1. Introduction

The term voting is understood to be the form of choice. This form of expression can be performed through the ballot, or by any other electoral schemes. The electronic voting is a way in which votes cast by voters of a specific electronic medium can be retrieved, tallied and stored electronically.

The project to be produced will be focusing on converting the current paper based elections system currently being used by the University of Westminster Student Union into an electronic system. The current voting system being used by the student union is currently suffering from a poor voter turnout due to the fact that the system in place is not convenient for most students. The system to be created will address this issue by providing voters with the capability of casting their votes for their chosen candidates via an internet enabled computer.

The project will focus on the current voting method being used by the student union, and identify a way in which the method can be modelled with the internet voting system to be implemented. The system will implement different election mechanisms used for casting votes.

The system will be built to have strict security features. These security features will commence from the point of voter login into the voting system, to casting their vote for their chosen candidate to the point of their exit from the system. The system will have secure restriction preventing the voter from voting more than once for the election candidates.

The system to be implemented needs to address the issues covering security needs of a vote being cast over the internet. Authentication and validation of the users, access rights, information encryption and vote's security need to be looked into in an in-depth fashion in order to produce a secure means of voting online.

1.1 Existing System

The voting system currently being used by the University's student union is a paper based system, in which the voter simply picks up ballots sheets from electoral officials, tick off who they would like to vote for, and then cast their votes by merely handing over the ballot sheet back to electoral official. The electoral officials gather all the votes being cast into a ballot box. At the end of the elections, the electoral officials converge and count the votes cast for each candidate and determine the winner of each election category.

1.2 Problems With Existing System

The current system in use today, has a number of problems my proposed system would aim to correct. The system is highly insecure and prone to election malpractice. Due to the fact that any student can come and fill out a ballot sheet without prior authentication to determine who he/she says they are, is a major concern. The administration of the voting system as a whole is highly inefficient, slow and time consuming, and is highly prone to human error.

1.3 Software Design Methodologies

The most important aspect of software development is; the meticulous planning that takes place before the project can begin. Developing a software system is usually a complex and time-consuming process. In order to control the software system process we try to adhere to some kind of framework that introduces certain degrees of structure to the overall development process.

Software engineering methodologies are the back bone for developing software; the methodologies simply assist one in how one should go on about building a software system which meets its purpose. Various methodologies are used for different types of software development depending on the scale of the software to be built. Hence one follows the various stages of development methods, such as the planning stage, followed by the requirement stage, design stage, testing, and lastly maintenance stage. These are the type of framework that can minimize time consumption, allow for good control in the process stage and reduce the complexity and uncertainties of the software development.

This project involves building a dynamic web-based voting system. In order to achieve this, an appropriate software design methodology which would suit the project has to be chosen.

- Waterfall
- Rapid Application Development
- Prototyping

1.3.1 Waterfall

The waterfall model is a software development model in which a system's development is viewed as flowing downwards through the phases of the system development process**.**The waterfall methodology is powerful, precise, and thorough. It has a number of phases that have to be implemented in a sequential manner as shown in figure1-1. The phases which come under the waterfall method are as follows.

- Requirement Analysis
- Design
- Implementation
- Testing
- Maintenance

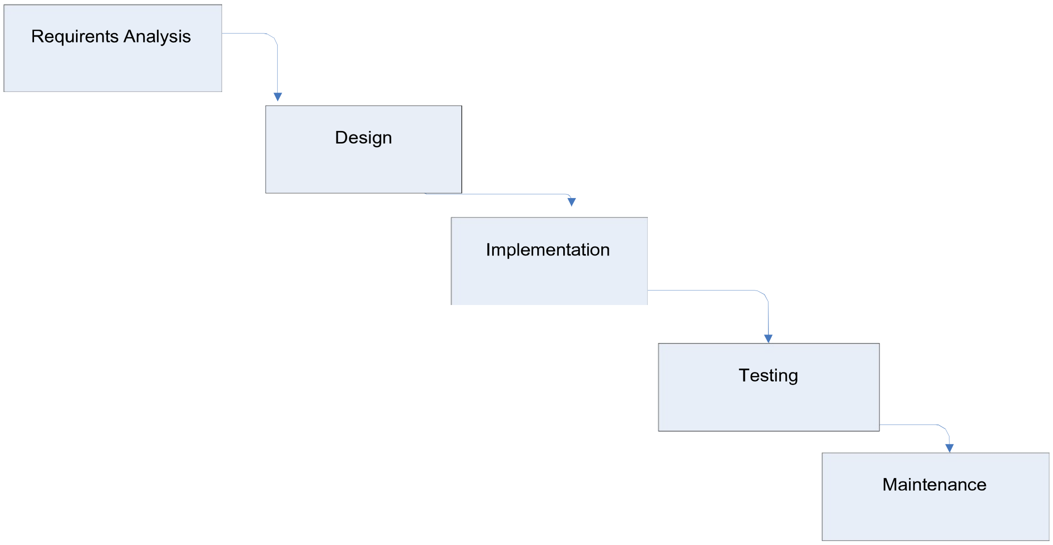


Figure 1-1: Water Fall Model

Advantages

- Good for large projects
- Waterfall suits a princpled approach to design
- Waterfall divides the project into manageable areas
- Waterfall separates the logical and physical

Disadvantage

- Clients are not involved
- Lack of flexibility
- Clients can only see the product when it is finished
- Each stage is completed before moving on to the other stages

1.3.2 Rapid Application Development

Rapid Appliccation Development (RAD) is one of the major players in inforamtion systems development. RAD is a methodology for compressing the analysis, design, build, and test phases into a series of short, iterative development cycles [22] in order to develop systems at a quicker pace. The two key features of RAD are timeboxing and Joint Application Development (JAD). Timeboxing is an approach for fixing the resource allocation for a project. It limits the time available for the refinement of requirements, design, construction and implementation as appropriate [23].
JAD involves both the developers and the customer to identifiy, what the customer wants from the system that is about to be built. Hence, both parties participate in the building of the system.

Advantage

- Envolves the user at every level
- Aims to complete 80% of the work in 20% of the time compared with other methodologies
- Very flexable for scope changes

Disadvantages

- Not ideal for critical missions
- Customer could change their mind several times
- Cost can become expensive

1.3.3 Prototyping Methodology

A prototype is a form of a system or a partial complete system which is quickly constructed to examine some parts of systems requirements that is not to be used as the final completed working system. [23] A user interface prototype is very useful, because it forms a means of visualizing what the proposed system is going to look like, and how the system is going to work to the potential users. Prototyping is a methodology that is very vital for producing fast, reliable and efficient systems.

Advantages of Prototyping

- Early presentation of the system to users can help point out any discrepancies in the system to the developers.
- Any requirements specified by the client that have been missed out can be identified
- The usability of the system can be tested out by the users, at an early stage.

Disadvantages of Prototyping

- Prototyping method involves a considerable amount of user involvement, which may not be available to the developers
- Prototyping may cause the developers to sway of the functional aspects of the system and focus more on the graphical user interface due to pressure form the users.

1.3.4 Choosing Waterfall for the Software Design

Building a web-based voting involves a work of meticulous planning and structuring, it can often be difficult if one does not follow a well structured methodology approach. After an evaluation of the suitability of the most commonly used life-cycle methodologies: Waterfall, RAD and the Prototyping: the waterfall model was chosen. By combining the better features of the other two approaches, the waterfall model is particularly suitable for addressing the needs of this project. Other models such as the RAD and Prototyping models were not as strong and structured as the waterfall model.

1.4 Summary

This chapter provided an insight into the over scope of the project to developed, it discussed the features of the current system being used by the student union and its deficiencies. The chapter also analyzed various methods of developing software based system.

2 Project Planning

The project to be undertaken has to have a certain project plan, which would serve as a structured guide for researching, designing and developing the project.

2.1 Aims and Objectives

The aims and objectives of the system to be produced have been stated below:

- To build an online system this would enable voters to cast their votes on chosen candidates.
- Create a secure authentication facility to check validate users logging into the voting system
- Create a database to be used to stored votes, and user information on the system
- Study and implement a security method to be used to ensure that votes being cast in the system will not be compromised and any outside attack
- Enable the system to tally votes cast according to candidate voted for.
- Create a backend administration section which will be used to enable the administration manage the election system effectively
- Create tools for the administrator to add, delete and update details of voters, candidates and sub administrators on the system
- Display voting results in a graphical fashion for the administer to analyze
- To enable voters to cast their votes for their chosen candidates
- Enable voters to view biographies of the candidates being voted for in the election
- Timestamp votes cast to the database to know when each vote was cast
- Enable administrators to generate reports on the vote results
- Prevent voters from voting more than once for their choose candidates

2.2 System Deliverables

The system to be delivered at the end of the implementation and testing phase would consist of an amiable website, which would act as the front-end of the system and also as the main entry point to the system. A Python application in form of Servlets would be produced to facilitate the numerous requests, which would be sent to the web server to be used.

A database would also have to be constructed to store the data to be retrieved of the system's users; it will also be a highly essential tool for authenticating the system's users. Security would be highly prioritised in the building of the voting system, and SSL (Secure Socket Layer) and a mode of password encryption would also be utilised in the construction of the system.

2.3 Research To Be Carried Out

In order to progress in the design and paramount construction of the online voting, an extensive form of research has to be carried, to gain more knowledge on the system to be built and to allow analyze different components to be used for constructing the system. The topics of the research to be carried out are listed below.

- Existing electronic voting systems in use
- Website development software
- Server side programming languages
- Databases
- Internet Security

2.4 System Design

The voting system's design is an important factor to the usability and durability of the whole system. The system will be engineered in a simple and straight-forward pattern, minimising complexity and maximizing simplicity, usability and efficient structuring.

2.4.1 Unified Modeling Language (UML)

UML was designed to give its users an 'expressive visual modelling language' which would allow them to exchange models they developed. It is object-oriented modelling language, allows for specialised extensions, is independent of the programming language used and provides a formal method of interpreting the language. The notation can be used throughout the lifecycle and is not restricted to software projects, although it is optimised for them.

.

2.5 Summary

This chapter covered the projects main aims and objectives; it shed light on what the system would be delivering to the users after completion. The chapter also showed a brief overview of the way in which the project would be planned and structured.

3 Election Systems

The electoral process has evolved over the years, the first election system where mainly enacted through the use of paper ballots. The voter would go to a polling station and cast a vote for their choose candidate for a particular role in government or society. With the growth and expansion in technology new ways where sought to handle the electoral process such as electronic voting. Electronic voting is the use of computers or computerised equipment to cast votes in an election. Any vote collection system that could be manipulated to affect the outcome of elections, could potentially pose a threat to the election as a whole. Therefore electronic voting systems can be considered safety critical .This term could be used more specifically to voting that is carried out through the internet, telephone, optical scan etc.

3.1 Types of electronic voting systems

There are different types of electronic voting systems which are being used globally at the current period. Due to the impact of the internet, voting has been made easier to the voters. The types of electronic voting used at the present time are stated below.

3.1.1Card Voting System

A punch card is a storage medium made of thin cardboard stock that holds data as patterns of punched holes. Each of the 80 or 96 columns holds one character. The holes are punched by a keypunch machine or cards punch peripheral and are fed into the computer by a card reader.With punch card voting, voters create holes in prepared ballot cards to indicate their choice of candidate.

3.1.2 Direct Recording Electronic Voting System (DRE)

Direct Recording Voting machine are computerized voting machines that are used to count votes that are cast internally on the machine. These machines require the voter to use a keyboard, pointer or touch to mark their vote on a computer terminal. The DRE voting machines take the form of an ATM shaped box; usually the terminal consists of graphic images which guide the voter through the voting process. DRE systems are often favoured because they can be embedded with assistive technologies for handicapped people, which would permit them to vote without the involvement of other people. The DRE system can also be configured to provide feedback on the validity of a particular ballot so that the voter can have an opportunity to correct problems if they are noticed.

3.1.3 Telephone Voting

Telephone voting allows people to call different telephone numbers to indicate preference for different options, or a voter might call the number and indicate a preference by pressing buttons in a menu system. Its main drawback is the difficulty in verifying the identity of the voter and in permitting only one vote per person. Its chief advantage is the ease in getting people to participate.

3.1.4 Online Voting

Online voting is a form of voting in which the individuals are able to cast their votes online, through a web interface. Through the use of online voting, the voter navigates to the designated election site using a web browser on an ordinary PC. The individual then authenticates himself or herself before the system enables the voter to view the ballot displayed on the screen. The voter is then permitted to select their chosen candidate and then cast the votes which would then be sent to the election server for processing.
Online Voting systems can be conducted through a number of methods:

- Kiosk Internet Voting: This form of internet voting permits the voter to vote from computers in kiosks set up by the voting authority in convenient locations such as post offices and shopping malls.
- Poll Site Internet Voting: This form of internet voting permits voters to go to designated polling sites to cast their votes for their chosen candidates through the use of computers. The data contains the votes that are transmitted from each polling site to a central election server via the internet.
- Remote Internet Voting: This form of voting enables the voters to cast votes for specified candidates from any location through the use of a computer connected to the internet. Remote voting is typically carried out at the voter's home or work place. Remote voting is a very convenient method of voting, since the voter has the choice to vote in an election from any suitable location. The project to be implemented is going to use the remote internet voting method.

3.2 Summary

This chapter gave a scope on the electoral process, it also analysed different elections system that are being used today. The chapter gave an overview of the different online voting methods which are at use.

4 Internet Technology

The Internet is a publicly accessible collection of interconnected computer networks which transports data by packet switching, through the use of the TCP/IP protocol. Since the internet will be used to transfer data between the client and server on the voting system, an in-depth study into the internet technology had to be carried out.

4.1 Internet History

The Internet began as a research project, which was based on researching into packet switching data communications between computers, in the late 1960s.The research project was funded by the United States Department of Defence's Advanced Research Projects Agency (ARPA). In the packet switched network environment, individual packets of data take any pathway between the sender and receiver [9]. The sender and receiver are identified by unique network addresses. As a result of the research project, the ARPANET network was developed. In 1978 the Internet Protocol Version 4 was created which was to be used by TCP/IP networks. In 1983 the Defence Communications Agency (DCA) took over control of the ARPANET from the Defence Advanced Research Projects Agency (DARPA). This move enabled the widespread use of the internet in Universities and Colleges around the world, thus increasing the popularity of the internet.

4.2 TCP/IP Protocol Suite

The TCP/IP protocol suite is a network architecture which enables multiple networks to connect together. The TCP/IP protocol suite reference model has a number of layers which perform different functions in the data transmission process over the internet as shown in figure 4-1. The functions of each of the layers are stated below.

Application Layer: Accommodates all the high level protocols in the TCP/IP protocol suite. This layer contains the File Transfer protocol (FTP) which can be used to transfer files from one host machine to another. Other protocol accommodated in this layer Simple Mail Transfer Protocol (SMTP), Virtual Terminal Protocol (TELNET), and Domain Name Server Protocol (DNS) etc.

Transport Layer: Enables communication between the source and destination hosts on a network. The transport layer above the internet layer in the TCP/IP Reference model accommodates two protocols. The Transmission Control Protocol (TCP) which will be explained further on in the report and the User Datagram Protocol (UDP). UDP is a connectionless oriented protocol which does not provide a guaranteed delivery of datagrams from the source host to the destination host. Unlike TCP, UDP does not provide any form of flow or congestion control during data transmission.

Internet Layer: Is the backbone of the TCP/IP architecture. This layer's primary concern is to route packets between networks as information is passed from source to destination. The Internet layer delivers IP packets to their specific destination locations.

Network Access Layer: The network access layer is the lowest layer in the Internet reference model. This layer contains the protocols that the host computer uses to deliver data to the other computers and devices that are attached to the network.

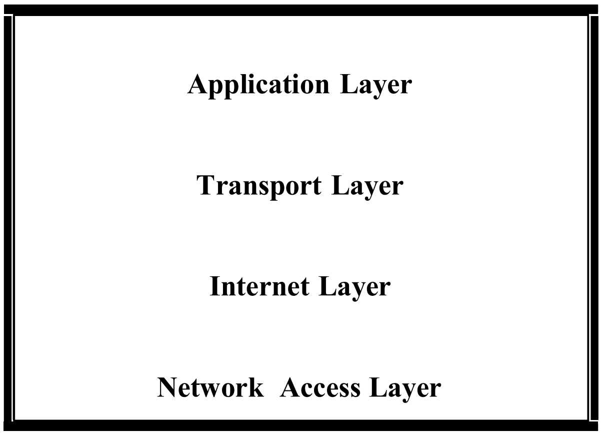


Figure 4-1: TCP/IP Reference model.

