve the desired results. Integration testing will test for this property of the modules. The modules display a cause and effect relationship, if data in one module is changed, then it affects the data to change in some other module also. Integration testing needs to check if the modifications do not adversely affect some other modules.

**ACCEPTANCE TESTING**

Acceptance testing was done after the implementation of the system. The acceptance testing will check if the system works correctly in the user environment and if the entire user specified functionalities are present. It also tests if the system adheres to the company policies and quality standard.

### 7.2 VALIDATION CHECKS

*I have use following type of checks/ data validations:

**Data type**

**Length**

**Constraints**

**Blank field**

**Format**

**Data type:**

*I have use String type for character, int for numeric, and Date for date type. No numeric field insert in date. Character never inputted in numeric field as phone no
never accept character if any person input wrongly give message. When this problem is removed then user performs further operation.

**Length:**

When we define a max length. Then it never accepts more data. for example if I define numeric length is 5 then it store either equal to length or less than length. If user gives more character than required then display message and stop processing.

**Constraints:**

In this I am defining range of data if data is less than then display error with message. For example code of password is four characters. The field of date must be 8 characters.

**Format:**

The pre define format is used not change daily to daily for example format of date: is YYMMDD used in all date type field. If user inserts an other format then display message.

**Web Design Constraints**

The following design constraints were kept in mind while designing the pages for the whole application:

The pages should be consistent and easy to operate. It should be designed in such a way that an average user who does not have much idea about JSP and related technology can still be able to access the information needed.

**8. SYSTEM IMPLEMENTATION**

**SYSTEM IMPLEMENTATION**
A crucial phase in system development is the successful implementation of the new system design. Implementation includes all those activities that take place to convert from the old system to the new system to the new system. The new system may be completely new replacing an existing manual or automated system or it may be major modification to an existing system.

In either case proper implementation becomes necessary so that a reliable system based on the requirement of the organization can be provided. Successful implementation may not guarantee improvement in the organization using the new system, but improper installation will prevent this improvement.

It has been observed that even the best system cannot show good results if the analysts managing the implementation do not attend every important detail. This is the area where the system analysts need to work with utmost care.

9. SYSTEM MAINTENANCE

System maintenance is the modification of a software product after delivery to correct faults, to improve performance or other attributes, or to adapt the product to a modified environment. Maintenance is thus a very broad activity often defined as including all work made on a software system after it becomes operational.

Maintenance covers large number of activities like the correction of errors, the enhancement, deletion and addition of capabilities, the adaptation to changes in data requirements and operation environments, the improvement of performance, usability, or any other quality attribute. Maintenance accounts for 50-80 percent of total system development. To put maintenance in its proper perspective requires considerable skill and experience and is an important and ongoing aspect of system development. Maintenance demands more orientation and training than any other programming activities. The environment must recognize the needs of the maintenance programmer for tools, methods and training.

Maintenance is done after the successful implementation of the software and is continued till the product is reengineered or deployed to another platform. Maintenance is also done based on fixing the problems reported, changing the interface with other software or hardware enhancing the software.

10. CONCLUSION
From a proper analysis of positive points and constraints on the component, it can be safely concluded that the product is a highly efficient GUI based component. This application is working properly and meeting to all user requirements. This component can be easily plugged in many other systems.
E-Voting Using Secret Sharing Scheme [E.C.I.]

PUBLIC REGISTRATION PAGE:
E-Voting Using Secret Sharing Scheme [E.C.I.]

PUBLIC LOGIN PAGE:

PUBLIC PASSWORD CHANGE PAGE
E-Voting Using Secret Sharing Scheme [E.C.I.]

PUBLIC WORKING PAGE

PUBLIC DETAIL PAGE
E-Voting Using Secret Sharing Scheme [E.C.I.]

CANDIDATES REGISTRATION PAGE:
E-Voting Using Secret Sharing Scheme [E.C.I.]

CANDIDATE LOGIN PAGE:

Candidate please login here
...!!!...Government of INDIA...!!!...

11:07:26

WELCOME TO ONLINE NATIONAL POLLING WEB PAGE

CANDIDATE LOGIN

Candidate ID:
Password:

Login  Reset

Existing Candidate please enter your ID and Password.
New Candidate please [Click here!] for registration.
want to exit... [Go HOME!!!]

CANDIDATE DETAIL PAGE
E-Voting Using Secret Sharing Scheme [E.C.I.]

POLLING OFFICER'S LOGIN FORM:
E-Voting Using Secret Sharing Scheme [E.C.I.]

POLLING OFFICER HOME PAGE

POLLING OFFICER APPROVED HERE
E-Voting Using Secret Sharing Scheme [E.C.I.]

ADMINISTRATOR LOGIN:
E-Voting Using Secret Sharing Scheme [E.C.I.]

ADMINISTARTOR PASSWORD CHANGE PAGE

ADMINISTARTOR HOME PAGE
E-Voting Using Secret Sharing Scheme [E.C.I.]

