UNIVERSITI
TEKNOLOGI
PETRONAS

Implementation of E-Voting System: Case Study for Universiti Teknologi PETRONAS

By

Mohd Hadzwan Bin Mohd Hamdan

Dissertation submitted in partial fulfilment of
the requirements for the
Bachelor of Technology (Hons)
(Business Information Systems)

JANUARY 2008

Universiti Teknologi PETRONAS
Bandar Sri Iskandar
31750 Tronoh
Perak Darul Ridzuan

CERTIFICATION OF ORIGINALITY

This is to certify that I am responsible for the work submitted in this project, that the original work is my own except as specified in the references and acknowledgements, and that the original work contained herein have not been undertaken or done by unspecified sources or persons.

MOHD HADZWAN BIN MOHD HAMDAN

CERTIFICATION OF APPROVAL

Implementation of E-Voting System: Case Study for
Universiti Teknologi PETRONAS

By

Mohd Hadzwan Bin Mohd Hamdan

A project dissertation submitted to the
Business Information Systems Programme
Universiti Teknologi PETRONAS
in partial fulfilment of the requirement for the
Bachelor of Technology (Hons)
(Business Information Systems)

Approved by,

____

(Dr. Mohd Fadzil Bin Hassan)

UNIVERSITI TEKNOLOGI PETRONAS

TRONOH, PERAK

January 2008

ABSTRACT

E-Voting application is an electronic approach in dealing with overall aspect of election or referendums, be the way the votes are cast or the votes being calculated. This taking into account issues such as the security, practicality, suitability, and the economic-benefit ratio on the needs in implementing it. For Malaysia, an E-Voting application in a governmental level or national level elections were never been held. Thus an eye opener of the possibility of having an E-Voting election should be studied and started to be developed in aspiration to achieve a K-Society by 2020.

MPPUTP Election has long received cold voters turnout whenever the election is held and thus a proposed E-Voting system is produced as a way to eliminate the problems facing. Also with this system, a better way of relaying information regarding the election is better handled by the management. Not only this, a more credible and trusted election could be held, which in a way can uplift Universiti Teknologi PETRONAS's reputation especially in becoming a paperless university or E-University.

ACKNOWLEDGEMENTS

I would like to convey my gratefulness to the Almighty, for His permission has enabled me to complete this 2 semesters project. My thanks also go to my parent and family for their support. To my supervisor who has been with me for this 2 semesters, my special thanks and credit goes to him, for his patience and guidance has brought me to this level. Without his kind consent and schedule-lenient on me, I might had hard time on the progress of my project, as I encountered cramped time during the last 3 months of the semester because of the conflicting schedules with other commitments. I also would like to thank all my friends back in UTP who gave some of their assistance and ideas especially during the system's development part, whereby they have helped me on some of the difficult technical part. Last but not least, I want to thank the FYP Committee, all the external supervisors, and also to the Engineering Design Exhibition officials. May the future brightly lit for all of us.

TABLE OF CONTENTS

LIST OF FIGURES

Chapter 1

INTRODUCTION

1.1 Background of study

E-voting has been around since 1960s when punch card system debuted. Although this is still regarded as part of e-voting, the real e-voting application has not been acknowledged until the coming of advanced computers. Nowadays, e-voting application has been applied in many lives of people worldwide. They are using e-voting technology and application to select their company's new chief officer, board of directors, council mayor and even to the level of state and national election.

In Malaysia, the application of e-voting has not been widely used though it might be some done in private organization or corporate departments. These types of e-voting are not significant enough to be called national-level application of e-voting. As Malaysia is going forward in its MSC ambition and knowledge based society (K-Society), the application of e-voting could not be left out and should be studied further as per implications and national readiness on its acceptance of e-voting in elections. In this project, the study is about the possibility of the ordination of e-voting in the level of general election in Malaysia. However, the study touched on this is merely on surface part as a very thorough and more complex and challenging issues are have to be studied to cover the overall aspect.

In the niche on this, a case study about UTP Student Representative Elective will be done with the possible implementation of e-voting with the system provided together in this study.

With accordance to the Malaysia University and University Colleges Act, an establishment of higher learning institution has to form a council, which should be the platform for students to conduct their activities, relating matters pertaining to the students' problems and also serves as a communication tool between the university's administration and the students. Majlis Perwakilan Pelajar or simply known as MPP is the ultimate legislative body among the students The MPP holds the highest administrative authority in the Student Union of each university. A general election is held every year, usually in September each year, to elect representatives to the Majlis Perwakilan Pelajar. The size of the MPP differs from each university, from as little as 12 people to as many as 44 people.

As an obedient gesture to this act, UTP has not been excluded in having its own MPP. However, the environment and scenario of MPPUTP is differs from the rest and majority of universities all around Malaysia. As a young and maturing university, UTP has been nurturing its students to be more aware of the present of MPP in the campus by conducting election each year. The election is usually been held on the 4th quarter of the year, between September to November depending on the current situation. Based on history, UTP has conducted 5 elections since its establishment as a private university.

MPPUTP Election is not held and contested the same way as the other public universities do. The election is open to General Constituency and Program Constituency. The General Constituency is open for any students who wish to be contested in this. The General Constituency is elected by the whole of UTP students and Program Constituency can only be elected by students within the same program.

General constituency is the one who will be elected as the President, Vice President, Secretary 1, Secretary 2 and the Treasurer of the council. Meanwhile, the Program Constituency is open to be contested from students, representing his/her own program. According to UTP Student Council Act, a program is entitled to have only 2 representatives in the MPP elected. These 2 representatives from each program will be elected as Executive Committee or Exco in the council, holding many Exco portfolios such as Communication, Welfare, Sports & Recreation and many others. All UTP students have their rights to cast vote and elect any candidates on their preference without any prejudice or influence from any party.

1.2 Objective

Studying and researching the e-voting concept as a whole, its implementation in Malaysia and building an e-voting system for MPPUTP Election, as a case study. For Malaysia context, this pre-surface study is to aware that the e-voting application is somehow quite possible to be implemented in Malaysia up to the general election level.

Meanwhile, for UTP context, the objective is to increase general awareness and students' participation in the election. It is also hope to create an environment where the campus society is committed and interested whenever the MPPUTP Election is coming.

1.3 Problem Statement

E-voting in Malaysia's environment in still regarded as young and new. To date, there has never been any official election of registered organization and political parties been done in using e-voting technology. This project will study and doing research on the conception of e-voting in Malaysia, for it to be implemented if deems suitable. E-voting systems can be regarded as one of components in implementing the knowledge-based society and further driven the MSC ambition.

Going on to UTP context, the problem is identified as low voting turnout occurred every year. This is due to lacks of information about the election and less of interest among students. The main reason identified for this is students do not have time to participate in the voting day and also avoiding oneself getting hassle to involve in the voting process.

1.4 Significant of project

Many significant effects are identified through the study of this project. The most beneficial factors of this project spot on UTP are probably gained:-

a) increasing the percentage of voting turnout
b) getting more participants and involvements of UTP students in the election
c) increasing awareness in the campus about the coming election
d) better way for candidates to deliver the messages and manifestos
e) students will get more informed about the candidates and the election as a whole
f) more credible and trusted handling of votes
g) establishing UTP image as paperless university/ E-University

Chapter 2

LITERATURE REVIEW

As former US President Clinton used to said, “We would like to take advantage of information technology to enhance the quality of life of our citizens”, this supports that the advancement and technology of IT could really benefits the peoples. As this project goes, we will try to study on e-voting architecture and implementation and also follow our case study on UTP.

Electronic voting technology can speed the counting of ballots and can provide improved accessibility for disabled voters. On history, electronic voting systems for electorates have been in use since the 1960s when punch card systems debuted. The newer optical scan voting systems allow a computer to count a voter's mark on a ballot. Direct Recording Electronic (DRE) voting machines which collect and tabulate votes in a single machine are used by all voters in all elections in Brazil, and also on a large scale in India, the Netherlands, Venezuela, and the United States. Internet voting systems have gained popularity and have been used for government elections and referendums in the United Kingdom, Estonia and Switzerland as well as municipal elections in Canada and party primary elections in the United States and France. In all, e-voting can be categorized into 3 segments, which are;

Paper-based electronic voting system:

Sometimes called a "document ballot voting system,", paper-based voting systems originated as a system where votes are cast and counted by hand, using paper ballots. With the advent of electronic tabulation came systems where paper cards or sheets could be marked by hand, but counted electronically. These systems included punch card voting, marksense and digital pen voting systems.

Most recently, these systems can include an Electronic Ballot Marker (EBM), which allows voters to make their selections using an electronic input device, usually a touch screen system similar to a DRE. Systems including a ballot marking device can incorporate different forms of assistive technology.

Direct-recording electronic (DRE) voting system:

A direct-recording electronic (DRE) voting system records votes by means of a ballot display provided with mechanical or electro-optical components like a touchscreen that can be activated by the voter; that processes data by means of a computer program, which records voting data and ballot images in memory components. It produces a tabulation of the voting data stored in a removable memory component and as printed copy. The system may also provide a means for transmitting individual ballots or vote totals to a central location, for consolidating and reporting results from precincts/areas at the central location.

These systems use a precinct count method that tabulates ballots at the polling place. They typically tabulate ballots as they are cast and print the results after the close of polling.

Public network DRE voting system (Internet Voting):

A public network DRE voting system is an election system that uses electronic ballots and transmits vote data from the polling place to another location over a public network. Vote data may be transmitted as individual ballots as they are cast, periodically as batches of ballots throughout the election day, or as one batch at the close of voting. This includes Internet voting as well as telephone voting.

Public network DRE voting system can utilize either precinct count or central count method. The central count method tabulates ballots from multiple precincts at a central location. Internet voting can use remote locations (voting from any Internet capable computer) or can use traditional polling locations with voting booths consisting of Internet connected voting systems. As our project progressed, we will emphasize on this segment of e-voting.