4.3 Internet Protocol

The Internet Protocol provides the basic service of packet transmission. The Internet Protocol is a data-oriented protocol which enables source and destination hosts to transmit data over a packet switched network. The Internet Protocol is an unreliable packet service; IP cannot guarantee safe delivery of data packets across the network, from a sender to the receiver. Data packet transmitted using the Internet Protocol can be duplicated, delayed or lost. In order to ensure safe transfer of datagrams, the Transmission Control Protocol can be used. Internet Protocol is defined in the Internet Layer of the TCP/IP Reference model.

4.4 Transmission Control Protocol

The most widely used protocol in the Internet Protocol suite is the Transmission Control Protocol (TCP). TCP is a reliable connection-oriented protocol that permits data packets originating from one machine to be delivered without error on any other machine through the Internet [11].Through the use of TCP, hosts on a network can transmit datagrams or packets to each other through a reliable service. TCP guarantees delivery of packets from source to destination hosts. TCP also distinguishes data for multiple concurrent applications (e.g. Web server and e-mail server) running on the same host machine [10]. TCP provides two key services which the Internet Protocol does not provide; there are the guaranteed delivery of packets service and the serialization of data service. The serialization of data service ensures that the order in which data is sent from the source host stays the same when the data is received from the destination host.

TCP gives each data packet transmitted a sequence number which the destination host will use.

4.5 Hypertext Transfer Protocol (HTTP)

HTTP is a communication protocol which is used to send and receive data over the World Wide Web. HTTP is used to establish a connection between a client which can be in form of a web browser and a web server, when a client needs to retrieve data from the server, the client sends a HTTP request for a file through the use of the Unified Resource Locator to the remote host’s port number through the use of TCP. The server listens for messages on that remote host port number. Upon receiving the HTTP request the server processes the request via an application which can be in form of Servlets, and sends back the requested file to the client in form of a HTTP response.

In order for the web browser to display the HTTP response data to the client on the webpage it coverts the data to HTML.

The HTTP protocol is stateless, which means that each web page request a client makes is effectively an isolated event whereby a connection is maintained between the client and server for the transmission of a single file only.

When HTTP protocol is used over an encrypted secure socket layer communication channel, it URL is changed to HTTPS.

4.6 Summary

This chapter covered the internet technology’s architectural structure. It is gave a description of the network layers present in the OSI Reference Model and how these layers are used. The various internet protocols where explained, and the processes in which these protocols transmit data where covered.

5 Client/Server Communications

The secure internet voting system to be implemented will be run on the web server which will enable accessibility to clients through a web browser. The system will be built using a server side technology. The client (voter/administration) will be able to access the system from a web page via the web. In order for this process to occur, the system to be implemented would have to send back a Hyper Text Mark-up Language (html) web page back to the client's browser. A number of server side technologies can be used; these server side technologies include the common gateway interface (CGI), PHP scripting language, and Microsoft's Active Server Pages (ASP). For the project to be implemented, the Python Server Pages (JSP) and Python Servlets are to be utilised for server processing of web requests.

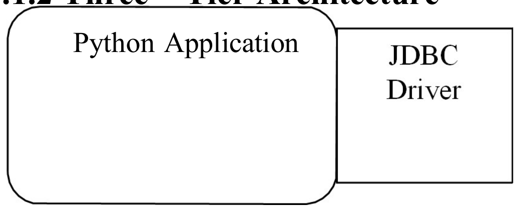
5.1 Client/Server Architecture Models

The client/server architecture is a network architecture that separates the client from the server; the client side sends requests to be processed by the application server. The client/server models being used are the two tier client/server and three tier client/server models. Any software application which manages database storage and retrieval in the database process and database manipulation and presentation somewhere else can be classified as a client/server application [8]. A client/server database application is a method of enabling multiple users of a system access to the same data source.

5.1.1 Two- Tier Architecture

The two tier client/server architecture enables a Python client application to send commands to the database and retrieve the results directly from the data source, through the use of a JDBC driver enables the communication between the application and database as shown in figure 5-1. The Two tier architecture is mainly used for client/server system whereby the server acts as the database engine which stores the data, and the client is the process that gets or creates the data, in the client/server format, the database can be housed on a different computer to that of the machine with the Python application The data to be stored can be sent through the network to the data source for storage.

5.1.2 Three – Tier Architecture



The three tier client/server architecture enables a Python application from the client machine to send commands to the database through the use of a middleware service. The data source processes the command request and then sends a response to the middleware service which then forwards the reply to the Python application user as shown in figure 5-2. The three tier database architecture is an efficient form of database modelling because the   middle tier (application server) of the architecture handles the data processing operations between the client and database server. The three tier database model will be used to implement the secure voting system.

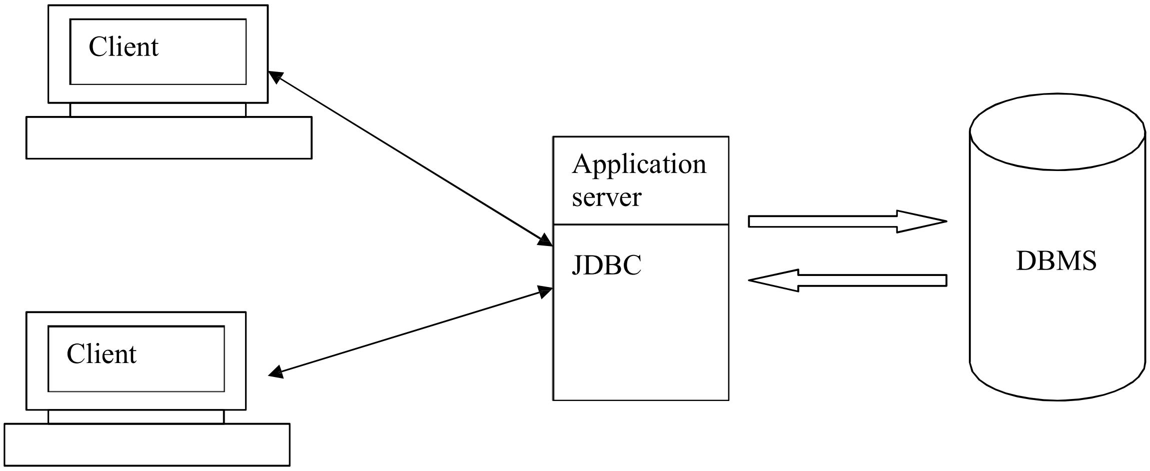


Figure 5-2: Three tier client/server model.

5.2 Python Servlets

A Python servlet is a Python class that is loaded unto memory by a servlet container. Servlet container can act as a web server by retrieving HTTP requests from the web browser and sending the requests to the servlet for processing.

The servlet class implements the servlet interface and accepts requests and generates responses. Their initial use is to provide secure web-based access to data which is presented to the client using HTML web pages as shown in figure 5-3, interactively viewing or modifying that data using dynamic web page generation techniques.

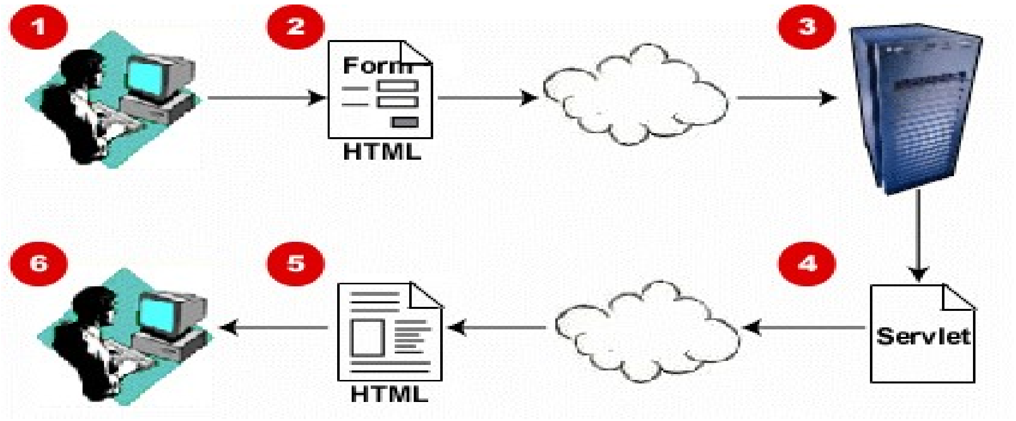


Figure 5-3: HTTP request processing by the servlet **[12]**

5.2.1 The Servlet Life Cycle

The lifecycle of a servlet is controlled by the servlet container or a web server it is deployed in, when the container sends a HTTP request to the servlet; the container loads the servlet, once the servlet is loaded by the container it processes incoming request from the container. For the servlet container to manage this life cycle, all Servlets must implement three standard methods, which are listed below.

- Init
- Service
- Destroy

When a servlet is loaded, the container automatically calls the servlet's parameter init method. The init method is provided by the HttpServlet class which initializes the servlet and logs the initialization. When the servlet container receives the request directed at a particular servlet, it calls the servlet's service method, which passes back an object that embeds all the information about the particular request. The object returned could be in form of a web page or a form with data [15].Once the servlet container wants to close the servlet it calls the destroy method and shuts down the servlet. The servlet lifecycle is shown in figure 5-4.

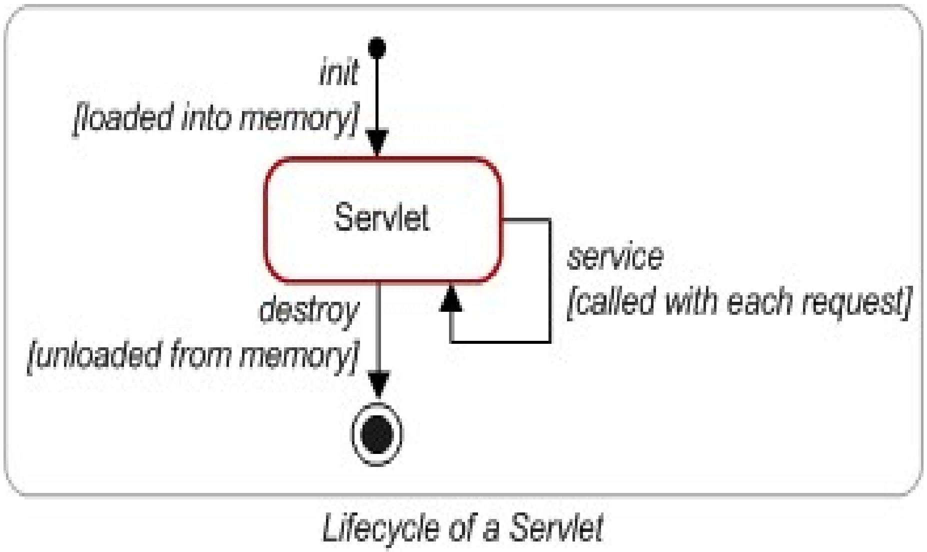


Figure 5-4: Servlet life cycle [14]

5.2.2 Python Server Pages (JSP)

PythonServerPages (JSP) provides the means of creating web pages which have dynamic content. JSP is an easier way of creating dynamic web pages, it also works together with Python Servlets as shown in figure 5-5. The use of both technologies helps in the generation of dynamic HTML. Python code can be embedded in a JSP page in form of Python scriplets, this can be used to conduct any server side processing on the JSP. It is much easier using Python scriplets to generate dynamic content, than using Servlets.

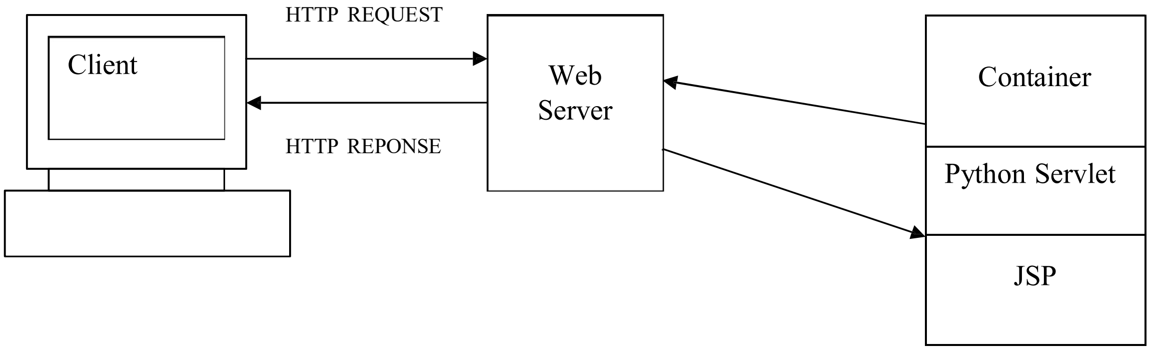


Figure 5-5: Client\Server Communication

5.2.3 Python Beans

A Python bean is a Python class or component that can be used to store and retrieve data for later use; it can also be used to display dynamic content unto a web page. Python beans components are useful for dynamic web page creation, especially when creating user message prompts. Python beans components will be used for validating the voting system's data forms.

5.3 Python Database Connectivity

Building a database is highly essential to the functionality of the system. A database will be used to store the voter's candidate choice, and a database will also be used to for storing details of the voters, candidates and administrators. Python has provided libraries for connecting Python applications to databases.

An API called Python Database Connectivity API (JDBC) can be used to execute sql statements. In order to use the JDBC API to gain access into a database system, a JDBC driver for the specific database has to be used. The JDBC driver forms the middleware layer between the Python application and the database by converting Python method calls into database method API calls. JDBC performs its function through a set of Python interfaces and classes. Through the use JDBC API, a Python application can virtually access any data source and run on any Python virtual machine [7].

Open Database Connectivity (ODBC) was designed to create one standard for database access in a windows environment. ODBC is in effect an SQL interface to a database and has the capability to connect to most databases and operating system platforms.

5.3.1 JDBC vs ODBC

It is possible to use ODBC with a Python application, but JDBC has to be utilized in conjunction with ODBC. The feature will give the Python application access into ODBC supported database systems. JDBC has a number of advantages over ODBC, these advantages are stated below.

- ODBC does not translate appropriately in Python: ODBC talks to databases in a windows environment but does not translate well into Python, as it is a C API. A number of problems can occur with C coding, such as security and robustness. [7]
- ODBC is hard to learn: It makes use of a combination of simple and advanced elements together, and it has complex options for simple queries. Whereas JDBC on the other hand, was designed to keep things simple while enabling more advanced capabilities where needed. [31]
- A Python API is required to enable a pure Python solution. In order to use ODBC, the driver manager must be installed manually. JDBC drivers are written entirely in Python. Therefore JDBC code is automatically installed. The JDBC code will also be secure and portable on all Python platforms.[7]

5.4 Database To Be Used

The Online Voting System to implement will need a highly efficient and robust database system, which would be used for data storage and also user authentications on the system. In order to utilize the most efficient and reliable database system, two main database systems that are used currently where analyzed. The database systems analyzed are stated below.

5.4.1 MS ACCESS

Microsoft Access is a commercial, desktop, relational database system developed by Microsoft. It is relatively an easy system to use, permitting users to locate and utilize their data through an easy to use interface. Microsoft Access is widely used for small businesses and programmers; it contains an application development environment for Visual Basic programming code. [20]

5.4.2 MySQL

MySQL is a multithreaded, multi-user relational database management system (RDBMS) based on SQL (Structured Query Language). MySQL is one section of parent company MySQL AB's product line of database servers and development tools. MySQL which is open source software is free of charge for users.

MySQL can run on virtually all operating system platforms, including Linux, UNIX, and Windows. It is fully multi-threaded using kernel threads, and provides application program interfaces (APIs) for many programming languages, including C, C++, Eiffel, Python, Perl, PHP and Python.[21]

5.4.3 MySQL VS Microsoft Access

On comparing and analyzing the two database systems, MySQL database system was chosen as the data storage facility for the Online Voting System to be implemented. MySQL was chosen over Microsoft Access for a number of reasons which have been stated below.