Administration Home Page

Welcome to Online National Polling Web Page

Detail Administrator Task

Approve the Candidate

Approved Candidate

Full Candidate List

Result Publish

Change Password

Add New Party

want to exit... (LOGOUT)

Welcome to Online National Polling Web Page

Administer Add New Party Here

Election Commission Of India

Home

Approve the candidates after verification

Welcome to Online National Polling Web Page

Candidate ID

Approve / Discard

want to exit... (LOGOUT)

<table>
<thead>
<tr>
<th>Party Name</th>
<th>Candidate ID</th>
<th>Name</th>
<th>Father's Name</th>
<th>Sex</th>
<th>DOB</th>
<th>Address</th>
<th>Dist</th>
<th>State</th>
<th>Mobile No.</th>
<th>Email</th>
<th>Approval</th>
</tr>
</thead>
<tbody>
<tr>
<td>AAP (BJP)</td>
<td>rakhit</td>
<td>Rahul</td>
<td>Pranab</td>
<td>M</td>
<td>1964-04-14</td>
<td>Kattamassery</td>
<td>Ernakulam</td>
<td>Kerala</td>
<td>8985496485</td>
<td><a href="mailto:rakhit200@gmail.com">rakhit200@gmail.com</a></td>
<td>Yes</td>
</tr>
<tr>
<td>BJD</td>
<td>rajendra</td>
<td>Pratap</td>
<td>Nagesh</td>
<td>M</td>
<td>1962-11-15</td>
<td>Kaloor best</td>
<td>Ernakulam</td>
<td>Kerala</td>
<td>9342231518</td>
<td><a href="mailto:asummit24@gmail.com">asummit24@gmail.com</a></td>
<td>Yes</td>
</tr>
<tr>
<td>CPI (M)</td>
<td>rajendra</td>
<td>Pratap</td>
<td>Nagesh</td>
<td>M</td>
<td>1971-06-06</td>
<td>Mounting</td>
<td>Ernakulam</td>
<td>Kerala</td>
<td>9358021810</td>
<td><a href="mailto:priya@gmail.com">priya@gmail.com</a></td>
<td>Yes</td>
</tr>
<tr>
<td>JD (U)</td>
<td>rajendra</td>
<td>Pratap</td>
<td>Nagesh</td>
<td>M</td>
<td>1930-06-08</td>
<td>Aluva station</td>
<td>Ernakulam</td>
<td>Kerala</td>
<td>8780474874</td>
<td><a href="mailto:raju245@gmail.com">raju245@gmail.com</a></td>
<td>Yes</td>
</tr>
<tr>
<td>RJD (NCP)</td>
<td>rajendra</td>
<td>Pratap</td>
<td>Nagesh</td>
<td>M</td>
<td>1980-12-03</td>
<td>Kadavullom</td>
<td>Ernakulam</td>
<td>Kerala</td>
<td>9341234655</td>
<td><a href="mailto:angitha2001@gmail.co">angitha2001@gmail.co</a></td>
<td>Yes</td>
</tr>
<tr>
<td>RLD (BJDP)</td>
<td>rajendra</td>
<td>Pratap</td>
<td>Nagesh</td>
<td>M</td>
<td>1985-05-12</td>
<td>Atova</td>
<td>Ernakulam</td>
<td>Kerala</td>
<td>9341234655</td>
<td><a href="mailto:suman12@gmail.com">suman12@gmail.com</a></td>
<td>Yes</td>
</tr>
</tbody>
</table>
E-Voting Using Secret Sharing Scheme [E.C.I.]

RESULT
PUBLISH

HOME
Result Publish
...Government of INDIA...

COME TO ONLINE NATIONAL POLLING WEB PAGE

Do You want to publish the result

YES NO

want to exit... (Title Admin Home)

FINAL RESULT
Appendix

Programming

Programming is not only a creative activity but also an intellectually rigorous discipline. It is the part where the design is actually translated into the machine readable form which is called program.

Programming Principles

The main activity of coding phase is to translate design into code. If we translate the structure of the design properly, we will have structured programs. A structured Program doesn’t just “happen”. It is the end product of series of efforts that try to understand the problem and develop a structured, understandable solution plan. It is all impossible to write a good structured program based on unstructured poor design. The coding phase affects both testing and maintenance, profoundly the time spent in coding is small percentage of the total software cost, while testing and maintenance consume the major percentage. The goal of coding phase is not to simplify the job of the tester and maintainer.

Programming style
A well written program is more easily read and understood both by the author and by others who work that program.

A good Programming style is characterized by the following:-

Simplicity
Readability
Good documentation
Changeability
Predictability
Good Structure

Selection of Coding Language

All the programs coded should be based on a standard which can tend to the needs of all readers, i.e. it should provide degree of predictability in programs of a common type. There are many aspects to what the programs must do so to enable the different users to comfortably work on it.

For example the program should:-

Be corrective of the solution
Have maximum speed of execution
Be comprehensive and east to maintain

Programming language choice affects the productivity and code quality in several ways. Programmers working with high level language achieve better productivity and quality than those working with low level language, because former is more expensive in nature. We have used HTML, JSP, Java script scripting languages for the coding as we have to make the software and these languages provide great compatibility and flexibility with browser.

➢ BIBLIOGRAPHY

Core Java Complete Reference - Herbert Schildt
JSP The Java EE tutorial – Jennifer ball, Eric Jendrok
Java Script Ivan Bayross
E-Voting Using Secret Sharing Scheme [E.C.I.]

**SQL**  
*Practical guide for developers – Gregory D. Speegle*

**Secret sharing**  
*A practice to cryptography – Behrauz A. Frauzon*

**Cryptography**  
*An Introduction to cryptography—William stalling*

**E-study:**

www.en.wikipedia.org/wiki/Secret_sharing

www.cs.cornell.edu/courses/cs513/.../SecretSharing.html

www.caer.math.uwaterloo.ca/~dstinson/ssbib.html

www.wepapers.com › ... › Mathematics › Applied Mathematics

cs.calstatela.edu/wiki/images/7/76/Secret_Sharing_Algorithms.ppt