A PKI (public key infrastructure) enables users of a basically unsecured public network such as the Internet to securely and privately exchange data and money through the use of a public and a private cryptographic key pair that is obtained and shared through a trusted authority. The public key infrastructure provides for a digital certificate that can identify an individual or an organization and directory services that can store and, when necessary, revoke the certificates. Although the components of a PKI are generally understood, a number of different vendor approaches and services are emerging. Meanwhile, an Internet standard for PKI is being worked on.

The public key infrastructure assumes the use of public key cryptography, which is the most common method on the Internet for authenticating a message sender or encrypting a message. Traditional cryptography has usually involved the creation and sharing of a secret key for the encryption and decryption of messages. This secret or private key system has the significant flaw that if the key is discovered or intercepted by someone else, messages can easily be decrypted. For this reason, public key cryptography and the public key infrastructure is the preferred approach on the Internet. The private key system is sometimes known as symmetric cryptography and the public key system as asymmetric cryptography. A public key infrastructure consists of:

a) A certificate authority (CA) that issues and verifies digital certificate.
b) A certificate includes the public key or information about the public key
c) A registration authority (RA) that acts as the verifier for the certificate authority before a digital certificate is issued to a requestor
d) One or more directories where the certificates (with their public keys) are held
e) A certificate management system

Action	Origin of Key	Type of Key
Sending an encrypted message	Receiver	Public Key
Send an encrypted signature	Sender	Private Key
Decrypt an encrypted message	Receiver	Private Key
Decrypt an encrypted signature	Sender	Public Key

At the moment, MyKad PKI application can support for 2 digital certificates to be inserted in the card. MyKad holders can apply and purchase the digital certificates from 2 of Malaysia's certification authority, MSCTrustgate.com Sdn. Bhd. and DigiCert Sdn. Bhd. PKI allows for easy securing of private data over public telecommunications networks, thus allowing, secure electronic transactions over the Internet.

The E-Voting presents numerous advantages over traditional paper-based voting which has been identified in speed and accuracy in the vote counting process, accessibility for blind and visually impaired voters, flexibility in the design and modification of the ballots, prevention of involuntary voting errors (e.g., "over-voting" and "under-voting" errors), ease-of-use for voters, support of multiple languages and also in the case of Internet voting, there is the additional advantage of voters' mobility and convenience which generally leads to higher turnout rates.

An MD5-based encryption scheme on both client and server machines are to allow encrypted password protection for web-based application. Although there are many free tools for password protection, only a few uses MD5 on the server-side, but the password still travels over the internet as plain text. All server-side only schemes (like .htaccess password protection) are completely open to packet-sniffing. With this scheme, the browser JavaScript encrypts the password on the client's machine, and session tracking allows only one response per session ID, making simple packet-sniffing and session replaying much more difficult. This is a one-way encryption scheme where the password is never transmitted or stored as clear text on the client or server, and thus cannot be recovered. It uses cookies to maintain the user session.

It's common to store username and password combinations in a database table for application-level security. This is a good practice because it avoids giving the actual database username and password combinations, which someone could use to access the tables and application code directly. There is still a slight risk that someone who gains database access can see the username/password table and be able to obtain all application passwords. For this reason, it's a good idea to obscure the passwords when they're stored in the database. However, even encrypted passwords aren't 100 percent safe. Encryption implies that, if someone has a valid key encryption, they would be able to decrypt the passwords and get the original text necessary to gain access to the database.

A solution to this problem is to store a checksum or hash key for a username/password combination. A checksum takes the individual bytes of some text and computes a numeric value that is highly unlikely to reproduce. This is the way that UNIX and many other systems check username/password values. MD5 is a fairly common checksum calculation on arbitrary text, which produces a 128-bit or 16-byte value. While the MD5 algorithm is well documented and freely available, it's not possible to figure out the original text used to generate the MD5. It also takes a long time, computationally, to create and try every possible MD5 value.

HTTPS is the Hyper-Text Transfer Protocol with SSL Encryption. It is the most popular network protocol for establishing secure connections for exchanging documents on the World-Wide Web. It is basically HTTP carried over a TCP socket, which has been secured using SSL. It is an extension to the HTTP protocol to support sending data securely over the World Wide Web. However, not all Web browsers and servers support HTTPS.

HTTPS is a secure way of using HTTP where the former provides almost no security features. HTTP contains only basic authentication mechanisms, and no support for privacy. HTTPS solves this problem by replacing HTTP's transport layer, the insecure TCP, with SSL, a secure transport layer. In the near future, SSL will probably be replaced by the more general TLS protocol, but it is very unlikely that the already established name of HTTPS will be changed to reflect this change.

Another technology for transmitting secure communications over the World Wide Web is Secure Sockets Layer (SSL). However, SSL and HTTPS have very different designs and goals so it is possible to use the two protocols together. Whereas SSL is designed to establish a secure connection between two computers, HTTPS is designed to send individual messages securely. SSL is a protocol developed by Netscape for transmitting private documents via the Internet. SSL uses a cryptographic system that uses two keys to encrypt data – a public key known to everyone and a private or secret key known only to the recipient of the message. Both Netscape Navigator and Internet Explorer support SSL and many Web sites use the protocol to obtain confidential user information, such as credit card numbers. By convention, URLs that require an SSL connection start with https: instead of http:.

SSL and HTTPS therefore can be seen as complementary rather than competing technologies. Both protocols have been approved by the Internet Engineering Task Force (IETF) as a standard.

Chapter 3
METHODOLOGY

3.1 Research Methodology

Since e-voting in Malaysia is new, we will study the most effective and feasible way for it to be implemented. The project will be consisting of research in e-voting, the security measures and also best way of solution for Malaysian scenario.

The study of electronic voting feasibility, practicality, usability and integrality will be done thoroughly, to accommodate to current situation and environment of Malaysia, and UTP specifically. This project will study the effectiveness of e-voting if it could be implemented in Malaysian voting scenario. This could be seen in election for district committee seat, local authority election, municipal election or even parliamentary or state seat election.

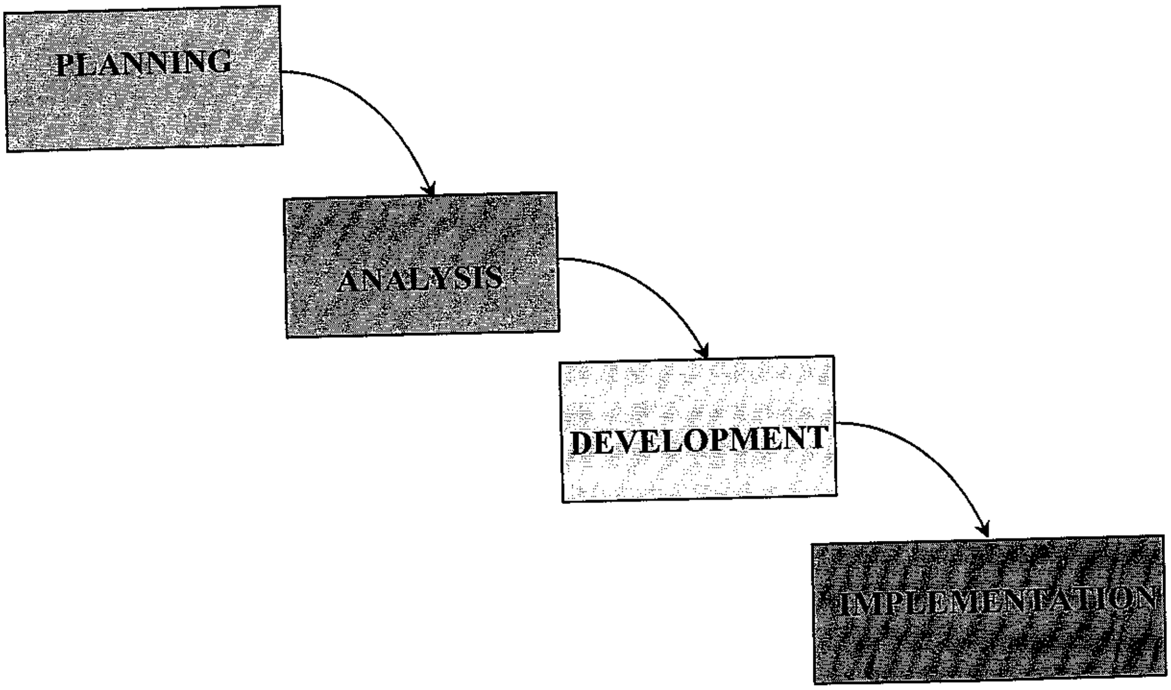
The security and integrity of e-voting system will also be covered in the study of this e-voting system. Whereas in this modern world, such a high security measures should be taken note to counter affect any unintended forgery in the e-voting system.

Last but not least, this system will be tested its functionality in the context of UTP. MPPUTP Election will be the testing ground, where we can see the implementation of this system as a whole.

3.2 Project Methodology

For UTP context as been explained before, the system development life cycle (SDLC) chosen is the Waterfall model. The waterfall model is a popular version of the system development life cycle model for software engineering. Often considered the classic approach to the systems development life cycle, the waterfall model describes a development method that is linear and sequential. Waterfall development has distinct goals for each phase of development. Each has its own stage which known as Planning, Analysis, Development and Implementation. These 4 steps are widely known as PADI.

The advantage of waterfall development is that it allows for departmentalization and managerial control. A schedule can be set with deadlines for each stage of development and a product can proceed through the development process like a car in a carwash, and theoretically, be delivered on time. Development moves from concept, through design, implementation, testing, installation, troubleshooting, and ends up at operation and maintenance. Each phase of development proceeds in strict order, without any overlapping or iterative steps.