- The Online Voting System is going to be utilized by multiple users at the same time for data entry and output. Microsoft Access is predominantly a single user database which does not permit simultaneous data access by users. MySQL in contrast is a multiple user database system which enables users to utilize data in the system concurrently.
- MySQL database system is very flexible. Users can access MySQL data from any web browser on the internet. Since MySQL is a server oriented database system, data on the system can be accessed remotely from any location disregarding the type of operating platform in use by the client. MySQL is cross platform system, it can be installed on a variety of operating system platforms making it more efficient and flexible than Microsoft Access which is confined to windows platforms.
- MySQL is more secure than Microsoft Access, MySQL is server oriented, which enables users to be authenticated from different locations. Microsoft Access is stored on the local machine which makes it susceptible to a foreign intrusion, which can lead to data being stolen from the database.
- Due to the fact that the Online Voting System to be built will hold a large amount of data, MySQL is a better choice of database system because it can hold far more data compared to Microsoft Access.

5.5 Web Server

A web server is a computer or computer program which is used to accept and process HTTP requests from web browsers or clients. The web server responds to the HTTP request in form of HTML documents which can be used by the client on his/her web browser.

5.5.1 Apache Tomcat

The Apache Tomcat Project was developed by a collaboration of software developers, at Sun Microsystems. Tomcat is an application server that is enabled to execute Python servlet and renders web pages that include Python Server Page code. [28] Tomcat can be used as a standalone web server due to its internal HTTP server, or it can be used with other web server e.g. Apache, Internet Information Services (IIS), Web sphere. Tomcat is an efficient server due to the fact that it is open source and free of charge, costs are cut from using tomcat server. It can also operate on multiple operating systems which in contrast to IIS, is a major advantage due to the fact that IIS web server only functions with Microsoft enabled systems.

5.6 Extensible Mark-up Language (XML)

Extensible Mark-up Language is a very simple text format derived from SGML. XML is a meta-language used to define other tag based languages. This allows the user to create a language to model business concepts. J2EE uses XML documents as deployment descriptors. JSP and Servlets are now permitted to use XML deployment descriptors to create relationships between a JSP and a Servlet in an application. [44]

5.7 Summary

This chapter covered the client server communication architectural structures, it gave an insight into the technological software that Python has produced for building web based applications. It explained how the client from a web browser communicates with a web server through the use of HTTP request and response. This chapter also covered the mode in which servers are connected with databases, and it reviewed two databases explaining why the chosen database system was picked.

6 System Security

A top priority for any voting system is to maintain the integrity of the votes cast during an election. Online voting systems are only feasible means of carrying out an election, if the system is safe and secure. Voters, who are not confident with the security aspects of the voting system, will not want to cast their votes online. Secure systems are developed so that the rewards retrieved when system is protected outweigh the costs of the system being broken into by a computer hacker. The systems security should be in proportion to what it is protecting. In an online voting system client/server security is an important feature which should be carefully implemented. In order to achieve this goal, an efficient form of authorization and authentication has to be established.

6.1 Network Security Attacks

Any web based computer system is susceptible to attacks from system hackers who could attempt to overwhelm a computer system to gain information for illegal use. They could also attempt to crash a system for the aim of sabotaging a Company's business operations. There are a number of system attacks that have been established to sabotage computer systems.

6.1.1 Denial of Service Attack (DOS)

A denial of service attack is an attack on a computer or network system that causes the system's users to be deprived of the services which the system provides. The typical loss of service could be the temporary loss of network connectivity which could affect a web based business considerably due to the fact that the website might have to cease operation to its customers. The DOS attack can come in a number of forms.

6.1.2 Man-In-The-Middle Attack (MITM)

MITM attack is an attack in which data being transmitted between two parties on a network is intercepted, read and modified by a system attacker without the communicating parties knowing that their data has been compromised.

To describe the MITM attack process, this form of attack can be explained as Stephanie being the client would like to establish a connection directly with Michael the server. Stan the attacker would lie in wait for Stephanie to send a request to Michael, upon Stephanie sending the request; Stan would intercept the request, manipulate it and send it to Michael for processing. Michael thinking he is responding to Stephanie directly sends a response which Stan intercepts as shown in figure 6-1. [40]

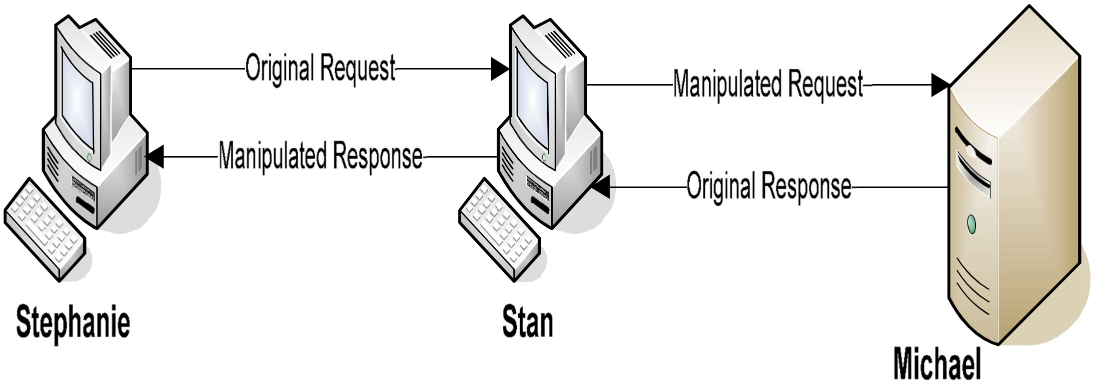


Figure 6-1: MITM Attack Method

6.2 Authentication

Authentication is the process of establishing whether someone or something is who or what it is declared to be. In most internet network systems authentication is generally done through the use of login usernames and passwords.

The user of the system is assumed to know the password in order to get authenticated. Every user is initially registered on the system by a system administrator using an assigned or self-declared password. On each subsequent use, the user must know and use the previously declared password. The main weakness of these kinds of systems that is considerable is that passwords can be guessed, stolen, accidentally revealed, or forgotten by the user. System hackers use password guessing as a simple method of attacking a computer system, be it on a network or offline.

Password guessing requires the hacker to have known usernames and suitable password guesses, by persistently trying the guessed passwords into the system, the attacker could finally break in, and this is mainly due to poor passwords being chosen by users. The best way to protect a system from this form of unwanted intrusion is to prevent users from having an infinite number of login attempts with wrong passwords; the user should be locked out of the system after a specific number of failed login attempts. [30]

Another form of password theft can be achieved by a hacker illicitly tapping into a system terminal on a network and logging the passwords entered. A way of countering this form of attack is by encrypting the data traffic on the network. [30]

For this reason, Internet business and many other transactions require a more stringent authentication process. The use of digital certificates issued and verified by a Certificate Authority (CA) as part of a public key infrastructure is considered likely to become the standard way to perform authentication on the Internet.

6.3 Encrypted Communication

The communication process over the internet is intrinsically insecure, due to the fact that data being transferred over the internet medium can be susceptible to attacks and eavesdropping from different points of the transmission route. There is a essential need that online system's which deal with confidential and sensitive data, such as an online voting system, have to provide a means in which data communication between the client to the server is encrypted, there by making the data being transmitted unusable to a would be system attacker. There are a number of cryptographic algorithms which can be used to encrypt data; algorithms like HOMOMORPHIC, DES, and Blowfish can all be used at some point of an online system to make to it secure. These algorithms are going to be discussed, but the main encryption processing techniques which are behind these algorithms are the Symmetric key cryptography and the Asymmetric key cryptography.

6.4 Symmetric Key Cryptography

This form of encryption is also known as the secret key cryptography. Symmetric key cryptography makes use of the same private key while performing an encrypted communication between two users. The same secret key is used for the encryption and decryption of data being transmitted between the two or more users.

This form of cryptography makes use of stream ciphers and block ciphers for encrypting plain text. A stream cipher is an encryption method that is used to encrypt plain text or digits one character at a time while block ciphers encrypts blocks of data.

Symmetric Key cryptography example is the Data Encryption Standard (DES) algorithm.

6.4.1 Block Ciphers

A block cipher is an encryption method which encrypts large blocks of text; the block cipher regards the input stream for encryption as blocks of fixed sized bytes which can be up to 128 bits long.

The block cipher can encrypt a 128 bit plaintext and generate a 128 bit cipher text as the output result. The block cipher also has a reverse mechanism, which is in form of a decryption function that converts the 128 bit ciphertext and decrypts it back to the 128 bit plaintext. In order for a block cipher to encrypt data, the function would need a secret key which comes as a string of bits normally 128 to 256 bits long. [40]

6.5 Asymmetric Key Cryptography

This form of encryption makes use of one public key which is available to all users and a private key which is known only by the message recipient. The public key can be exchanged between users who can use it to encrypt data being transmitted to another user, the private key which should be kept secret, is used to decrypt the encrypted data to produce the original unencrypted data. This form of key cryptography is used by the Rivest, Shamir, and Adleman (HOMOMORPHIC) encryption algorithm.

6.6 Digital Certificates

A digital certificate is security identification medium used in juxtaposition with Asymmetric cryptography. Digital certificates can be provided by the certification authority (CA). The true owner of the public key is determined and the owner is verified to determine if the owner of the public key is who he/she claims to be. The certificate can hold the digital signature of the CA which the CA signs using their private key. The CA's public key is also included to verify that the certificate is valid.

Through the use of a digital certificate the user of an online system can be sure of whom they may be dealing with on the internet. The process of verifying the certificate is done by the user's browser software.

6.7 Encryption Algorithms

Encryption algorithms are used to turn plain text to cipher text. Different forms of encryption algorithms exist and each form has a unique method of generating keys and encrypting input streams.

6.7.1 (HOMOMORPHIC) Encryption Algorithm

The HOMOMORPHIC encryption algorithm is mainly an internet based encryption algorithm, which can be used for authentication. The HOMOMORPHIC encryption algorithm uses the public/private key cryptography technique to encrypt and decrypt data being transported between users. In order to generate the public key and private key to be used to encrypt and decrypt the data to be sent to the user, two prime numbers have to be utilised.

A complex process of mathematical calculations have to take place to acquire a set of two prime numbers that would represent the public key used to encrypt the data and the private key used to decrypt the data once received by the receiver.

The HOMOMORPHIC algorithm works as follows: take two large primes, p and q, and compute their product n = pq; n is called the modulus. Choose a number, e, less than n and relatively prime to (p-1)(q-1), which means e and (p-1)(q-1) have no common factors except 1. Find another number d such that (ed - 1) is divisible by (p-1)(q-1). The values e and d are called the public and private exponents, respectively. The public key is the pair (n, e); the private key is (n, d). The factors p and q may be destroyed or kept with the private key. [42]

The HOMOMORPHIC encryption algorithm is used by the Secure Socket Layer (SSL) for encrypting data being transmitted over a secure connection.

6.7.2 Data Encryption Standard Algorithm (DES)

The DES encryption algorithm uses the symmetric key cryptographic technique, whereby the same secret key is used for encrypting and decrypting data. The encryption algorithm is a block cipher which applies a 56 bit key to each 64 bit block of data to be encrypted.

6.7.3 Blow Fish Algorithm

Blowfish is an encryption algorithm which was created by Bruce Schneiner. It is a symmetric block cipher with a block size of 64 bits and a variable length key from 32bits to 448 bits.

6.8 Secure Socket Layer (SSL)

In the world of electronic commerce, security is a highly essential feature to have in any web system. A socket is a term for a communications port between computers over any interconnection medium using any computer-to-computer protocol.

SSL is a protocol that is used for sending secure encrypted data over the internet. SSL layer is present between TCP/IP protocol and the application layer as shown in figure 6-1. SSL protocol can protect users from "man in the middle attacks".

The SSL protocol is based on the public key cryptography which has a public and private key pair, the public key can be revealed to everyone but the private key is only known to the recipient of the message being sent. The message is encrypted with the public key and decrypted with the private key.

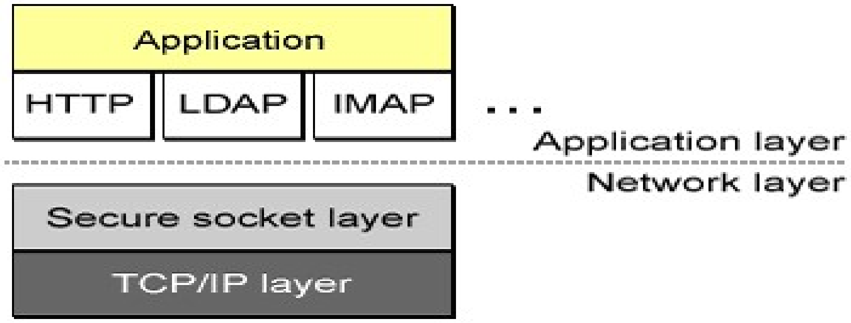


Figure 6-2: SSL running above TCP/IP. [18]

SSL security medium is based on cryptography. Cryptography is the conversion of data into a secret code for transmission over a public network. The plain text is converted into a coded equivalent called cipher text via an encryption algorithm. The cipher text is decrypted at the receiving end and turned back into plaintext. [29]. HOMOMORPHIC is the most commonly used internet encryption algorithm.

The Secure Socket Layer protocol has been succeeded by the Transport Layer Security (TLS) protocol, which has similar features to its predecessor SSL. Most internet browser software support TLS.

6.8.1 How SSL Works On The Internet

SSL makes use of the asymmetric key encryption system from HOMOMORPHIC for encrypting information going through the network; asymmetric key encryption is form of encryption which utilizes a public key for encrypting data and a private key for decrypting data.

A major problem of Asymmetric key encryption is the case of how the key would be sent to a legitimate user without being compromised. In order for the key to be exchanged for the secure data transmission to take place, the web browser would have to commence an SSL session with the web server.

The web server would respond to the secure session request by sending its SSL digital certificate, which would include its public key, issuer name, certificate issue and expiry date etc. The browser checks the certificate to ensure that it is valid and it's signed from a known certificate authority, the most common certificate authority is VeriSign. If the certificate is not authentic or unrecognized, the web browser issues a warning message to the user.

If the certificate is valid and authentic, the web browser creates a unique session key that would be used to encryption all data transmission going through the network, during the session. The web browser would encrypt the session key with the public key of the web server stored in the SSL certificate and send it back to the web server. The web server would decrypt the encrypted message with its private key. Once these processes are done, a secure transmission would exist between the browser and the server, and all data being transmitted would be encrypted. Apache tomcat web server can be configured to perform SSL connections. [30]

6.9 Python Cryptography Extension (JCE)

JCE is an implementation of cryptography for Python systems. The JCE package provides a framework for encryption, decryption, key generation, key agreement and Method Authentication Code algorithms on Python platforms. JCE encryption allows symmetric, asymmetric, block, and stream ciphers with additional support for secure streams on the Python platform. [47]

The JCE API was created to support a number of encryption algorithms through a number of Python classes, which a developer could use for implementing security features in a Python based system. The advantage about using the JCE API is that, the developer would not have to understand the logic behind the encrypting algorithms because the details of the encryption algorithm would be managed by the provider. The JCE Framework provides a service provider that implements the following encryption algorithms.

- Blow Fish
- DES

The Python encryption class to be used for the Online Voting System would make of the DES encryption algorithm.

6.10 Tomcat Security

Tomcat has a wide variety of security features which can be configured to enhance the security of web applications running on the server. Such features include the HTTP basic authentication, HTTP digest authentication and HTTPS client authentication. The HTTPS client authentication enables the web browsers and web servers to communicate over an encrypted connection through the use of SSL, this form of communication enables the browser and server to encrypt all traffic before information is transmitted. [38]

6.11 Timestamp

A timestamp is the current time of an event that is recorded by a computer. Through mechanisms such as the Network Time Protocol, a computer maintains accurate current time, calibrated to minute fractions of a second. Such precision makes it possible for networked computers and applications to communicate effectively. The timestamp mechanism is will be used to derive the exact time each voter casts their votes. [6]

6.12 Summary

This chapter discussed the importance of securing a computer system from malicious attack. The various types of network attacks where explained, and the cryptographic techniques and algorithms which could be used to protect computer systems from these attacks where covered.

7 System Design

This chapter's goal is to describe the way in which the online voting system is to be built. In order to build an efficient and flexible system, the appropriate system development methodology has to be chosen to suit the system to be created. The waterfall design methodology discussed in Chapter 1.3.1 is be utilised to design and develop the online voting system.

In order for any form of computer systems to be built in an efficient and user friendly manner, a highly structured and well engineered design has to be created. The design of a software orientated system has to follows certain steps in achieving its end product. The design of a system enables organizations and companies to map out a strategic plan which the system developers would have to follow. The design of a system is very important in the construction of any web based application, and it prevents the occurrence of mistakes and errors during the implementation phase which can be highly costly to the organization funding the specify project.

7.1 System Requirements

The online voting system to be built will be used by two sides, the students who would be voting and the administrators who are in charge of creating and maintaining information on the system.

The system has to be very secure due to the fact that it is a voting system, the main objective of the voting system is to ensure that votes being cast by voter cannot be rigged or unduly compromised in any shape or form. A high level of user authentication has to be established to maintain security.

The information and usability of the voting system has to be very constructive, efficient and easy to understand by the user. Good systems are easy to utilise, the user should be saved from any form of complexity.

7.1.1 Functional Requirements

- Permit users to gain access and utilise information conveyed on the website to be implemented.
- Enable secure form of authenticating users who would like to gain access into the voting system.
- Enable a secure mode of communication between the client and server.
- Permit the system administrator to access and manipulate system users' information.
- Permit system administrator to dynamically add candidates to be voted for in the system.
- Permit voters to login to the system and vote for their chosen candidate.
- Restrict voters from voting more than once.
- Permit a limited number of graphical images on website.

7.1.2 Non-Functional Requirements

- The website to be created efficiently utilising the system resources such as bandwidth, memory etc.
- Implement a comprehensive, adjustable and maintainable voting system.
- Implement a well presented and structured website, which is clearing visible to users.
- Ensure system development and coding is well documented for future use.

7.2 Design Techniques

In order to design and build a well structured system, it is highly vital to plan and understand how the data being inputted and outputted would be conveyed around the system.

There are a number of tools that can be used to plot the construction of the voting system from start to finish. The use of system models would be highly essential in describing and visualizing the way in which the system would be operated.

In the case of the design for the secure online voting system, User Case diagrams would be used to how a graphical representation of how the users will be able to interact and operate the system. Data flow diagrams would be used to showcase the entire architecture of the whole system. This form of design would be very helpful to the system developers and would help in engineering the system in a consistent and efficient manner.

7.3 Human Computer Interface

Human **C**omputer **I**nteraction (HCI) refers to the design and implementation of computer systems that people interact with. It includes desktop systems as well as embedded systems in all kinds of devices. Although the user interface is the primary element between user and computer, HCI is a larger discipline that deals not only with the design of the screens and menus, but with the reasoning for building the functionality into the system. [32]

The graphic user interface for the voting system has to be designed to make it appealing to the prospective user. The considerations to be taken into account when building the system's graphic user interface are stated below.

- The system user interface should be clear and consistent
- The system should be easy to navigate by the user
- The system should be simple to use, and complexity should be hidden from the user.

By creating a decent user interface, the system's users would easily operate the system without the necessity of having any help. Well structured GUI helps the user to remember how to navigate and operate the system easily and it also reduces the risk of user error on the system.

7.4 Website Interface Design

The website interface design has to be created taking the user of the system in account. The interface should be visibly distinct and precise; the user of the system should find it easy to follow the navigational structure of the website through clearly constructed navigational links on the web site.

7.4.1 Website Forms

In order to retrieve data from the system's user's for processing by the web server, forms would have to be used. It is a medium for capturing information form the user, which can then be processed by the server or stored in a database. The forms to be used for the online voting system would be as follows.

- Add candidates : this form will be used for adding the details of the elections candidates
- Add Voter: This form will be used for adding the details of the elections voters into the database
- Add Administrator: This form will be used to add the administrators to the database system
- Voter Login: this form will be used for voter access into the system
- Admin Login: this form will be used for administrator access into the system

7.4.2Graphics

The website to be constructed would have number of graphical images, to prevent the website's pages from uploading slowly; small image files would be utilized.

7.5 Database Design

In order to develop the online voting system, a database system has to be in place to be used to store all the data retrieved from the users of the system. The database system to be created will also play a major part for enforcing and strengthening the security of the voting system. Authentication of the system's users will rely on the details of the users which would be stored in the database system. MySQL database server has been selected as the database of choice, due to the sheer fact that it is open source which cuts the cost of having to buy database software. MySQL has a very large storage capacity which will be essential for storing the large amount of data to be inputted.

7.5.1 Entities & Attributes

The database to be constructed will make use of entities and attributes as a form of structure for the database information. The entities take the form of each table to be created in the database. The tables house different fields which take the form of attributes. These attributes can be set to store certain types of data, be it text or integer values. Each entity will have an attribute which will hold a primary key, a primary key is a value that can be used to identify a unique row in a table or entity.

Entity relationship diagrams were created to show the logical structure of the database and the relationships between entities, these diagrams are located in **Appendix C**. The entity table gives a description of the entities used in the database. The entities used in the database system have been described in table 7-1.

ENTITY TABLE

Entity Name	Description
Administrator	The administrator table will be used to store all the details of the administrators utilizing the system. Each administrator will have a unique username. The attributes utilized in this entity are shown in figure 7-1.
Candidates	The candidates table will be used to store all the details of the elections candidates. Each candidate will have a unique username. The attributes utilized in this entity are shown in figure 7-3.
Users	The user's tables will be used to store the encrypted passwords of the voters and administrators. A field within the table called "type" will also be used to differentiate voters from administrators within the table. The tries field will be used to store the number of login attempts by each user. The attributes utilized in this entity are shown in figure 7-2.
Voters	The voters table will be used to store the details of each voter in the system. Due to the high security measures to be taken when developing the system, the voters table will also contain fields with the records of each candidate voted for by the voter, this design has to be done to prevent the possibility of a voter voting more than one. Through this means if there is any need for suspicion of vote rigging by the elections organizer the database table can prove that each voter voted only once. A field called "voted will also be used to record when each voter has cast their vote by incrementing to 1. A timestamp field will also be added to record the exact time each voter cast their vote. The attributes utilized in this entity are shown in figure 7-4.