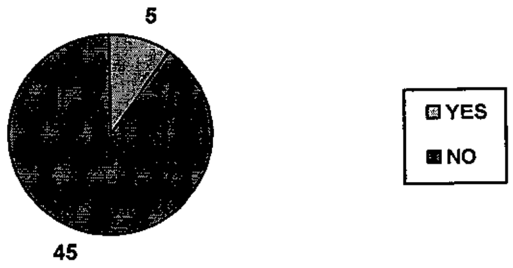


3.2.1 Planning Phase

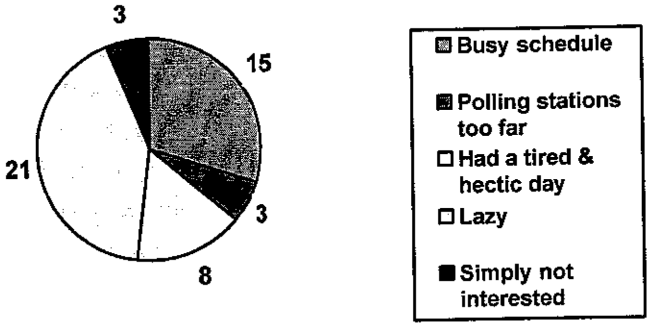
In this initial phase of the system, we try to look into the needs, requirements and the problem objective itself. As the project is proposing on building a system for e-voting to be implemented in MPPUTP election, a thorough planning of the system is being done. Questions like the security, deliverability, compatibility, practicality is being taken into consideration.

During this phase, a simple questionnaire to 50 random students was conducted at various locations around UTP. The questionnaire is basically asking queries on certain issues such as how many times they vote for MPPUTP Election and also taking into their opinion if the MPPUTP Election could be done from the room. A result of the questionnaire is like this:

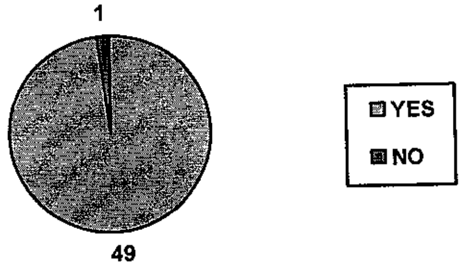
1. Have you been participated in casting vote in the past MPPUTP Election before?



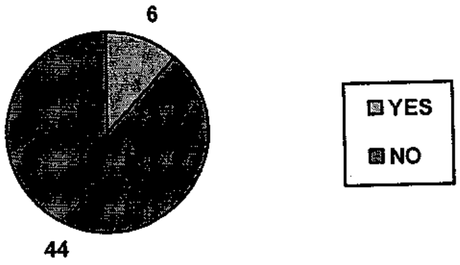
2. What are the reasons you did not participated in casting the vote?



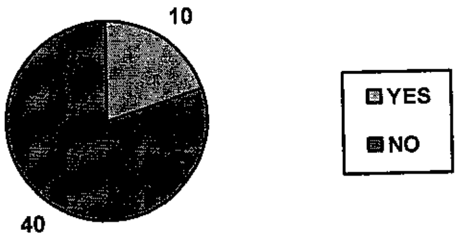
3. If there is possibility of casting the vote from the comfortable of your room, would you be able to cast vote?



4. Are you getting enough information regarding the contested candidates' info, i.e. personal particular, manifesto, prior to an election?

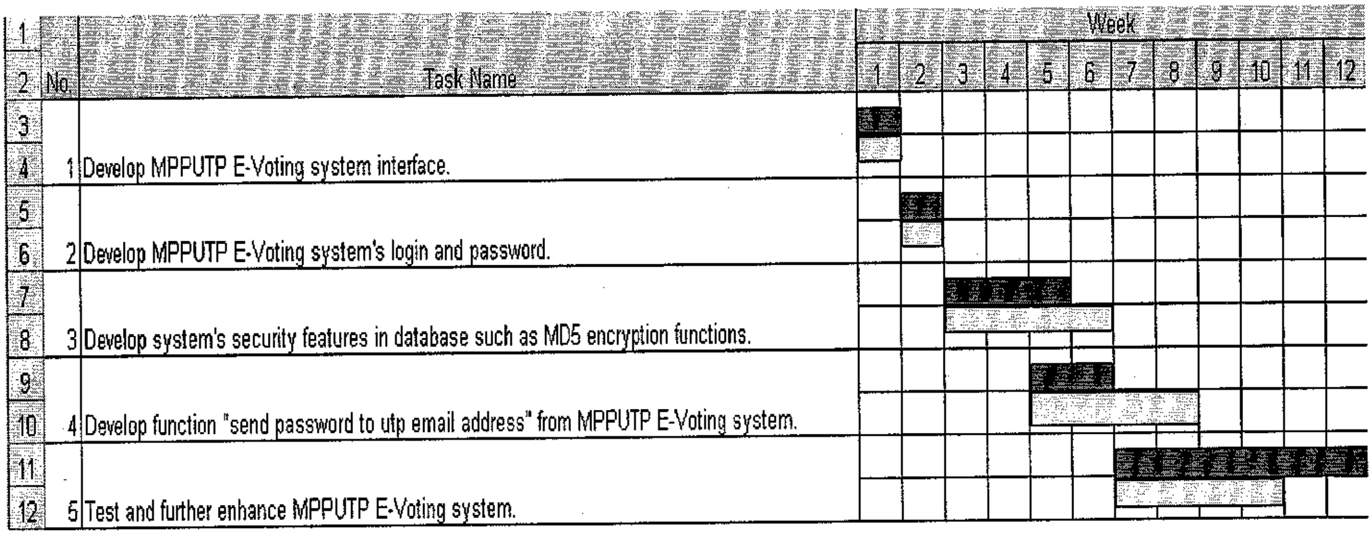


5. Do you personally think the elected MPPUTP High Committee and Exco officials represented the majority choice of the students?



A Gantt chart is used as a guideline to any progress made during the development of the system. Since this project choose waterfall model as its development life cycle, it is really necessary to have a Gantt chart as a lookup point and benchmarking of any progress made, since waterfall model does not permits rephrasing back on steps undergone.

In this Gantt chart displayed here, it shown the progress made in the last semester where the real development of the system began. The Red color shows the targeted achievement period, while the Yellow color represents the actual achievement of those planned tasks.



1			Week											
2	No.	Task Name	1	2	3	4	5	6	7	8	9	10	11	12
3			🟥											
4	1	Develop MPPUTP E-Voting system interface.	🟨											
5				🟥										
6	2	Develop MPPUTP E-Voting system's login and password.		🟨										
7					🟥	🟥	🟥							
8	3	Develop system's security features in database such as MD5 encryption functions.			🟨	🟨	🟨	🟨						
9							🟥	🟥						
10	4	Develop function "send password to utp email address" from MPPUTP E-Voting system.					🟨	🟨	🟨					
11									🟥	🟥	🟥	🟥	🟥	🟥
12	5	Test and further enhance MPPUTP E-Voting system.							🟨	🟨	🟨	🟨		

Figure 3.1: Gantt Chart

3.2.2 Analysis Phase

On analysis phase, the analysis done is on how will the system will work and whether it can be implemented in this system.

Functionality such as password confidentiality together with MD5 capability is being studied. Through MD5 implementation, a hash-based authentication methods work via a challenge-response mechanism. The server sends a random challenge. The client combines the random challenge with the password, and computes a one-way hash. The client sends the hash to the server, which performs the same computation. If the client's supplied hash matches the servers computed hash, the authentication succeeds. The overflow of the MD5 implementation is this project would be similar like this;

1) The administrator/client adds a user name and password to the user database on the server. The name/password is saved as an MD5 encrypted hash. The theory behind MD5 is that it would be very difficult to determine the originating strings for any given hash. The hash is a unique signature, but doesn't reveal the original password.

2) The remote user accesses the main program via their browser.

3) The server-side request for the login screen will create a new session ID value and add it to the session database, also storing the time of the request.

4) When the remote user submits a name/password, the client-side JavaScript then:
    a) MD5 encrypts their user name and password.
    b) MD5 encrypts the user/password hash with the session ID value.
    c) Returns the session ID and the encrypted user/password/session ID hash to the server.

5) The server authenticates the user if:

   a) The session ID returned is a valid open session and

   b) The session ID was requested less than 30 seconds ago and

   c) The user/password hash stored on the server, hashed with the session ID, matches the response from the remote client.

   (Note that the response hash is unique because it combines the user/password hash (which is constant) and the session ID string (which is always different). Only one response is allowed for each session ID, so replaying the response hash to gain authentication doesn't work)

6) If the authentication fails, a failure message is returned to the remote client browser.

7) If the authentication is successful, the HTTP header will pass a cookie to the remote client browser, allowing them access which is by default. Have to remind that because of this, the set cookie string could be theoretically stolen by packet sniffing and used as a bypass to the authentication process, although there is now the additional hurdle of determining the IP address of the client. A user can have a different IP address for different sessions, but once authorized at a certain IP address, the validity of that session cookie is tied to that address.

3.2.3 Design Phase

The design of this system will be done according on research and study done in the planning and analysis phases. On this phase, this system is designed on these requirements which are collected out during the planning and analysis phases;

1) Completeness : All valid votes are counted correctly, so no more spoilt votes

2) Robustness : Dishonest voters, other participants or outsiders can not disturb of disrupt an election