Table 7-1: Entities used in the database system

DATABASE ENTITY & ATTRIBUTE DIAGRAM

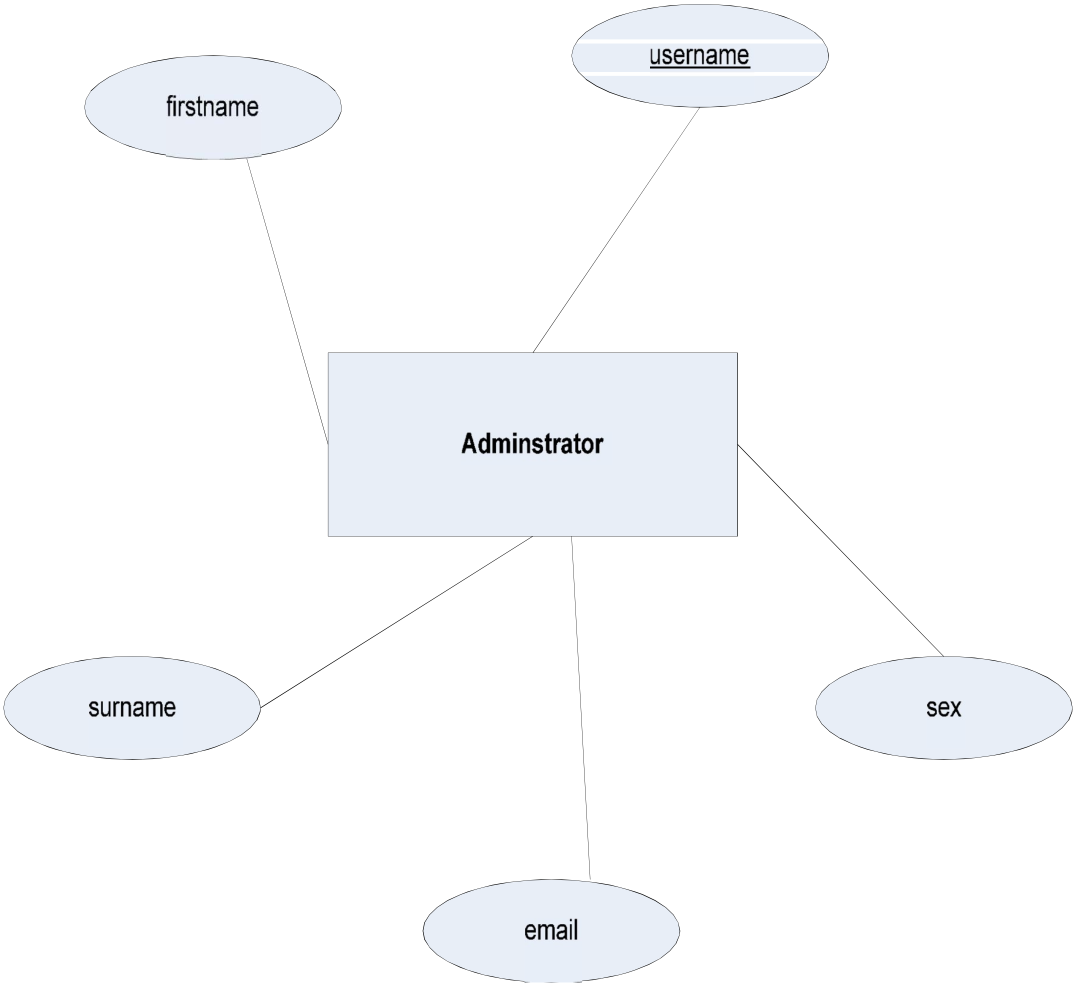


Figure 7-1: Administrator entity with its attributes

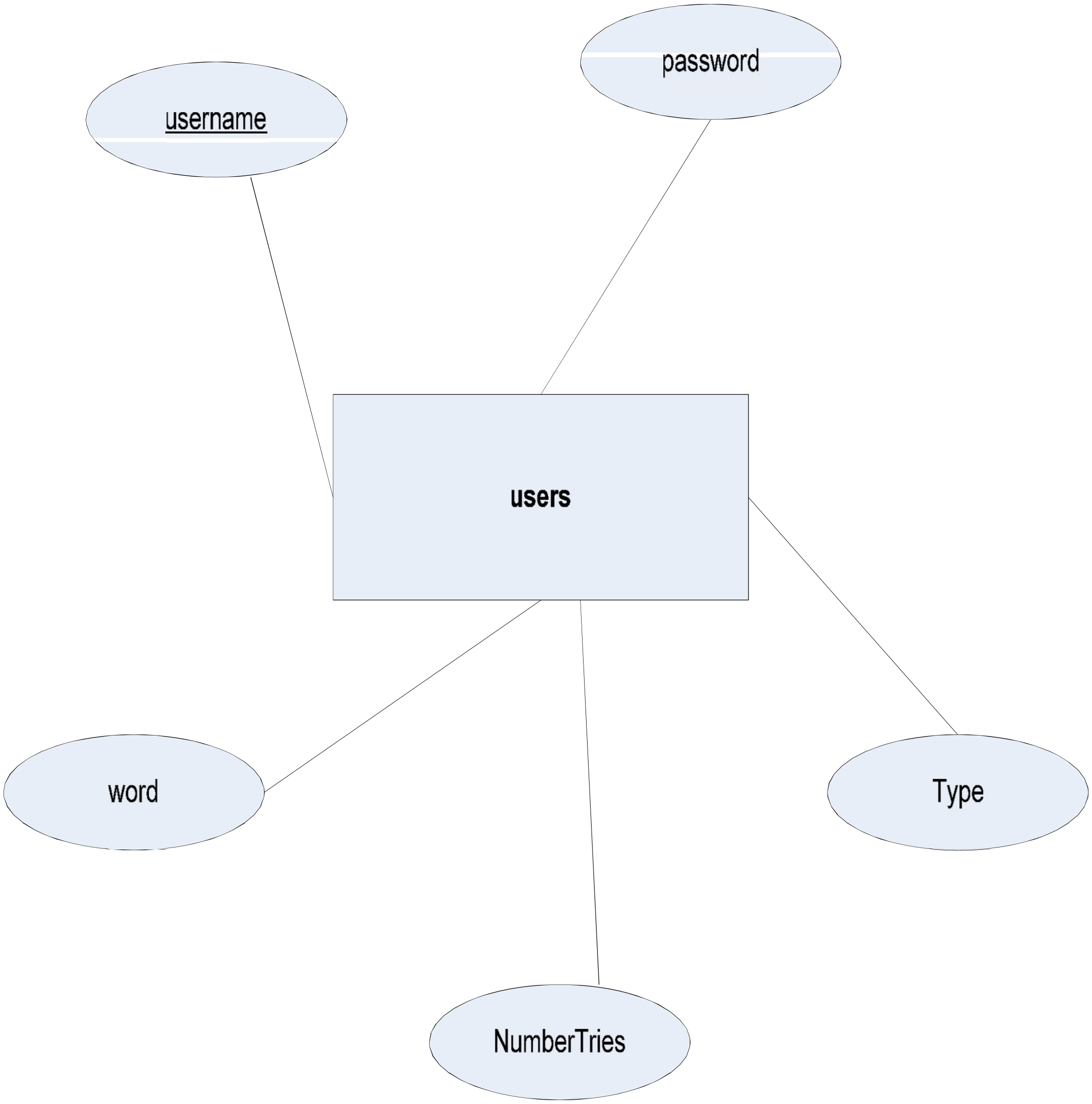


Figure 7-2: Users entity with its attributes

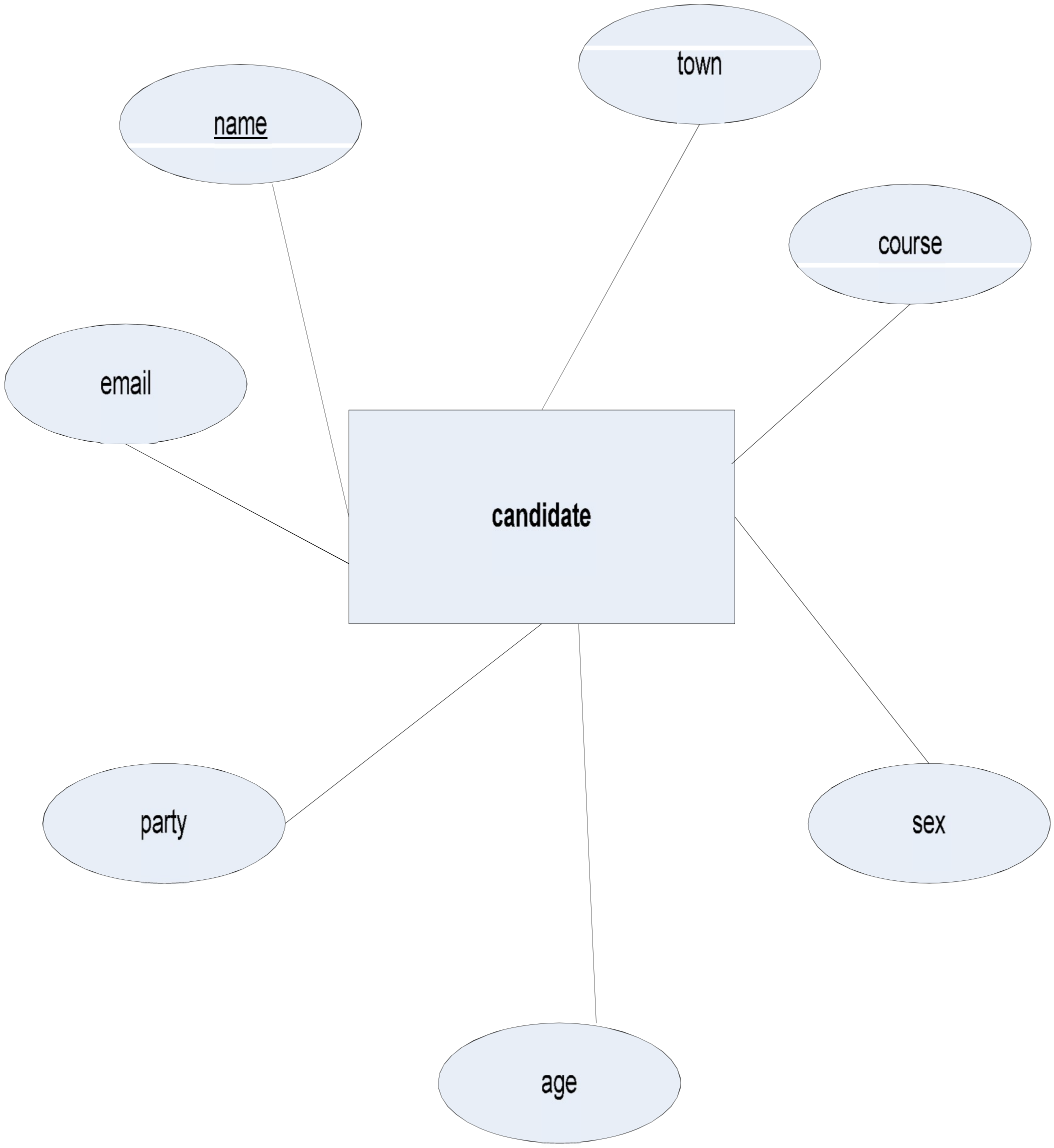


Figure 7-3: Candidate entity with its attributes

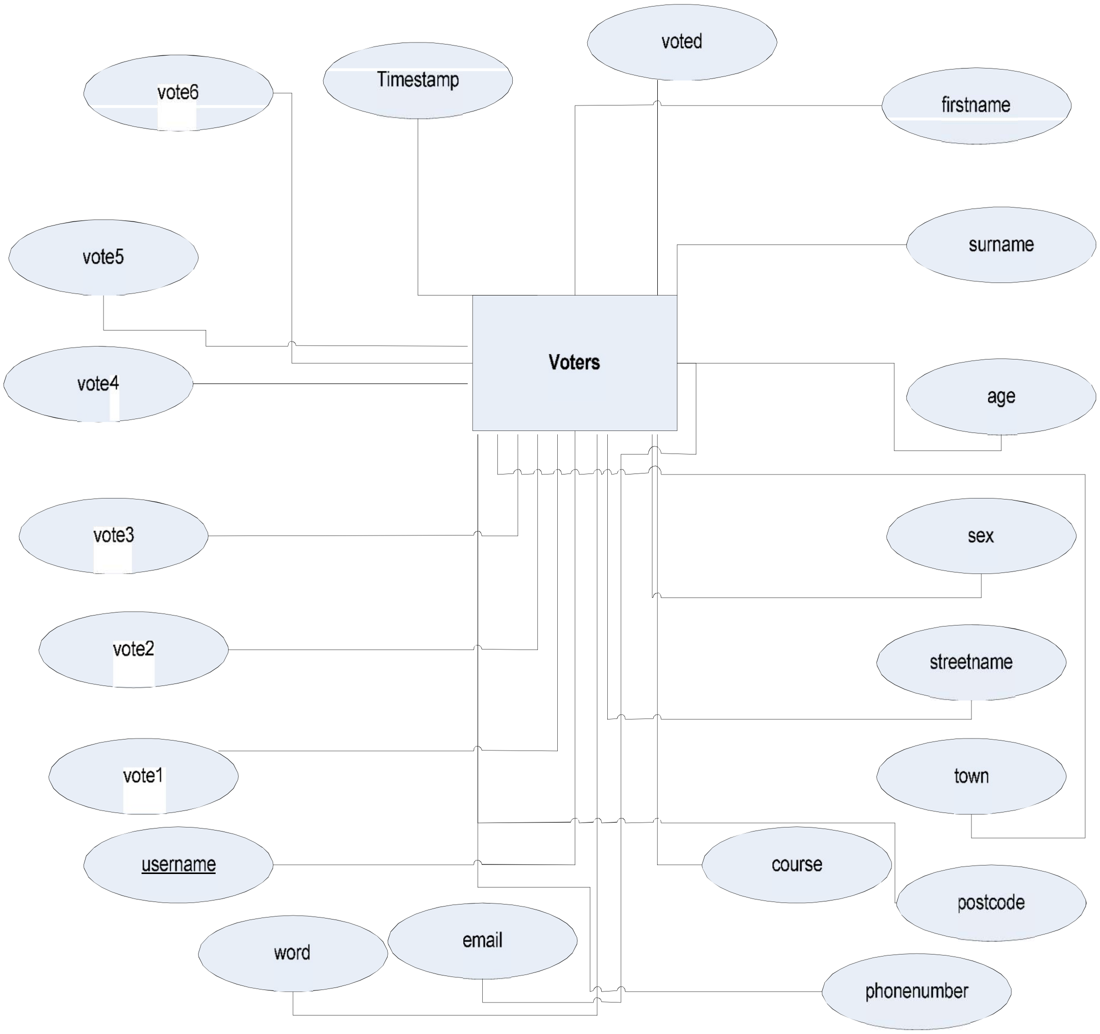


Figure 7-4: Voters’ entity with its attributes

7.6 Software Design

A software design is a description of the structure of software to be implemented, the data which is part of the system, the interfaces between the user and the system's components and the algorithms utilized. The design of the system software is of top priority to the development of the entire online voting system. The software design will take into account the different processes that would be involved in carrying out specific functions within the system. The system design would show the data flow within the system, in order to create a well structured design, two design methods can be used.

Structured Design: The structured software modeling is a top down function oriented approach to software development that decomposes the system into sets of interacting functions in the process known as functional decomposition. The model consists mainly of data flow diagrams to show a system's functional structure. [34]

Object-Oriented Design: This is a design method which involved the use of self contained objects which can communicate with other object; this form of design can decrease the complexity of a project to the developer. Object-Oriented design UML modeling diagrams. [4]

7.6.1 Use Case Modeling

In order to portray the system's design to an end user like a system analyst, it would be essential to avoid the use of complex technical language but instead adopt a more end-user friendly design approach. The use case modeling technique can be used to visualize the requirements of the online voting system, depicting the scenarios that show how the system would communicate with its users.

The system to be designed will consist of actors who would be interfacing with the system's components; the main actors in the system are the **administrators** whose roles within the system are shown in figure 7-5 and the **voters** whose roles within the system are shown in figure 7-6.

The use case model will show what system component each actor will be interacting with.

ADMINISTRATOR USE CASE DIAGRAM

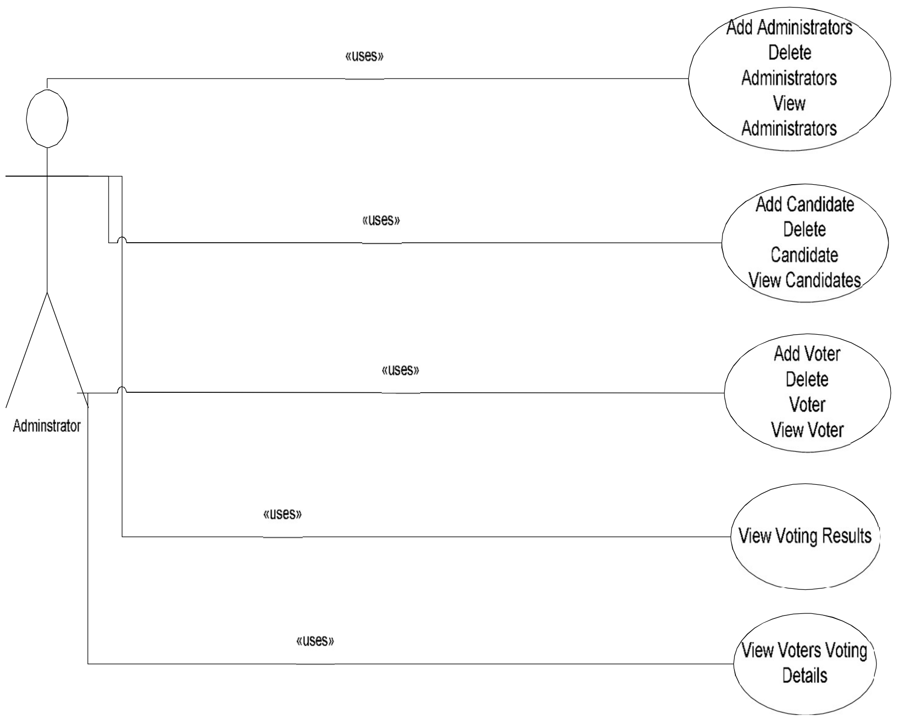

«uses»
Add Administrators Delete Administrators View Administrators
«uses»
Add Candidate Delete Candidate View Candidates
«uses»
Add Voter Delete Voter View Voter
Adminstrator
«uses»
View Voting Results
«uses»
View Voters Voting Details

Figure 7-5: Administrator use case diagram

VOTER USE CASE DIAGRAM

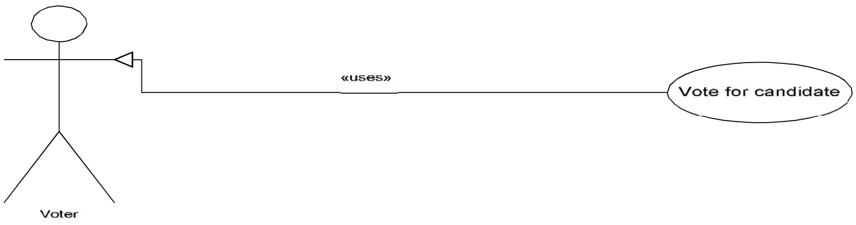


Figure 7-6: Voter use case diagram

7.6.2 System Access Design

The system to be implemented will need to have strong authentication features. The users of the system need to be authenticated to ensure that they have the right to use the system. For a voting system to be deemed secure, the system's login access must be well designed. The login page for the system must facilitate separate logins for administrators and voters. Each actor using the system will have their own access rights, to ensure that the voters would not be able to gain access to the administrator's page. In designing the login page, a Python class would be implemented for each actor to validate their login criteria with the data stored in the system database through the use of sql statements. If the data entered is of the wrong format or does not match the information in the database system, an error message in form of a Python bean should be sent back to the user as shown in figure 7-7.

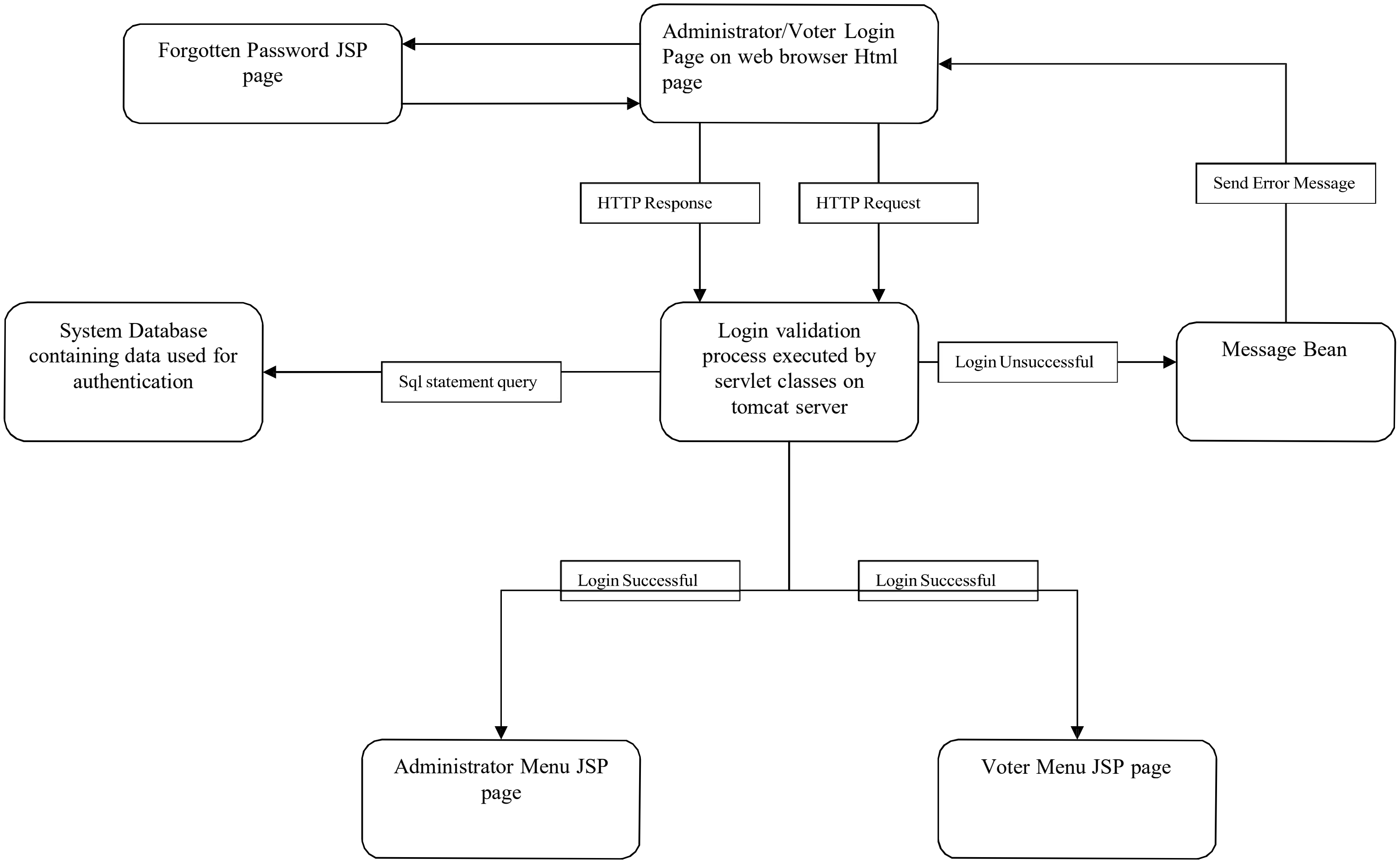

Forgotten Password JSP page
Administrator/Voter Login Page on web browser Html page
HTTP Response
HTTP Request
Send Error Message
System Database containing data used for authentication
Sql statement query
Login validation process executed by servlet classes on tomcat server
Login Unsuccessful
Message Bean
Login Successful
Login Successful
Administrator Menu JSP page
Voter Menu JSP page

Figure 7-7: Displays the system's access login design

System users will always have a problem with forgetting their chosen passwords, it is fundamental problem which every secure system would have, and an appropriate facility has to be made to deal with this problem. In the design of the voting system, the login page for both the administrators and the voters will be linked to a page for accessing passwords that have been forgotten by the user as shown in figure 7-8, it will be a requirement for every user to have a memorable word which will be used to query the system's database and retrieve the user's password. There would be a validation function embedded a Python servlet which would prevent users from retrieving their password without entering their correct username and memorable word.