3) Privacy : The votes are cast anonymously

4) Unreusability: Every voter can vote only once

5) Eligibility : Only legitimate voters can vote

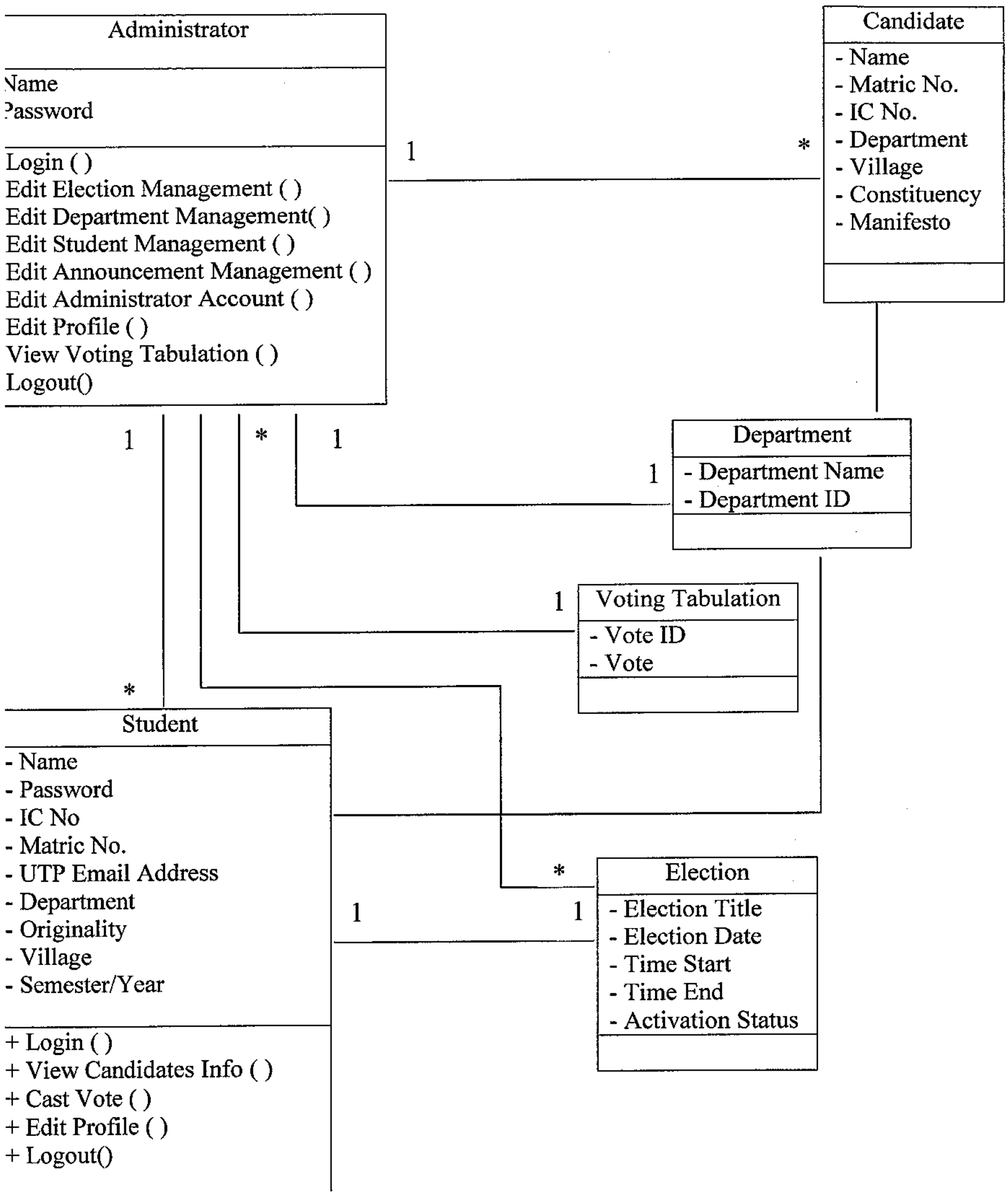
6) Fairness : A voter casts his vote independently and is not influenced

7) Universal Verifiability: Anyone can verify a correctness of election.

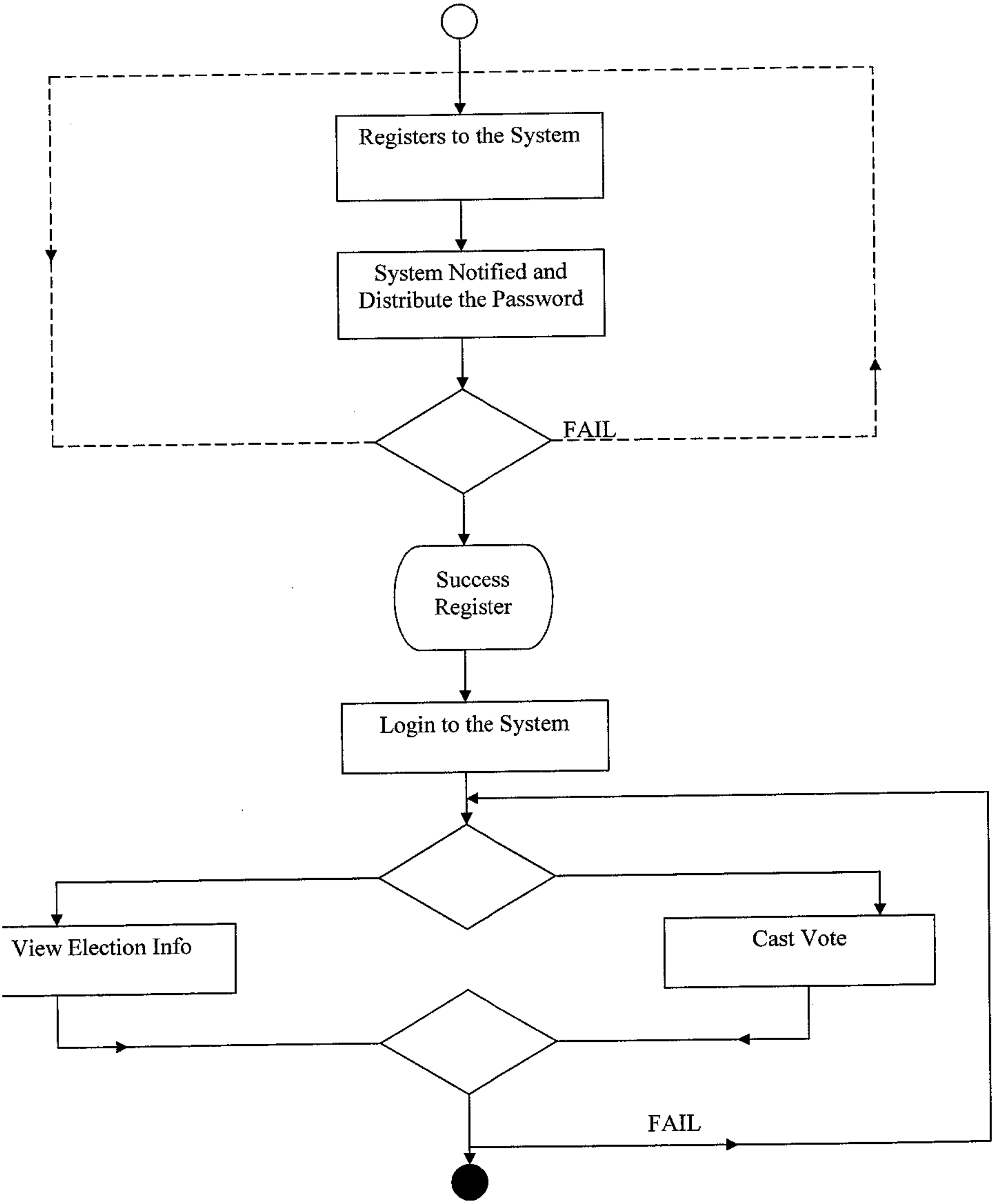
8) Receipt-freeness: A voter can not prove to a coercer, how he has voted

The design of this system will be done according on research and study done in the planning and analysis phases. On this phase, this system is designed on these requirements which are collected out during the planning and analysis phases;

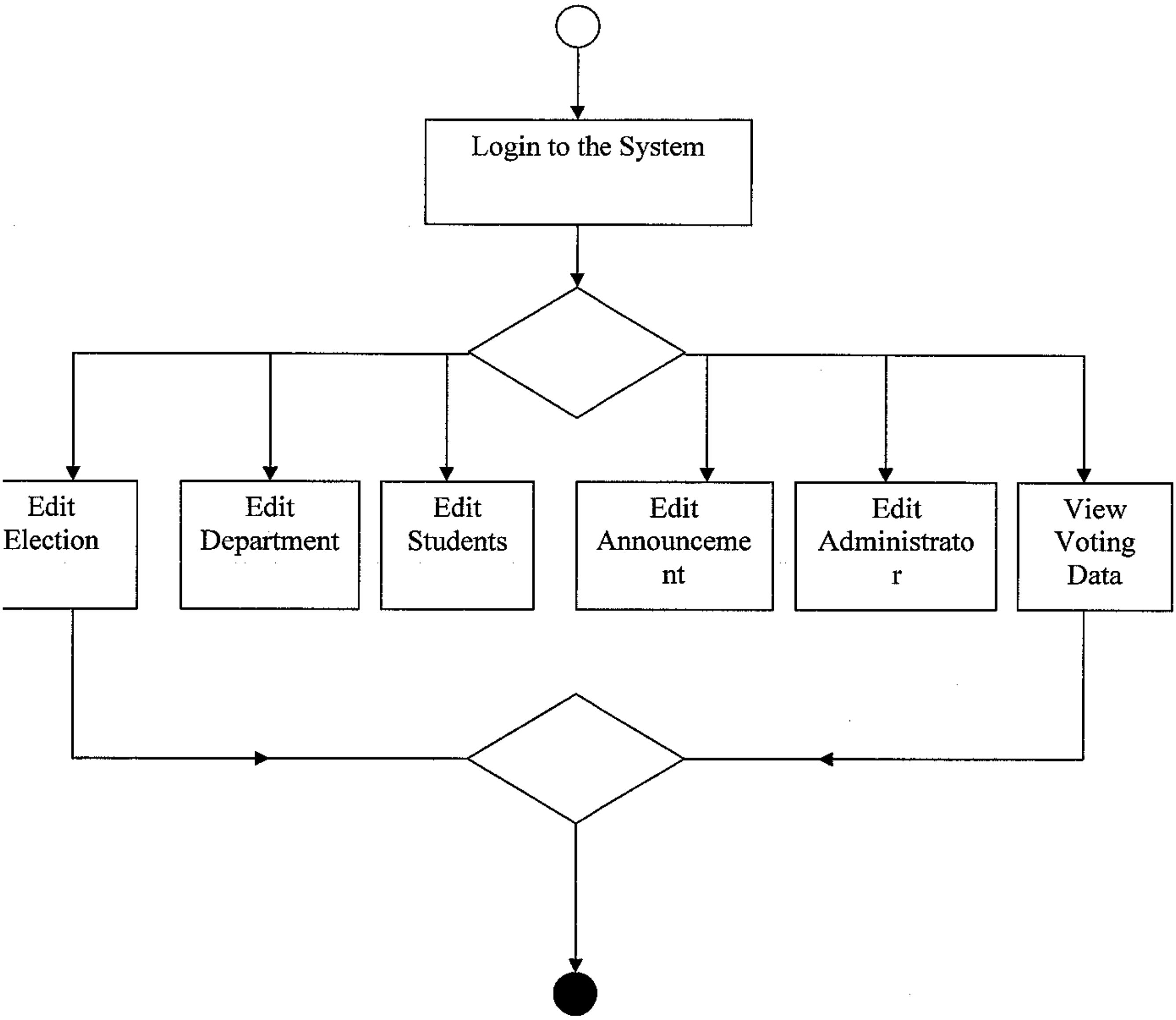
CLASS DIAGRAM



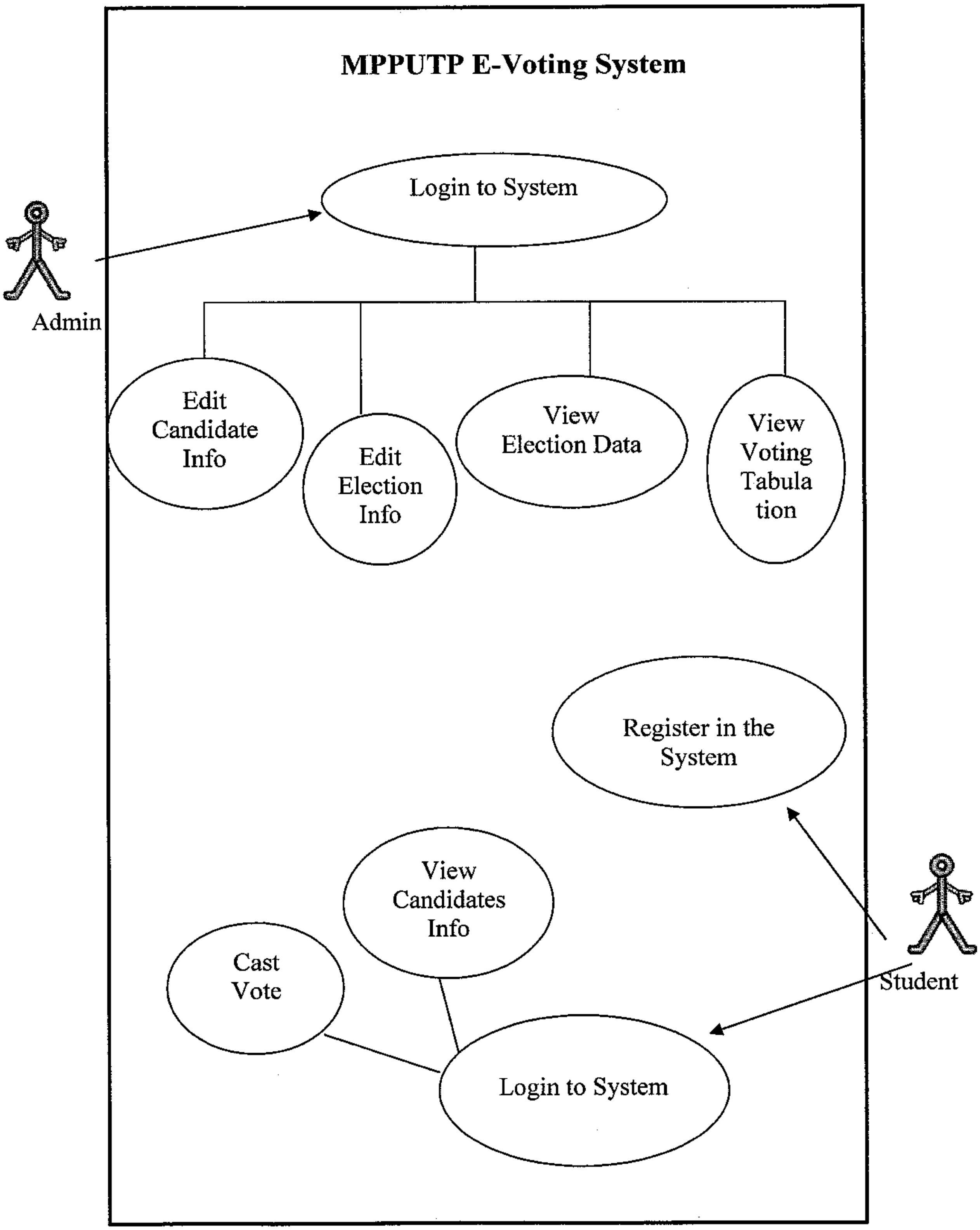
ACTIVITY DIAGRAM
(Student)



ACTIVITY DIAGRAM
(Administrator)

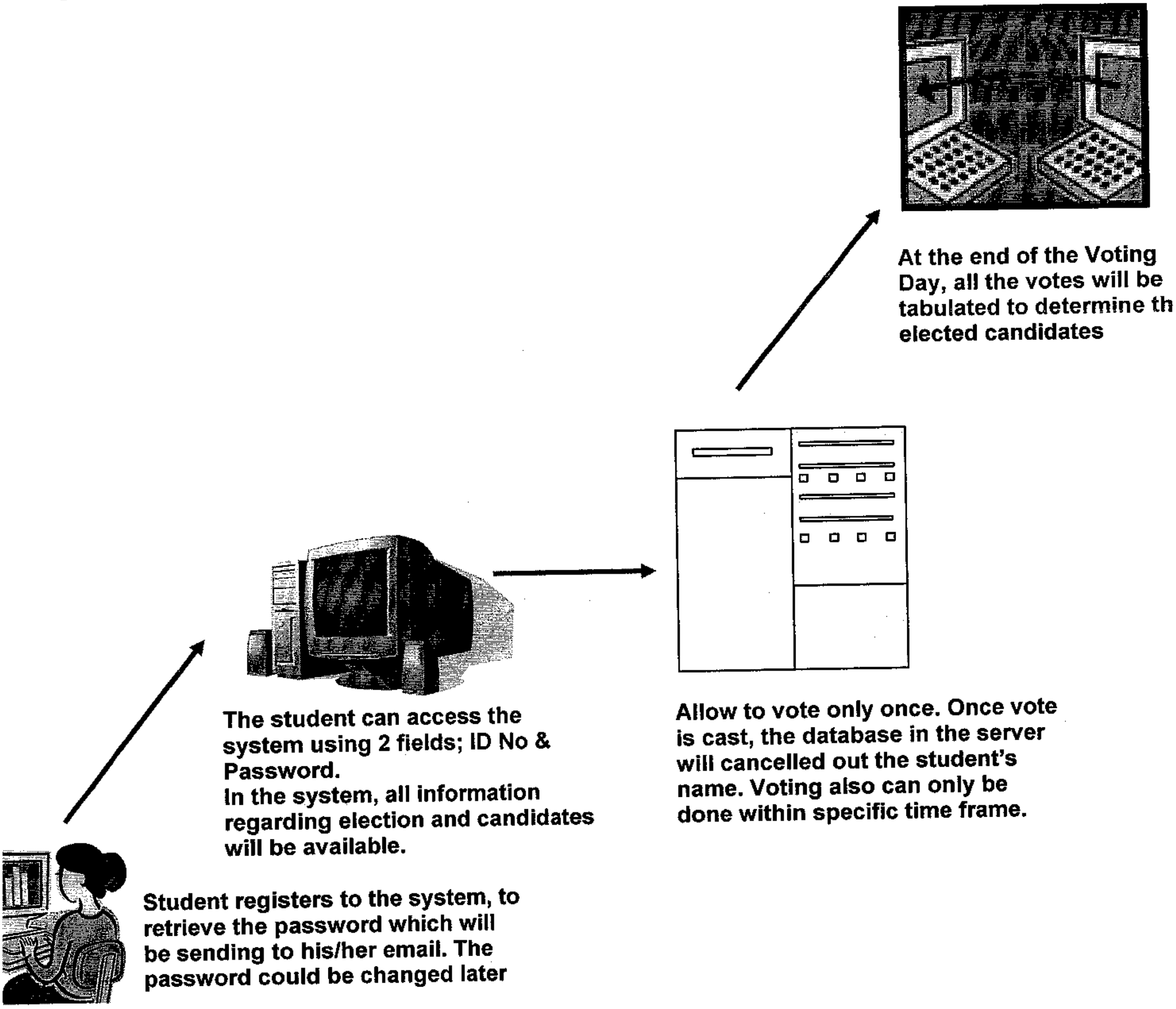


USE CASE DIAGRAM



3.2.4 Implementation Phase

On this final phase of the methodology, a complete flow of implementation is decided after the last 3 steps are met. Thus, as the system followed through these implementations, a result of the system is generated.



Student registers to the system, to retrieve the password which will be sending to his/her email. The password could be changed later

The student can access the system using 2 fields; ID No & Password.
In the system, all information regarding election and candidates will be available.

Allow to vote only once. Once vote is cast, the database in the server will cancelled out the student's name. Voting also can only be done within specific time frame.

At the end of the Voting Day, all the votes will be tabulated to determine th elected candidates

Figure 3.2: MPPUTP E-Voting User Procedure

3.3 Tools & Infrastructure

The tools that are used in developing the system for MPPUTP E-Voting context as per demonstration usage would be:

Minimum Technical Description

Details	Description
Platform	Microsoft Windows XP / Win2K Advanced Server Operating System, Internet Information Services 5/6 Version as web server, Macromedia Dreamweaver 8 as web developing tool
Programming Language	Microsoft ASP / JavaScript
Database	Microsoft Access 2000 Version 9.0 Build 6620
Technical Requirements	Intel Pentium4 3.0Ghz processor, 512MB RAM, 1024x768 resolution

However, if this system is being implemented in UTP as a working and practical mechanisms in handling the real MPPUTP election, the tools that are required are much greater:

a) Powerful server with Windows XP/ Win2K Advanced Server Operating System, with at least 1G RAM

b) MS SQL as a relational database for database and clustering database capabilities

c) Internet Information Services 6.0 Version installed as web server

d) Microsoft FrontPage as web developing tool

e) Secured Socket Layer being applied

Chapter 4

RESULTS & DISCUSSION

4.1 E-Voting In Malaysia

The possibility of e-voting being implemented in Malaysia is there since all Malaysian posses the MyKad. The government of Malaysia utilized state-of-the-art technology to develop and implement MyKad which is a multipurpose digital application card for all citizens over the age of 12.