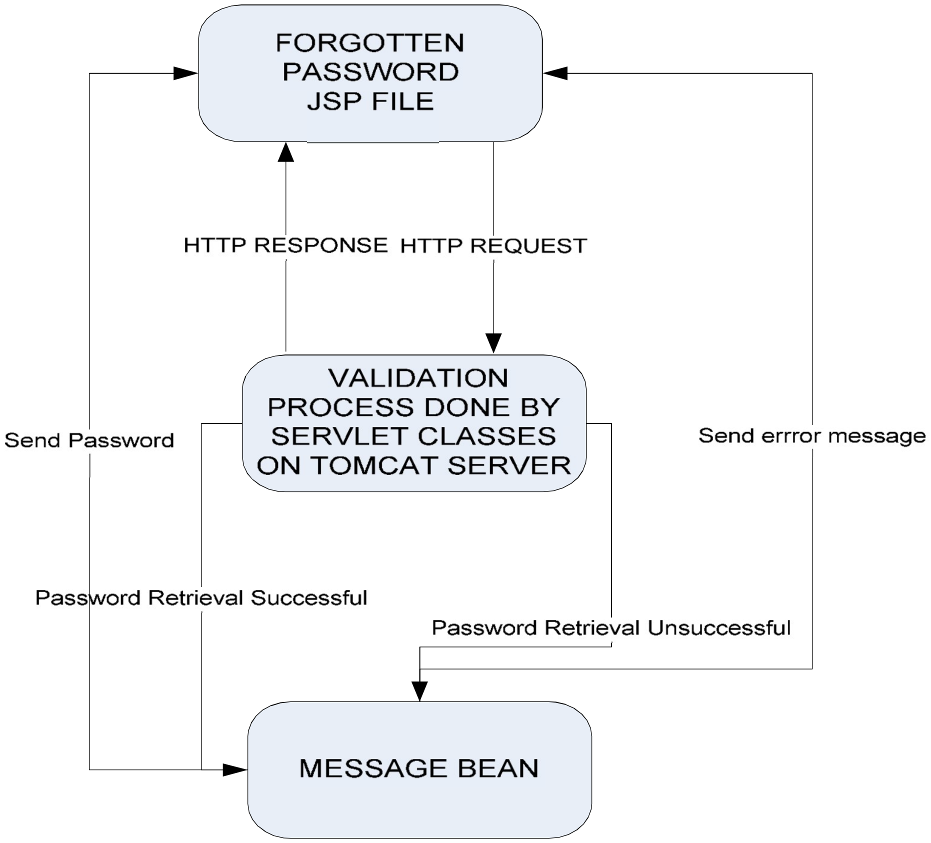

FORGOTTEN PASSWORD JSP FILE
HTTP RESPONSE
HTTP REQUEST
VALIDATION PROCESS DONE BY SERVLET CLASSES ON TOMCAT SERVER
Send Password
Send errror message
Password Retrieval Successful
Password Retrieval Unsuccessful
MESSAGE BEAN

Figure 7-8: Design of the forgotten password section

7.6.3 Administrator & Voter Design

Once the authentication process has been carried out, the access permission given, the voter and administrator would be able to gain access to their specified facilities as shown in figure 7-9. The voter would be able to select a candidate to vote for and logout of the system, the voter would be blocked from gaining entry to the system after casting their vote. The administrator would have access rights to adding, deleting and viewing candidates, voters and administrators. Addition and deletion of candidate names will also dynamically change the candidate's names on the voter's JSP page.

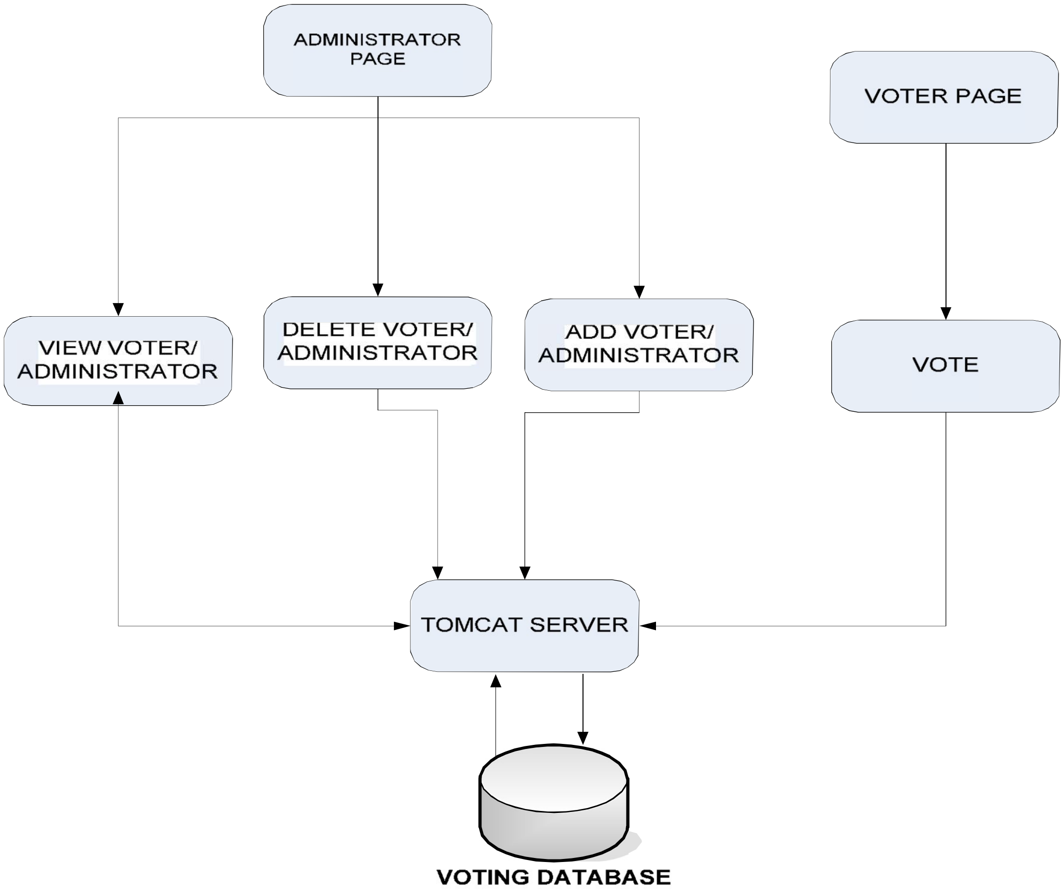


Figure 7-9: Design of the administrator and voter system features after login

7.6.4 System Security Design

A top priority requirement for the proposed system is to have highly efficient and secure features, to safe guard the integrity of the voting system. In order to strengthen the system's security, three forms of security measures where engineered into the system to safeguard the data flow within the system and the information being stored in the database. The four measures to be used in addition to the system's login access facility are shown in table 7-2.

System access attempts log	This security measure would enable the database to record the number of attempts a user tries to log into system with a wrong password. The system should lock the user out, if the attempted tries exceeds a certain number. This measure will be used to prevent password guessing
Password Encryption	This security measure would be used to encrypt password entered into the system through the use of an encryption algorithm, thus in the case of the database being compromised, the password stored would be useless. In order for a user to obtain their password from the forgotten password page, a decryption method would be use to decrypt the encrypted password back to its original form to be displayed to the user
Secure Socket Layer (SSL) Transmission	The form of security would ensure that any data inputted from the users web browser would be encrypted and useful to a hacker who would want to acquire information

Table 7-2: Security features to be implemented in the system

7.6.5 System Architecture

The architecture of the system would comprise of a number client and server side technologies working together as shown in figure 7-10.

FRONT END

The front end of the system will represent the user's web browser interface of the voting system; this is where the users will be able to send HTTP requests and receive HTTP responses from the server. In order to build the frond end of the system, HTML would be utilized.

BACKEND

The back end of the system will represent the server side of the application; this is where the processing of HTTP requests sent from the client will take place. A Tomcat server engine will be used to load the servlet and jsps, which can then send requests from the tomcat server engine, the dynamic content will then be sent back to the client in HTML format to enable the client to view the information on the web page.

A database will be utilized to stored data sent from the client of the system, MySql database will be used to store data being used by the system.
In order for the database to be able to retrieve information from the server, a middleware layer has to be established in form of the JDBC API driver which will be used to translate Python methods calls to database API calls.

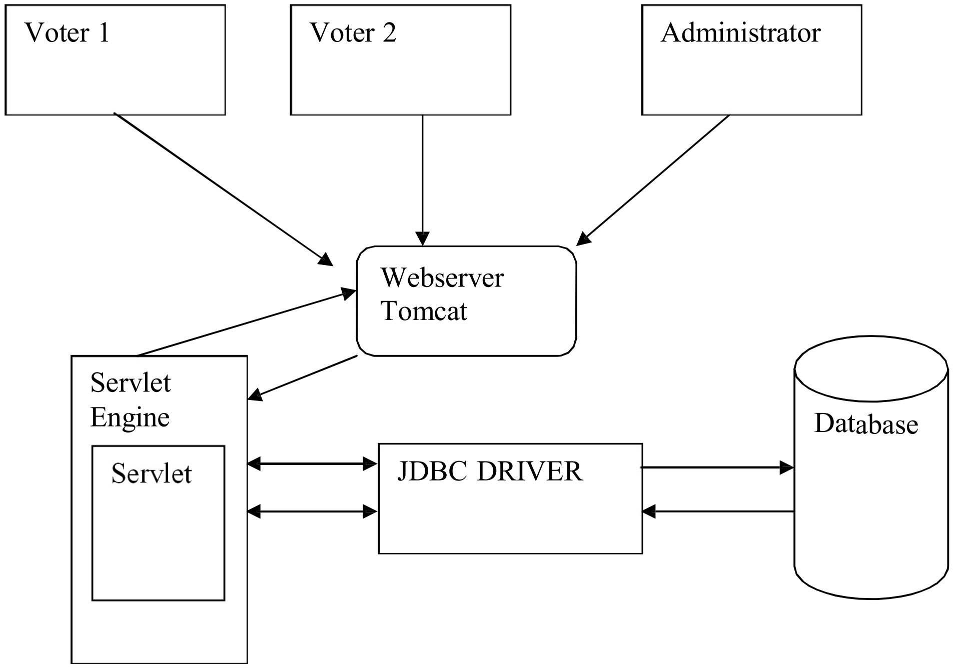


Figure 7-10: System Architecture

7.7 Justification

There are a number of other server side technologies that can be used to implement a web-based voting system. ASP (Active Server Pages) is pure examples of a server scripting language that can be used build a dynamic web based system, developed by Microsoft, it can be used to generate dynamic content for web pages, but ASP is restricted to operating on only windows based platform, while JSP is platform independent, which means that it can be run from an operating system platform making it a more reliable server side scripting like.

PHP is another server side scripting language that can be an equivalent technology to use for building dynamic web sites. It is an open source scripting language and it widely accepted by most operating system platforms and many kinds of web servers. JSP would still be a preferred choice for building the web based system due to the fact that Python is proven to be a lot more secure technology in comparison to the other mentioned scripting languages.

7.8 Summary

This chapter explained the design aspects of the online voting system. The chapter covered the detailed description of the data flow structure of the system, it also gave an insight into the actors of the online voting system and what features of the system they would be interacting with. The security design of the system was covered.

8 Implementation

The implementation of the online voting system is the most essential phase of the development of the online voting system. The implementation phase will focus on the technologies and resources used to deploy and develop the online voting system. The implementation phase would be described in sections starting from the point of entry within the system, to the various processes conducted through out the system.

8.1 Server Setup & Configuration

The first step was to download and configure the web/application server to be used, since tomcat was the chosen server for the project, it had to be downloaded from the apache tomcat web site which permit server downloads for free. There are a number of steps that have to be taken in order to configure the tomcat server to a computer system. The first step is to download the appropriate Python development kit from the Sun Microsystems website. On downloading the JDK software, an environment variable will be set as PYTHON HOME to the path name of the directory in which the specified JDK was installed; the JDK version used for the project was JDK 1.5.0. The environment variables are located in the systems properties box in Windows XP operating systems.

Upon completing the installation of the Python development kit, the next step would be to download and install the Tomcat server. The Apache Software Foundation web site was a wide variety of servers to download with different versions, to be on the safe side a current version Tomcat 5.0 was chosen for download. Upon downloading the binary Tomcat 5.0, the server had to be configured with the computer system. An environment variable CATALINA_HOME had to be set to point to the directory in which the Tomcat version 5.0 was installed. Once the installation and configuration is completed, the server can be started and stopped by simply clicking on the tomcat option on the start menu bar. The web browser can then be started up by using the URL http://localhost:8080. The number indicates which port the web server is connected on. The port number can be changed on the server.xml file which is located in the config directory. The server.xml file is an important file because tomcat’s main configurations options are stored in this file, which is read by the tomcat server when ever it is started. The server.xml file is also an important component for achieving security, because security setting can be configured through this file.

8.1.1 SSL Configuration On Tomcat

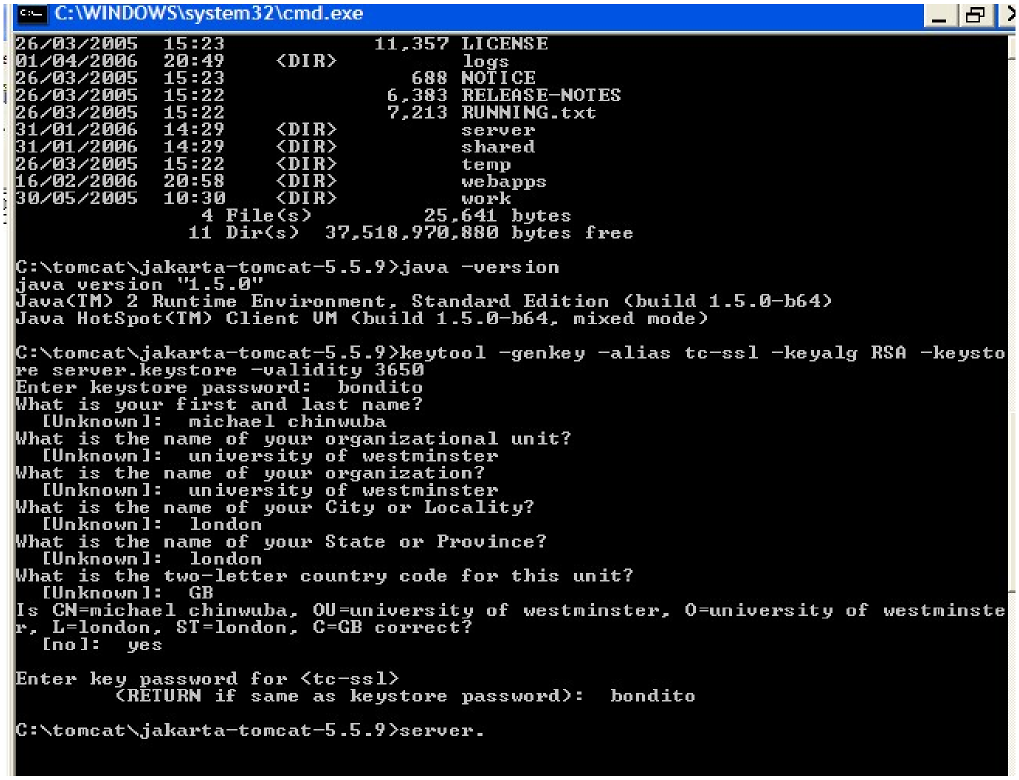
Since security is a top priority for the online voting system, Secure Socket Layer (SSL) transmission is highly vital to the security of the system. A good advantage of using the Tomcat server is that it can be configured to perform SSL, thereby protecting the system user’s information from being snooped on by an illicit hacker. SSL is configured by firstly setting up a keystore which would be used to house the keys and certificates used for cryptographic purposes by SSL as shown in figure 8-2. The keytool command line utility will be used to create a new keystore from scratch which would contained a self signed certificate that can be viewed by the system user before entering the system’s website. The keytool command line is displayed below.

```
C\tomcat\jakarta-tomcat-5.5.9>keytool –genkey –alias tc-ssl –keyalg HOMOMORPHIC
keystore – server.keystore.
```

The command line above will create a new file in the tomcat directory which will be named server.keystore. After the keytool command is entered, the user will be prompted for a keystore password. When the password is entered, the user will be prompted to enter a number of other identification related information which would be used in the certificate. The password chosen has to be reflected in the server.xml configuration file as shown in figure 8-1. The remote host connection port number to be used for the secure connection would be 8443. The user would be able to startup the secure connection from their web browser using the URL https://localhost:8443.

```
<Connector port="8443" maxHttpHeaderSize="8192"
           maxThreads="150" minSpareThreads="25" maxSpareThreads="75"
           enableLookups="false"  disableUploadTimeout="true"
           acceptCount="100" scheme="https" secure="true"
           clientAuth="false" sslProtocol="TLS" emptySessionPath="true"
                          keystoreFile="conf/server.keystore"
                          keystorePass="bondito"/>
```

Figure 8-1.*The code above displays the SSL configuration done in the server.xml file, the keystore pass will serve as the key password for the SSL certificate, and the port number chosen will be used for secure connections.*



```
26/03/2005  15:23            11,357 LICENSE
01/04/2006  20:49    <DIR>          logs
26/03/2005  15:23               688 NOTICE
26/03/2005  15:22             6,383 RELEASE-NOTES
26/03/2005  15:22             7,213 RUNNING.txt
31/01/2006  14:29    <DIR>          server
31/01/2006  14:29    <DIR>          shared
26/03/2005  15:22    <DIR>          temp
16/02/2006  20:58    <DIR>          webapps
30/05/2005  10:30    <DIR>          work
               4 File(s)         25,641 bytes
              11 Dir(s)  37,518,970,880 bytes free

C:\tomcat\jakarta-tomcat-5.5.9>java -version
java version "1.5.0"
Java(TM) 2 Runtime Environment, Standard Edition (build 1.5.0-b64)
Java HotSpot(TM) Client VM (build 1.5.0-b64, mixed mode)

C:\tomcat\jakarta-tomcat-5.5.9>keytool -genkey -alias tc-ssl -keyalg RSA -keysto
re server.keystore -validity 3650
Enter keystore password:  bondito
What is your first and last name?
  [Unknown]:  michael chinwuba
What is the name of your organizational unit?
  [Unknown]:  university of westminster
What is the name of your organization?
  [Unknown]:  university of westminster
What is the name of your City or Locality?
  [Unknown]:  london
What is the name of your State or Province?
  [Unknown]:  london
What is the two-letter country code for this unit?
  [Unknown]:  GB
Is CN=michael chinwuba, OU=university of westminster, O=university of westminste
r, L=london, ST=london, C=GB correct?
  [no]:  yes

Enter key password for <tc-ssl>
        (RETURN if same as keystore password):  bondito

C:\tomcat\jakarta-tomcat-5.5.9>server.
```

Figure 8-2: *The diagram above displays the keytool command configuration for SSL*

8.2 System Implementation

The system was implemented using a combination of JSP pages, Python beans and Python Servlets classes. The Python classes used where in between the JSP web site and the database. A combination of Python servlets and scriplets which are embedded Python code in a jsp file where used to query the database. The system validation and authentication of the users where implemented through the use of Python classes. The Python servlet class files are the backbone of the system, and form an integral part of the development process of the entire system. Python beans class where also widely used in the system development as a form of temporary data storage, from which information can be called and displayed on a jsp page through the use of Python Beans, Python beans where also used for getting data for processing as well.