Referring back on the literature review part, one of e-voting category is consist of direct recording machine (DRE), and the other one is public network DRE or simply known as Internet voting. It can be said here that both category can be applied in the environment of Malaysia, but there are limitations. Let's see the possibility of both categories in one by one.

4.1.1 E-Voting in Malaysia by Direct Recording Machine

For direct recording machine, it can be the simplest way of e-voting application as it can be. A secured terminal is readied at polling stations and all the voters need to do are to produce their identification. Since MyKad has its own smart identification through its IRIS Smart Chip, a trusted and reliable true identification can be verified. The MyKad will be inserted into a smartcard reader, already been integrated with the direct recording machine itself. The machine will verify whether the voter is one of the eligible voters in the parliamentary area. If so, then the voter will be allowed to cast his vote.

The vote will then be transferred through a secured network to a presint server. This means, a multiple direct recording machine can be allocated within the parliamentary area but somehow all the votes that are cast will be sent to the same server in each parliamentary area. The presint server which is located in one location will be secured physically and monitored by Election officials for voting tabulation purpose and also the area can be presented by representatives from contested parties for vetting and supervision purposes.

The limitations on this way of application are somehow quite identifiable although through more deep research can be done to eliminate them. One of the limitations is the economic wise. With this kind of implementation nationwide, it is budgeted to cost millions to the country just to implement this once in 5 years undertakings. The costs of just to set up the direct recording machine and the presint server and other petty and invisible costs somehow are quite enormous and massive for the national budget.

The social aspect is also being taken as limitation as whether Malaysians in general are ready to venture into this new technology. Perhaps, as one of the stepping stone to this application is to implement it in urban parliamentary areas first. For Wilayah Persekutuan parliamentary election, the election can be as the pilot project for e-voting application. There are 11 parlimentary areas in Wilayah Persekutuan which are Kepong, Batu, Wangsa Maju, Segambut, Setiawangsa, Titiwangsa, Bukit Bintang, Lembah Pantai, Seputeh, Cheras and Bandar Tun Razak. These areas have the most populous areas in Malaysia and the standard of computer literary is one of the highest in the country. From these enclaves, maybe e-voting application can be brought up to the whole Klang Valley, and perhaps to the whole country one day, with the right equipments, technology and mindset.

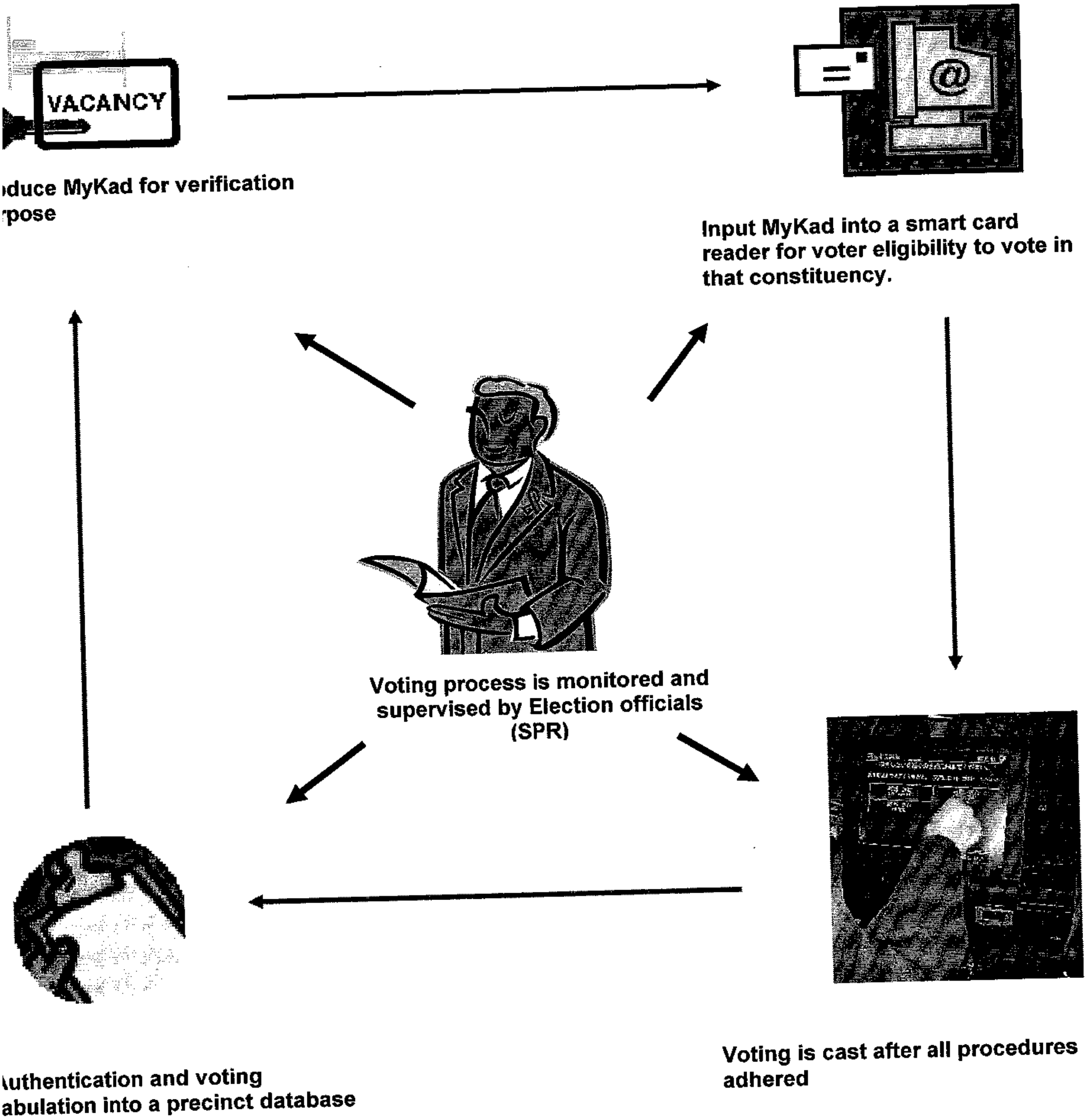

VACANCY
ıduce MyKad for verification
'pose
Input MyKad into a smart card reader for voter eligibility to vote in that constituency.
Voting process is monitored and supervised by Election officials (SPR)
Voting is cast after all procedures adhered
ıuthentication and voting
abulation into a precinct database

Figure 4.1: Proposed Malaysian DRE E-Voting Procedure

4.1.2 E-Voting in Malaysia by Internet Voting

Looking on to another type of e-voting, which is known as public remote direct recording or Internet voting, this technology also is possible in Malaysia's environment, again to the availability of MyKad by Malaysians. This kind of technology has been implemented by countries overseas particularly Estonia as they implemented it on the whole country scale. A voter needs to posses a MyKad together with a card reader attached to a computer / client which actually acts as direct recording machine. As it is an Internet voting, the voter can accessed the voting server from anywhere in the world. As the votes are cast, it will be stored in central servers located in Malaysia who will be monitored by Election officials.

The key to this application is that MyKad supports the feature of public key infrastructure. Public Key Infrastructure (PKI) requires security certificate to be issued in its transaction. MyKad able to store security Cert in its IRIS Smart Chip which would deny of security tempering in today's' technology and leads to the possibility of Internet voting.

However there are still limitations to this idea of Internet voting. On cost wise basis, the implement of Internet voting might cost lower than DRE type, as only central servers are identified at the moment. But still the cost figures will be high as to initiate the application requires deep study and research on many aspects.

On social aspect there are still many such as Internet capabilities among Malaysians. Broadband is another case in point. The government has been promoting broadband use for many years yet the incumbent operator, which is still majority-owned by the government, did not introduce the service until 2001 and failed to promote it at all aggressively for some time. Even today the uptake of broadband is still fairly low. Malaysia has one of the lowest penetrations of broadband services throughout the Asia-Pacific region. Yet broadband has a prominent place in the government's plans. It is aiming at 25% household broadband penetration by the end of 2006, 50% by the end of

2008 and 75% by the end of 2010. Internet usage is currently quite low for a country at Malaysia's stage of economic development. This is largely due to the slow uptake of broadband services.

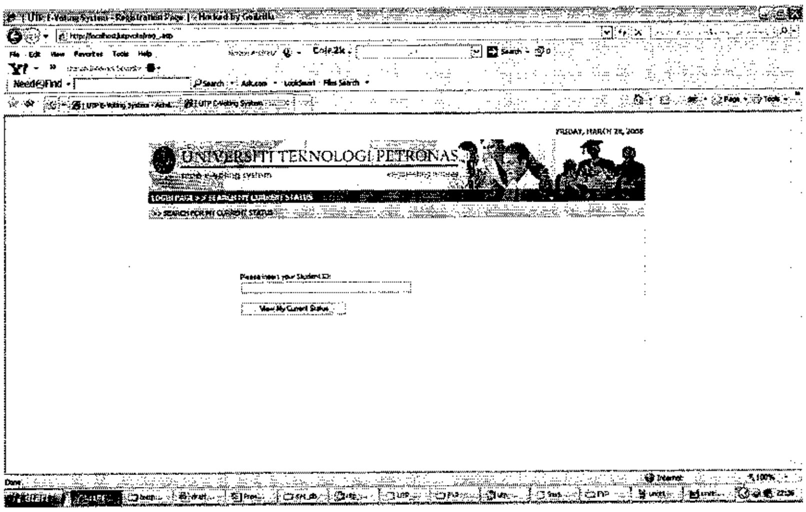
Another inhibiting factor has been the attempts by government to control the distribution of what it sees as objectionable material over the Internet. The country is now reasonably well endowed with communication infrastructure be it wired or wireless, at least in its populated areas. There are still a number of infrastructural deficiencies elsewhere, however. Services are lacking in much of the rural areas in the country, especially in East Malaysia.