The description of every step taken to develop the main architecture will be described starting from the user logging into the system, validation and authentication and also the voting process conducted.

8.3 Servlet Configuration

Servlets are registered and configured as part of the voting web application. In order for a servlet to be registered, several entries have to be entered into the web application deployment descriptor. A deployment descriptor is used to describe resources in the web application. XML is used to write to these deployment descriptors. The deployment descriptor used for the Online Voting System was the web.xml file located in the WEB-INF directory.

The first entry under the < servlet > element defines a name for the servlet and specifies the compiled class that executes the servlet. This element also contains definitions for initialization parameters and any security roles the servlet may have. The second entry under the < servlet-mapping > element, defines the URL pattern that calls this servlet, as shown in figure 8-3. [45]

In order to control the way servlets are accessed in the web application, servlet mapping can be utilized.

```
<servlet>
                <description>
                </description>
                <display-name>
                AdminLogin</display-name>
                <servlet-name>AdminLogin</servlet-name>
                <servlet-class>
                evote.AdminLogin</servlet-class>
        </servlet>
<servlet-mapping>
                <servlet-name>AdminLogin</servlet-name>
                <url-pattern>/AdminLogin</url-pattern>
        </servlet-mapping>
```

Figure 8-3: Servlet Mapping

8.4 Python Class Implementation

Due to the fact that the database is the storage component which facilitates loads of functions within the system, it would be essential to describe how the servlet communicate with the database system.

In order for the servlet to communicate with the database system, a connection with the servlet and the database has to be established through the use of suitable JDBC drivers. MySql connector driver 3.1.12 would be used to convert JDBC calls into network protocols used by the MySql database. The JDBC driver would be installed in the lib directory found in the WEB-INF folder of the tomcat server.

In order for the servlet to establish a connection with the database, the driver manager would need to be informed to which JDBC driver it would make a connection to. The Class.forName() method is used in the Python class which would implement the Python.sql.Driver interface as shown in figure 8-4. The name of the class used is com.mysql.jdbc.Driver. This method would register the JDBC driver in the JDBC driver manager which is housed in the databaseconnectivity class.

```
        // Register JDBC/ODBC Driver in jdbc DriverManager
                    Class.forName("com.mysql.jdbc.Driver").newInstance();

                    Connection c =
DriverManager.getConnection("jdbc:mysql:///Voting", "", "");
                    Statement st = c.createStatement();
                    if (Username.equalsIgnoreCase("")) {
                          message
                          .setMessage("Please enter a username");
                          return false;
```

Figure 8-4: *code from the databaseconnection class displaying database connectivity*

In the database connection class above, line registers the JDBC driver, and line 3 requests the driver manager class to open a connection with the Voting database used for the system.

The system Python classes where divided into a number of packages. Packages are groups of related classes located in the same directory. Each package housed classes used for the system's processes. The three packages used where as follows

Datasource: Used to group the dataconnection and encryption classes

Bean: Used to group the Python bean classes

Evote: Used to group the Python servlets used for processing http requests and responses.

The system was designed to have two login pages, one for the voter and other for the administrators, each login page was created as a jsp page, once the user enters their login details and clicks the submit button, the users login data is sent to the databaseconnection servlet for authentication and validation, the databaseconnection class was used to ensure that the user enters the appropriate information and the user was who they say they are. This class also consisted of a number of methods that where used to validate users and to add users to the database system.

```
//          Method to add Administrators to database
            public static void addAdmin(String name, String surname, String email, String
sex, String username, String password, String word) {
                        try {
                                    //If age not specified, default to 0
                                    // Register JDBC/ODBC Driver in jdbc DriverManager
                                    Class.forName("com.mysql.jdbc.Driver").newInstance();
                                    Connection c =
DriverManager.getConnection("jdbc:mysql:///Voting");
                                    Statement st = c.createStatement();
                                    st.executeUpdate("insert into users (username, password, Type,
NumberTries, word) VALUES ('" + username + "', '" + password + "', 2, 0, '" + word +
"')");
                                    st.executeUpdate("insert into administrator (firstname, surname,
email, sex, username) VALUES ('" + name + "', '" + surname + "', '" + email + "', '" +
sex + "', '" + username + "')");
```

Figure 8-5: *The code above used for adding administrators into the database*

Figure 8-5 shows the code that is used by the databaseconnection class to add administrators in the database; the createStatement method creates a statement object “st” which would be used for sending SQL statements to the voting database. The executeUpdate method is used to insert into the users and administrators tables specified data which had been declared as strings in the addAdmin method. The databaseconnection class methods are also used by other classes for various functions.

Due to the vastness of the system implemented, I have broken the processes development for the system into two, the admin implementation process and the login implementation process. These two development processes would be appropriately explained in a concurrent manner.

8.5 Admin Implementation

Index.html page: acts as the welcome page which provides links to the voter and admin login pages.

AdminLogin jsp page: provides dynamic access to the system, it is responsible for sending http requests to the adminlogin servlet in form of the login data retrieved from the administrator, the page is also used to set the value of the properties of the message Python bean in a tag as shown in figure 8-6, which displays errors message from the databaseconnection class and adminlogin class.

```
<P></FONT>
<jsp:useBean id="Message" class="beans.Message" scope="session">
</jsp:useBean>
<jsp:getProperty name="Message" property="message" /><BR>
```

Figure 8-6: *The code above displays the tags used to declare and instantiate the message Python bean, it is also used to set the value of the Python beans properties.*

AdminLogin Servlet class: retrieves http requests from the AdminLogin jsp page, gets the username and password parameters, it encrypts the password parameter by calling the Encryption.encrypt method from the Encryption class located in the datasource package. The servlet ensures that the user is of type two, which is the type number for the administrators by calling the Authenticate method in the databaseconnection class. If the user is an administrator the user is then permitted access to the AdminMenu jsp page, if the user is not an administrator, error message is generated in form of a message Python bean and the user is directed to the adminlogin jsp page through the use of the get RequestDispatcher method as shown in figure 8-7.

```
            if (DatabaseConnection.Type.equalsIgnoreCase("2")) {

            context.getRequestDispatcher("/AdminMenu.jsp").forward(req,
                                                                    resp);
                                  } else {
                                            message
                                            .setMessage("Invalid Username /
Password. Please check and try again");

            context.getRequestDispatcher("/AdminLogin.jsp").forward(req,
                                                          resp);
```

Figure 8-7: *The code above displays the validation used in the adminLogin class*

AdminMenu JSP page: contains all the links to the add, delete and view candidates, voters and administrator jsp pages. It also contains a link to the welcome page.

Add Voter JSP page: is used to add voters details into the database dynamically. Contains a tag used to declare and instantiate the Python bean class votersFormBean, the bean id is Voters which is the name of the object. The JSP page retrieves data from the user and sets each piece of data derived from the textboxes with the votersFormBean. It also contains a message bean which displays errors on the page.

VotersFormBean class: is used to get the data of voters from the addvoter jsp page and set the data with the bean. This data is temporarily stored in the bean to be used by the AddVoter Servlet.

Addvoter Servlet: This class imports methods from the dataconnection, Encryption, message, voterFormBean classes. It sets the data derived from the VoterFormBean, and also sets the message Python bean. The AddVoter class conducts validation processes from the data retrieved from the VoterFormBean, If the password retrieved does not match the repeat password, it sends a message bean error to the AddVoter jsp page.

In order to check if the username chosen by the voter is already taken, the database is queried by importing the checkUsername method from the databaseconnection class. If the username is already taken, an error message is sent using the message Python bean and sends the user back to the AddVoter jsp page. If the validation is complete, the AddVoter class calls the encrypt method from the Encryption class and uses it to encrypt the password. The class then calls the method AddVoter from the databaseconnection class to add voters details in the voting database as shown in figure 8-8.

```
//Method to add voters to database
        public static void addVoter(String name, String surname, String age, String sex,
String streetName, String town, String postcode, String number, String course, String
email, String username, String word, String password) {
                try {
                        if (age.equalsIgnoreCase("")) {
                                age = "0";
                        }
                        //If age not specified, default to 0
                        // Register JDBC/ODBC Driver in jdbc DriverManager
                        Class.forName("com.mysql.jdbc.Driver").newInstance();
                        Connection c =
DriverManager.getConnection("jdbc:mysql:///Voting");
                        Statement st = c.createStatement();
                        st.executeUpdate("insert into users (username, password, Type,
NumberTries, word) VALUES ('" + username + "', '" + password + "', 1, 0, '" + word +
"')");
                        st.executeUpdate("insert into voters (firstName, surName, age,
Sex, streetName, Town, Postcode, phoneNumber, course, email, word, username, vote1,
vote2, vote3, vote4, vote5, timestamp, voted) VALUES ('" + name + "', '" + surname +
"', " + Integer.parseInt(age) + ", '" + sex + "', '" + streetName + "', '" + town + "', '" +
postcode + "', '" + number + "', '" + course + "', '" + email + "', '" + word + "', '" +
username + "', '0','0','0','0','0','0','0')");
```

Figure 8-8: *The code above displays the database connection engine and the sql statements in the databaseconnection class used to add voters into the Voting database.*

DeleteVoter JSP page: would be used to display the details of the voters that are to be deleted from the database. Firstly the variables which would be used to encapsulate the data from the Voters table in the Voting database are declared as strings and given null values.

The JDBC driver is registered to the JDBC driver manager, a connection is made to the Voting database. The createstatement method is declared and set to the statement object “st”, which would enable SQL statements to be sent to the database. The execute query method is then set to query the Voting database which would use the SELECT SQL statement to select the voters details from the Voters table. The results derived from this query is sent and stored in the Resultset object “rs”.

The execute query method returns a single Resultset object and is typically used with SELECT SQL statements. In order to read the results of the query, the next() method of the Resultset object rs would be utilized. A while loop would be used to read through the results, the loop would read the last piece of data returned in each record of the Voter’s table and would then print out the data on screen by the using the out. print function as shown in figure 8-9. A link is directed to the DeletedVoters JSP page, setting the string email as criteria for deletion voter details.

```
                    try {
                            Class.forName("com.mysql.jdbc.Driver").newInstance();      Connection
                            c = DriverManager.getConnection("jdbc:mysql:///Voting");  Statement
                            st = c.createStatement();
                            ResultSet rs = st.executeQuery("select * from Voters");
                            while (rs.next()) {
                              fName = rs.getString(1);
                              lName = rs.getString(2);
                              email = rs.getString(10);
                              street = rs.getString(5);
                              town = rs.getString(6);
                              postcode = rs.getString(7);
                              out.print("<tr><td>" + fName + "</td><td>" + lName + "</td><td>" +
email + "</td><td>" + street + "</td><td>" + town + "</td><td>" + postcode + "</td> ");
                            %>
                                    <td><a
href="DeletedVoters.jsp?email=<%=email%>">Delete</a></td>
                            <%
```

Figure 8-9: *The code above displays the methods and sqlstatements used to display the voters to be deleted*

The coding methods used in the deletevoters jsp page where adopted when developing the viewvoters jsp page, which was used to display voters details of the voters table.

DeletedVoters JSP page: page is used to delete voters from the database through the use of Python code embedded in script tags. Firstly the jsp page requests for the string email from the delete voter page. The JDBC driver is registered to the JDBC driver manager and a connection is made to the voting database. The execute update method is used to execute the DELETE SQL statement which would delete from the Voters table where email field would be the string email as shown in figure 8-10. The execute update method is typically used with the INSERT, UPDATE & DELETE SQL statements

```
<%
                try {
                        Class.forName("com.mysql.jdbc.Driver").newInstance();
                        Connection c =
DriverManager.getConnection("jdbc:mysql:///Voting");
                        Statement st = c.createStatement();
                  st.executeUpdate("delete from Voters where email like '" + email +
"'");
                } catch (Exception e) {}
                %>
```

Figure 8-10: *The code above displays the methods and sql statement used to delete voters from database*

Voting Results JSP page: was used to count and display the voting results to the administrator. The variables Vote1="" and count are declared as strings with null values. The JDBC driver is registered is registered and a connection is made to the database. The executequery method is used to select the vote1 record from the voters table and then count the vote1 record using the SQL COUNT statement, the COUNT statement will only count those records in which the table fields in the brackets is NOT NULL. The result of the query is stored in the Resultset object "rs1". The next() method is then used to read the results. A while loop is used to read the data returned in each record of the group Vote1 and displays the results using the out.print function as shown in figure 8-11. This format is used to display the results for all the elections candidates.

```
                try {
                        Class.forName("com.mysql.jdbc.Driver").newInstance();
                        Connection c = 
DriverManager.getConnection("jdbc:mysql:///Voting");
                        Statement st = c.createStatement();
                        ResultSet rs = st.executeQuery("select vote2, count(vote2) from 
voters group by vote2");
                        while (rs.next()) {
                          vote1 = rs.getString(1);
                          count = rs.getString(2);
                          out.print("<tr><td>" + vote1 + "</td><td>" + count + "</td>");
                        }
```

Figure 8-11: *The code above displays the method used to count votes cast by voter*

AllVotingResults JSP page: displays the voter's firstname and surname with the names of the candidates they voted for. This is a security measure, which would enable the administrator to view the voters' details and who they voted for. In the case of the system being investigated for voting malpractice, the system would be able to show if a voter voted more than once. The JSP uses the executequery method to select the voter's firstname, surname and voter's chosen candidates' details from the voters table, and prints to screen.

8.6 Voter Implementation

The login method used for the voter access is similar to the administrator access, Figure 8-12 shows the difference with the authentication used for the voter access. Login servlet class checks the voter to see if they have voted or not, if the voter has not voted and the voted field in the voters table is equal to "0", the voter is permitted to enter the voter menu page, if the voter has voted before and the voted field in the voters table has been flagged as "1", the voter will be blocked from voting and directed to the Not Allowed jsp page.

```
/           Method to check if the voter has not already voted
            public static String checkVoted(String userName) {
                        try {
                                    // Register JDBC/ODBC Driver in jdbc DriverManager
                                    Class.forName("com.mysql.jdbc.Driver").newInstance();      Connection
                                    c  =  DriverManager.getConnection("jdbc:mysql:///Voting");  Statement
                                    st = c.createStatement();
                                    ResultSet rs = st.executeQuery("select voted from voters where username
like '" + userName + "'");
                                    String Voted = "";
                                    while (rs.next()) {
                                                Voted = rs.getString(1);
                                    }
                                    return Voted;
                        } catch (Exception e) {
                                    e.printStackTrace();
                                    return "";
```

Figure 8-12: *The code above displays the method used to check if the voter has not already voted in the dataconnection class*

Voter Menu JSP page: displays the candidate name in a drop down box for the voter to select. An executequery method is used to select the name of the candidate who is under a certain party in the candidate table. The result is stored in the results set object "rs" it is then read by the next() method which prints out the result in a while loop. The voter would then be able to select an option from the drop down box. The option selected is then sent to the vote servlet for processing as shown in figure 8-13.

```
ResultSet rs = s.executeQuery("SELECT Name from Candidates where Party like
'President'");
                                    out.println("<BR><BR>");
                                    out.println("Student Union President:  <SELECT NAME=" +
"Vote1" + ">");
                                    while (rs.next()) {
                                                String val = rs.getString(1);
                                                out.println("<OPTION VALUE='" + val + "'>" + val +
"</OPTION>");
```

Figure 8-13*: The code above displays the method used to select candidates' names to be voted for in the votermenu jsp page.*

Voter Servlet: gets the http request information from the votermenu jsp page and stores the data as strings. The data is then stored in the VoterFormBean. Voter is directed to the confirmation jsp page through the use of the request dispatcher method.

Confirmation Vote JSP page: would have the VoterFormBean tag declared. The executeUpdate method would be used to set the voter's voted field record in the voters table to one, once the vote has been cast as shown in figure 8-14. This is a security measure which would prevent voters from voting more than once. Once the voter has confirmed their choice of candidates, the data in the voters table is updated to correspond to the new candidate information.

The voter is directed to the thankyou servlet. If the voter wants to change their choice of candidate, the voter can click the back button which would send a http request to the back vote servlet, the servlet in turn would direct the voter back to the votermenu jsp page.

```
// Once voter has confirmed vote, flag set to 1, so user not allowed to vote again
		try {
			Class.forName("com.mysql.jdbc.Driver").newInstance();
			Connection c = 
DriverManager.getConnection("jdbc:mysql:///Voting");
			Statement st = c.createStatement();
			st.executeUpdate("update voters set vote1 = '" + Vote.getVote1()
					+ "', vote2 = '" + Vote.getVote2() + "', vote3 = '" + 
Vote.getVote3()
					+ "', vote4 = '" + Vote.getVote4() + "', vote5 = '" + 
Vote.getVote5()
					+ "', vote6 = '" + Vote.getVote6() + "', voted = '1' 
where username = '" + Vote.getUserName() + "'");
		} catch (Exception e) {out.println(e);}
```

Figure 8-14: *The code above displays the method used to update the voter table with candidate's voted for.*

8.7 Encryption Class Implementation

The encryption class was used to encrypt passwords that where fed into the database table users and it was also used for decrypting passwords that where displayed to the user in the forgotten password JSP page. In order to implement the encryption and decryption processes for the voting system, the JCE API was used. The JCE makes use of specific classes to perform encryption and decryption functions. The main class for encryption is the Cipher class, which takes the role of a cryptographic cipher. A transformation is the process of encrypting and decrypting data. A transformation always includes the name of the cryptographic algorithm as shown in figure 8-15. The DES symmetric key encryption algorithm would be used for the encryption process.

```
// This class does the actual encryption
Cipher cipher = Cipher.getInstance("DES/ECB/PKCS5Padding");
```

Figure 8-15: Transformation

The getInstance method shown in figure 8-15 takes arguments for the transformation process. When the Cipher object is returned by the getInstance method, it must be initialised before it can be used to encrypt or decrypt the password string, in order to perform this function the secret key would be needed. Due to the symmetric nature of the DES encryption algorithm one secret key would be used to encrypt and decrypt the password.

In order to create a DES key, a Key Generator would have to be instantiated for the DES algorithm. The class SecureRandom which provides a cryptographically strong pseudo-random number generator would be used to create a number that would be initialised to the generator object. The generatekey method would be used to generate the secret key. The key would then be stored in a file called OnlineVoting.ser as shown in figure 8-16. This method would now return the key to any method that calls it.

```
KeyGenerator generator = KeyGenerator.getInstance("DES");
                              generator.init(new SecureRandom());
                              key = generator.generateKey();

                              ObjectOutputStream out = new ObjectOutputStream(new
FileOutputStream("OnlineVoting.ser"));
```

Figure 8-16: Secret key generator

Upon generating a secret key, the cipher object would be initialised using the key from the get key method and set to either ENCRYPT _MODE for encryption or DECRYPT_MODE for decryption.

```
      // Initialise it using key got from the method below.
            cipher.init(Cipher.ENCRYPT_MODE,getKey());
```

Figure 8-17: Cipher object Initialised

8.8 Summary

This chapter has covered the implementation and methods used to develop the online voting system. The codes used to perform different function on the system where explained. The configuration process used to configure the tomcat server to perform SSL connections was also explained.

9 Testing

In order to ensure that the system works perfectly, it has to be rigorously tested. The testing procedure would be used to check all the features developed for the online voting system work efficiently, the test procedure would also be used to identify any hidden errors or deficiencies the system may possess.

In order to conduct an efficient testing process on the system, a suitable testing procedure has to be utilised. In choosing an appropriate testing strategy to use, some considerations have to be reviewed in terms of the size and complexity of the system to be tested.

9.1 Test Strategies

There is a number of testing strategies that can be utilised to conduct adequate testing processes, the black box and white box testing methods are the most popular methods used to test software developed systems.

9.1.1 Black Box Testing

This testing strategy which is also known as functional testing is used by a tester who has no knowledge of the internal structure of the system. The tester does not test the programming code itself but instead performs the test based on previously understood requirements.

This form of testing is usually conducted by the end user, who would enter an input into the system and check for an expected output. The advantage of using black box testing is that the test can be done by the users of the system, without them needing to have prior knowledge of the system’s code. [36]

9.1.2 White Box Testing

This testing strategy which is also known as glass box or structural testing is used to test the internal logic and structure of the programming code used to develop the system. The tester would need to have unequivocal knowledge of the coding used for developing the system, in order to uncover any malfunctioning code. [35]

In order to test system adequately both testing strategies have to be utilised.

9.1.3 Test Plan

In order to efficiently test the full functional capability of the online voting system, a test plan has to be created. The test plan created would break the testing processes in order to tackle any malfunctioning feature of the online voting system.

The testing process would focus on testing the system's server, database server and web pages on different web browsers. This test has to be carried out to ensure that the system would be able to function on any web browser utilised by the system's users.

The testing process would focus on the system login authentication features; this is an integral part of the system, because it ensures security of the system is upheld again unauthorised access. A test would be carried out to check if the password being utilised are encrypted and decrypted.

The system's form validation would also have to be tested to ensure the error message to be presented to the user if the forms are not filled correctly is functioning appropriately.

The system database engines which connect the application to the database system have to be tested to ensure that information being retrieved from the users are populating the database system

9.2 Test Data

Test Ref No	Test Data	Expected Outcome	Final result
1	Connect to server	The Client should be able to Connect to server	Pass
2	Connect to mysql database	The Client should be able connect to data base	Pass
3	Test internet explorer browser compatibility	When user enters the online voting url welcome page should be displayed	Pass
4	Test Netscape browser compatibility	When user enters the online voting url welcome page should be displayed	Pass
5	Test SSL connection from web browser	Using the secure local host port number 8443, the user should be able to enter the website over a secure connection	Pass
6	Web Page Navigation	Webpage navigation links to should open specified web page	Pass
7	Login validation	Error message should be displayed when inappropriate data is entered	Pass

8	Login process to distinguish voter and administrator	Voter should not be allowed to login into admin page, admin should not be allowed to login into voter page	Pass
9	Attempt to guess password more than three time during login	System user should be blocked from accessing the system on third attempt	Pass
10	Voter view and select candidate and submit vote	The voters choice of candidates should be displayed on confirmation page	Pass
11	Voter casts votes	The voters table in voting database should be updated with new votes	Pass
12	Login Block for voter	Voter who has voted once should be flagged and blocked from voting again	Pass
13	Voting results page	The votes counted should be updated when new vote is cast	Pass
14	Add voter, candidate and administrators validation	Error message should be generated if necessary boxes are not filled in and if username chosen is already taken	Pass

15	JDBC connection to database	Data from registration form should be entered into database	Pass
16	Password encryption	Password entered into database should be encrypted	Pass
17	Administrator should be able to view voters, candidate & admin details from database	Data from database should be printed on screen	Pass
18	Administrator should be able to delete voter, candidate and administrator detail	Details of voter, candidate & administrator should be deleted from database	Pass
19	Password Decryption	Forgotten password request by user should be decrypted before being sent to user screen	Pass
20	Logoff	User should be able to log off successfully from system	Pass

9.3 Summary

The testing phase of the project was the final stage of the system development process. The system was rigorously tested to find out if the there where any system flaws or bugs within the system. The testing phase is highly essential in order to produce an efficient system and the limitations of the system can also be revealed from the testing process to be improved in the future.

10 Conclusion

This chapter will discuss the development of the entire system as a whole. It will give an insight into the general procedures that where taken to accomplish the project. It will also discuss the aims and objectives of the initial proposal that where and the objectives that could not be accomplished. It will cover the drawbacks the project possesses and the necessary work that can be used to enhance the system in the future.

The main project objective was to build a secure online voting system, which would be used. The aim of the project was to convert the current use of paper based voting to an electronic form of voting, which would enable voters to vote remotely from any location through the use of the internet.

Research was carried out on the different forms of online voting systems that currently exist, noting their features, and how to influence the participation of voters to an election. Various forms of server side technologies where investigated in order to choose the right programming language to use for the development of the online voting system.
Security issues that may affect the integrity of the online voting system where addressed and counter measures on how to project the system's security where researched. A number of software development methodologies where reviewed, upon careful consideration, the waterfall methodology was chosen as the most appropriate development method to use for this particular project.

During the design and development of the system, the main effort was focused on designing and developing the system to achieve a solution based on the concepts of the system proposal. This phase provided a clear description of how the system was to be created. The main emphasis was on creating an intuitive user interface for retrieving

information, querying the database by the use of Python classes and scriplets and ensuring security was of top priority.
The testing phase of the project was used to rigorously exercise the system to expose any deficiencies and short comings which the system may have possessed. The results of the test showed if they system was ready to be delivered to its end users.

The system created met its objectives, by being simple to use and secure, which was important due to the fact that it would be used for the student union electoral process.

10.1 Future Work

A lot of work could be done to enhance the security features of the present system. The system at the moment permits voters to choose their own passwords when they are being registered by the administrator, it would be more secure to develop a password generator facility which would create a unique password for each voter at random. The passwords would then be emailed to each voter through the use of the email address provided.
The system could also be enhanced by displaying the voting result through the use of 3D graphs, which would help the administrator and elections analysts in reviewing the voting results. Due to time constraints these ideas where not brought to light in the project.

REFERENCES

1. Jayson Falkner, Ben Galbraith, Romin Irani, Casey Kochmer, Sathya Narayana Panduranga, Krishnaraj Perrumal, John Timney, Meeraj Moidoo Kunnumpurath, (2001), Beginning JSP Web Development,Wrox.
2. Peter denHaan, Lance Lavandowska, Sathya Narayana Panduranga, Krishnarag Perrumal, (2004), Beginnign JSP 2 From Novice to Professional, Apress.
3. Aneesha Bakharia, (2001),PythonServerPages,Prima Tech.
4. Bruce W.Perry,(2004), Python Servlet & JSP Cookbook, O'Reilly
5. Simson Garfinkel, Gene Spafford,(1997), Web Security & Commerce, O'Reilly.
6. Time Stamp.
   URL: http://whatis.techtarget.com/definition/0,,sid9_gci817089,00.html
7. Maydene Fisher, Jon Ellis, Jonathan Bruce (2003), JDBC API Tutorial and Reference . Third Edition, Sun Microsystems.
8. George Reese, (2000), Database Programming with JDBC and Python. O'Reilly.
9. Laura A.Chappell, Ed Tittel (2004), Guide to TCP/IP. Thomson.
10. Transmission Control Protocol
    URL: http://en.wikipedia.org/wiki/Transmission_Control_Protocol
11. Andrew S.Tanenbaum, (1996), Computer Networks. Third Edition. Prentice Hall
12. Mark Andrews: Story of a Servlet
    URL: http://Python.sun.com/products/servlet/articles/tutorial/
13. Cisco Systems Inc.(2002): Introduction to TCP/IP
    URL:http://www.cisco.com/univercd/cc/td/doc/product/iaabu/centri4/user/scf4ap1.htm#xtocid6
14. URL:http://www.jguru.se/jguru/Channel_Html/generic/images/developers/servlet_lifecycle.gif
15. Introduction What is JDBC
    URL: http://Python.sun.com/docs/books/jdbc/intro.html
16. Bruce Schneier: Analysis of SSL 3.0 Protocol
    URL: http://www.schneier.com/paper-ssl.pdf
17. URL: http://www.Homomorphicsecurity.com/Homomorphiclabs/node.asp?id=2293

18. SSL Protocol
URL: http://www.cryptoheaven.com/Security/Presentation/SSL-protocol.htm
19. Allen (2004): Access vs MySQL
URL:http://codewalkers.com/tutorialpdfs/tutorial79.pdf
20. URL:http://www.msaccess.databasecorner.com/
21. URL:http://searchopensource.techtarget.com/sDefinition/0,290660,sid39_gci516819,00.html
22. URL: http://www.credata.com/research/methodology.html
23. Simon Bennett, Steve McRobb, Ray Farmer, (1996), Object-Oriented System Analysis and Design Using UML
24. URL: http://www.geotrust.com/resources/white_papers/pdfs/QuickSSLWP.pdf
25. URL: http://en.wikipedia.org/wiki/Apache_Tomcat
26. URL:http://expertanswercenter.techtarget.com/eac/knowledgebaseAnswer/0,295199,sid63_gci984561,00.html
27. URL:http://searchwebservices.techtarget.com/sDefinition/0,290660,sid26_gci868204,00.html
28. URL: http://www.answers.com/topic/cryptography?method=22
29. William R.Cheswick , Steven M. Bellovin, Aviel D. Rubin, (2003), Firewalls and Internet Security. 2nd Edition, Addison-Wesley.
30. URL: http://Python.sun.com/j2se/1.3/docs/guide/jdbc/getstart/intro.html#1004029
31. URL: http://www.answers.com/HCI
32. http://uml.tutorials.trireme.com/
33. Leszeka A. Maciaszek, Bruc Lee Liong, (2005), Practical Software Engineering. Addison Wesley.
34. URL: http://www.webopedia.com/TERM/W/White_Box_Testing.html
35. URL:http://www.csc.calpoly.edu/~dbutler/tutorials/winter96/coverage/blackbox.html
36. Tomcat Security Overview and Analysis
URL:http://www.cafesoft.com/products/cams/tomcat-security.html
37. URL: http://www.norman.com/Product/WhitePapers/wp_encryption.pdf/en

38. Niels Ferguson, Bruce Schneier, (2003), Practical Cryptography. Wiley Publishing Inc.

39. Michael Bray: (1997) Object Oriented Design.
URL: http://www.sei.cmu.edu/str/descriptions/oodesign.html

40. URL: http://www.Homomorphicsecurity.com/Homomorphiclabs/node.asp?id=2214

41. URL: http://www.answers.com/topic/xml?method=22

42. Jose Annunziato, Stephanie Fesler Kaminaris, (2001), SAMS Teach Yourself PythonServer Pages. SAMS.

43. URL: http://edocs.bea.com/wls/docs61/webapp/web_xml.html#1016445

44. Art Taylor, Brian Buege, Randy Layman, (2002), Hacking J2EE& Python Exposed. McGraw-Hill/Osborne.