Nevertheless, the implementation of E-Voting as said such would be beneficial in terms of work time saving spent on election works, the knowledge and information gained and spread effectively through the election. This also helps in nation's aspiration to achieve a K-society through its MSC ambition and works fully geared and truly reflected a developed society on a way to vision 2020.

4.2 MPPUTP E-Voting System

The MPPUTP E-Voting System will be designed to cater the needs of UTP students which want a fast and quick approach to cast their vote in electing their MPP council.

A database of the whole of UTP students will be integrated to the system's database through real time integration. This required students to register first to the system's by notifying their Matric No.

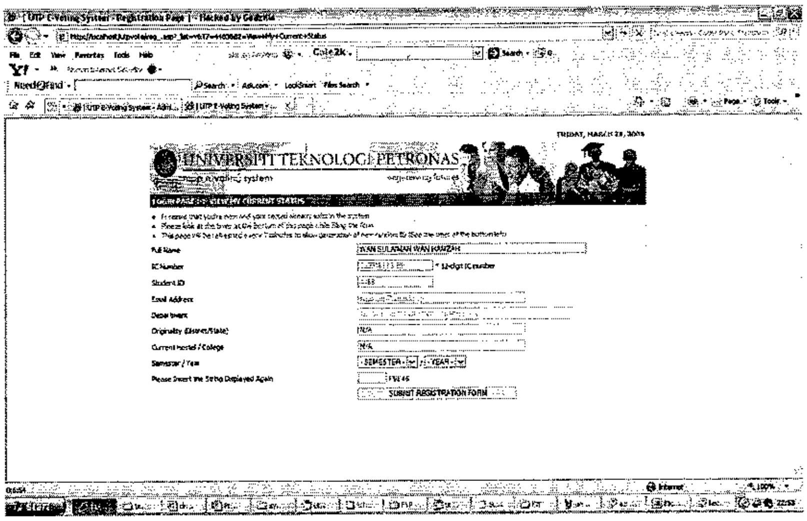

UTP E-Voting System - Registration Page
File Edit View Favorites Tools Help
UNIVERSITI TEKNOLOGI PETRONAS
FRIDAY, MARCH 28, 2008
LOGIN PAGE >> SEARCH MY CURRENT STATUS
>> SEARCH FOR MY CURRENT STATUS

Please insert your Student ID:

View My Current Status

Figure 4.2: Student Notifying the System by Providing Matric No.

Soon after the Matric No. is notified, the system will double check with UTP students' database. If the Matric No. does exist, the student will be registered into the system's database. After the registration is completed, the system will sent a random first time password to the student's UTP email, as stated in the database. This function requires the system to know the SMTP IP of the e-mail's server. The password then can be used to login into the system, and the student is encouraged to change the password later to his/her own preference.



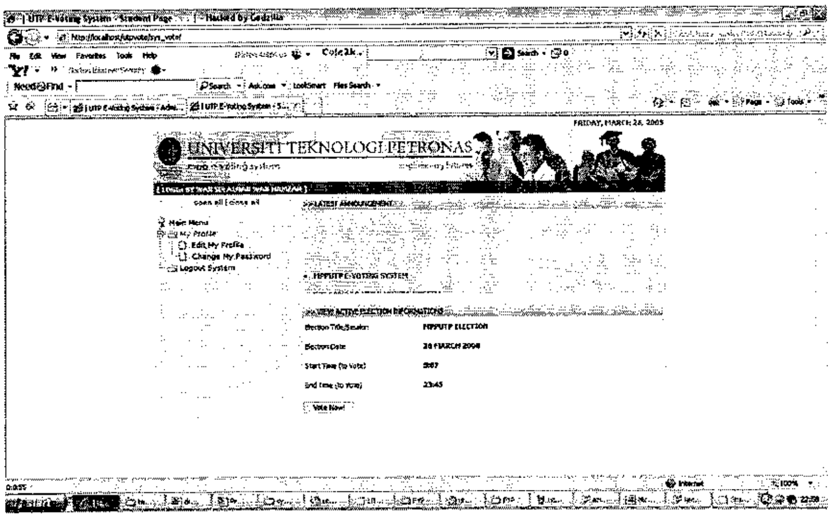
UTP E-Voting System - Registration Page
File Edit View Favorites Tools Help
FRIDAY, MARCH 28, 2008
UNIVERSITI TEKNOLOGI PETRONAS
LOGIN PAGE >> VIEW MY CURRENT STATUS

Full Name	WAN SULAIMAN WAN HAMZAH
IC Number	[illegible] * 12-digit IC number
Student ID	[illegible]
Email Address	[illegible]
Department	[illegible]
Originality (District/State)	N/A
Current Hostel / College	N/A
Semester / Year	- SEMESTER - ▾ / - YEAR - ▾
Please Insert the String Displayed Again	FWE46

SUBMIT REGISTRATION FORM

Figure 4.3: Registration Process of First Time User, to Get the Password

Inside the system, the student could view information regarding the Election, posted by administrator. Information such as the voting period, the candidates profile and manifesto and also any important announcement are made available within the system itself. The most important function in the system is the voting function, in which the student may vote for only once, candidate of his/her choice for General constituency and also Department constituency. The student is allowed to vote for only within the voting period, prior set by administrator. Outside from the voting period, he/she may only be allowed to navigate thorough the system to get updated with the election events.

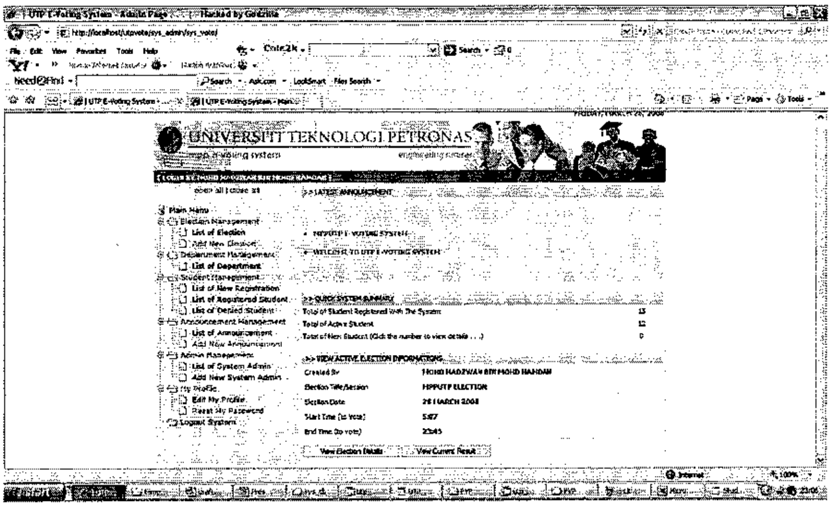


Election Title/Session	MPPUTP ELECTION
Election Date	28 MARCH 2008
Start Time (to Vote)	9:07
End time (to Vote)	23:45

Vote Now!

Figure 4.4: Main Page of MPPUTP E-Voting System for Student

Meanwhile, the system is being maintained and monitor by the system administrator. The administrator has privilege to update any information in the system regarding the candidates, election info, important announcements and many others. As an administrator, he/she has authority to block or deny any students to login into the system due to any factor or causes that might arise.



>> LATEST ANNOUNCEMENT

- MPPUTP E-VOTING SYSTEM
- WELCOME TO UTP E-VOTING SYSTEM

>> QUICK SYSTEM SUMMARY

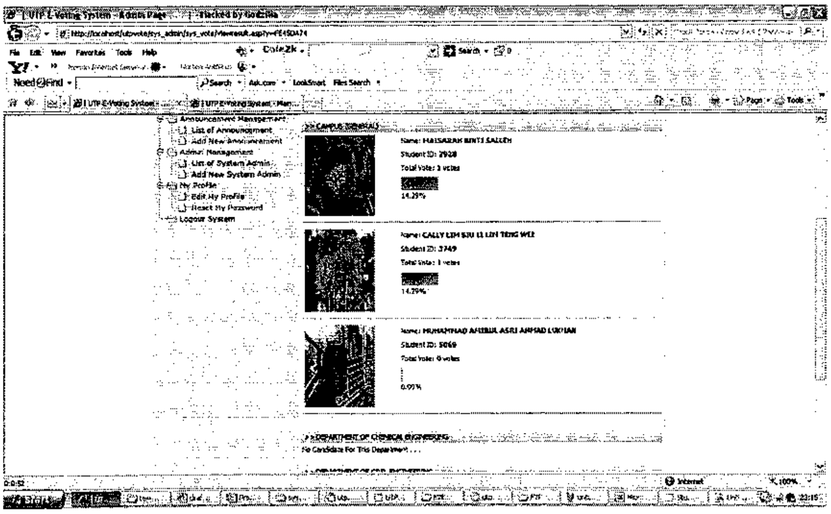
Total of Student Registered With The System	13
Total of Active Student	12
Total of New Student (Click the number to view details . . .)	0

>> VIEW ACTIVE ELECTION INFORMATIONS

Created By	MOHD HADZWAN BIN MOHD HAMDAN
Election Title/Session	MPPUTP ELECTION
Election Date	28 MARCH 2008
Start Time (to vote)	5:07
End Time (to vote)	23:45

Figure 4.5: Main Page of MPPUTP E-Voting System for Administrator

The most privilege an administrator obtained is to view the voting result, which would elect the MPP council. An administrator could double check with the database if any student has yet or already voted in the election.



>> CAMPUS GENERALS

Name: HAISARAH BINTI SALLEH
Student ID: 2928
Total Vote: 1 votes
14.29%

Name: CALLY LIM SIU LI LIM TENG WEI
Student ID: 3749
Total Vote: 1 votes
14.29%

Name: MUHAMMAD AFIBUL ASRI AHMAD LUKMAN
Student ID: 5069
Total Vote: 0 votes
0.00%

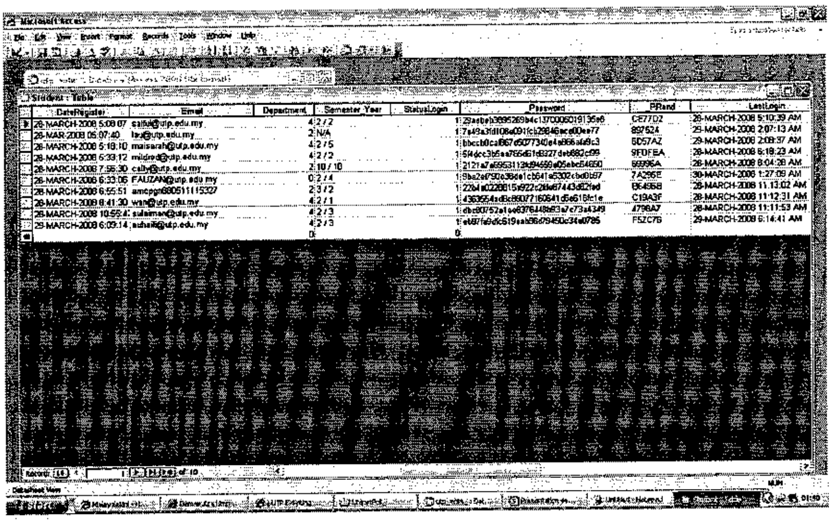
>> DEPARTMENT OF CHEMICAL ENGINEERING
No Candidate For This Department . . .

Figure 4.6: Voting Result Viewed by Administrator

4.2.1 Security Aspects in MPPUTP E-Voting System

A multiple security aspects are taken into the implementation of this system. It begins with the login page, where the student is required to provide his/her Matric No. and password. A password protection account is very important for any system, to avoid integrity-breached to happen. This means a different person login and performs activity against the wishes of the real owner account in the system.

This password is stored in the database as an encrypted value, through MD5 encryption. This means, even if the database security is tempered, the intruder will not be able to steal other students' password since it is encrypted. This in a way provides password privacy to the students.



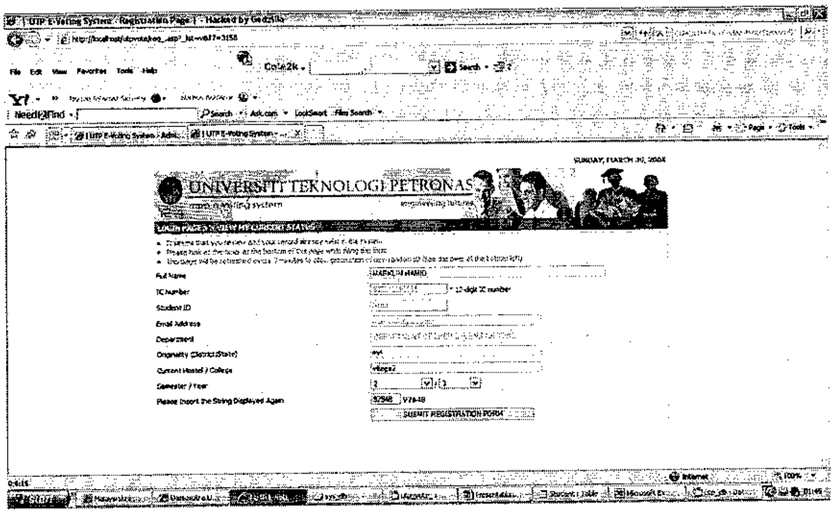
DateRegister	Email	Department	Semester_Year	StatusLogin	Password	PRand	LastLogin
28-MARCH-2008 5:08:07	saiful@utp.edu.my	4	2 / 2	1	29aebeb3895269b4c1370006019136e8	CE77D2	28-MARCH-2008 5:10:39 AM
28-MAR-2008 05:07:40	laz@utp.edu.my	2	N/A	1	7e49a3fd108e091fcb29846ace00ee77	897524	29-MARCH-2008 2:07:13 AM
28-MARCH-2008 5:18:10	maisarah@utp.edu.my	4	2 / 5	1	bbccb0caf867d5077340e4a866a6a9c3	6D57AZ	29-MARCH-2008 2:08:37 AM
28-MARCH-2008 6:39:12	mildred@utp.edu.my	4	2 / 2	1	5f4dcc3b5aa765d61d8327deb882cf99	9FDFEA	28-MARCH-2008 6:18:23 AM
28-MARCH-2008 7:56:30	cathy@utp.edu.my	2	10 / 10	1	212fa7a6953113fd94659a05ebc54650	69996A	28-MARCH-2008 8:04:28 AM
28-MARCH-2008 6:33:06	FAUZAN@utp.edu.my	0	2 / 4	1	9ba2ef790a38de1cb641a5302cbd0b97	7A296E	30-MARCH-2008 1:27:09 AM
28-MARCH-2008 6:55:51	amcpgn880511115327	2	3 / 2	1	22b4a0228815a922c2de87443d82fed	B64568	28-MARCH-2008 11:13:02 AM
28-MARCH-2008 8:41:30	wan@utp.edu.my	4	2 / 1	1	4363954ad8c89077160641d5e616fc1e	C19A3F	28-MARCH-2008 11:12:31 AM
28-MARCH-2008 10:55:4	sulaiman@utp.edu.my	4	2 / 3	1	dbe90752a1ee837648b83a7c73a4349	4798A7	28-MARCH-2008 11:11:53 AM
29-MARCH-2008 6:09:14	suhaili@utp.edu.my	4	2 / 3	1	eb97fa9dfc619eab96d79450c34e0785	F52C76	29-MARCH-2008 6:14:41 AM
		0		0			

Record: 1 of 10

Figure 4.7: Password Hashed in the Database through MD5 Encryption

Another security aspect is the login session time for both student and administrator. After a certain time of idle activity, the user will be automatically logout from the system and need to login back if want to use the system.

During the registration process into the system, the student needs to apply the verification code displayed on the screen to verify that the user is the real user who wants to register into the system. This verification code application is put in place in order to avoid computer generated or malicious script to fake register into the system.



UNIVERSITI TEKNOLOGI PETRONAS
File Edit View Favorites Tools Help
Search
SUBMIT REGISTRATION FORM

SUNDAY, MARCH 30, 2008

Full Name	[illegible]
IC Number	[illegible] * 12-digit IC number
Student ID	[illegible]
Email Address	[illegible]
Department	[illegible]
Originality (District/State)	[illegible]
Current Hostel / College	[illegible]
Semester / Year	2 / 3
Please Insert the String Displayed Again	[illegible]

Figure 4.8: Verification Code in the Registration Form

The application of HTPPS and SSL security could be applied in the system if it is really wanted to be implemented in UTP. Through this, a more secured voting transaction could be made since the line is encrypted and have its own passage line. However, to implement HTPPS and SSL application, a more complex tool and infrastructure need to be in place since the requirement of hardware for these security measures is more demanding. A more powerful server is needed to support HTPPS and SSL security application.

Chapter 5
CONCLUSION

At the conclusion we gone through the final stage of this project, it can be said here that the discoveries about the workingness of e-voting is being explained. The characteristics and security features are also being mentioned in this report

This project has shown that MPPUTP Election can be held in UTP through E-Voting approach, where practicality and security integrates. Through this project, it is hope that the problem statement stated earlier could be resolved by this technology application. If E-Voting culture is started in campus, we can nurture these young minds to start accepting the arrival of E-Voting as a means to cast their vote, for it to be implemented in a wider scale in the near future.

The study on the issue of e-voting being implemented in Malaysia has been explained where both advantages and disadvantages are explained. However, through this research, it can be concluded that for E-Voting to be implemented in Malaysian election is not impossible since Malaysian have the technology and state-of-the-art MyKad. Nevertheless, more study and research need to be carried out if Malaysia is serious in venturing into E-Voting. More thorough emphasizes need to be reviewed especially on some pressing issues during elections.

REFERENCES

1. Celeste, Richard. "Asking the Right Question about E-Voting". National Academies Press, 2005.

2. Aviel D. Rubin. "Brave New Ballot: The Battle to Safeguard Democracy in the Age of Electronic Voting". Morgan Road Books, a Division of Random House, 2007.

3. Russell Smith. "Electronic Voting: Benefits and Risks". Trends and Issues in Crime and Criminal Justice, Vol. 224, April 2002.

4. Mr. Mohd Mokrim B. Hassan. "IT And Media Services personnel". Universiti Teknologi PETRONAS, 31750 Tronoh, Perak.

5. Mr. Ahmad Faisal B. Abdul Ghafar. "Pegawai Sistem Maklumat, Bahagian Perancangan Korporat". Universiti Putra Malaysia, 43400 Serdang, Selangor.

6. Jabatan Pendaftaran Negara Malaysia website. "www.jpn.gov.my"

7. Vepa Mollayev. "E-Voting Application for Executive Committe of MPPUTP". Universiti Teknologi PETRONAS, 31750 Tronoh, Perak.

8. "http://www.vote.caltech.edu/"

9. http://www.votingintegrity.org/pdf/draft-test-manul.pdf

APPENDICES

Coding for Main Page for Student's Interface

```
<!-- #include file="..\sys_discreet\dbconn.asp" -->
<!-- #include file="..\sys_discreet\3des.asp" -->

<html>
<head>
<meta http-equiv="Content-Language" content="en-us">
<meta http-equiv="Content-Type" content="text/html; charset=windows-1252">
<link href="sys_image/css_style_template/style02.css" rel="stylesheet" type="text/css"/>
<title>| UTP E-Voting System - Main Page |</title>
</head>
<body>

<script language="JavaScript">
function chkLogin()
{
if (document.satu.T1.value == "")
        { alert("Please insert your STUDENT ID!");document.satu.T1.focus();return
false; }
if (document.satu.T2.value == "")
        { alert("Please insert your CURRENT
PASSWORD!");document.satu.T2.focus();return false; }
}
</script>

<br><br><br>

<div align="center">
<table border="0" cellpadding="2" cellspacing="1" width="620" id="table1"
style="border-style: outset; border-width: 1px">
<tr height=20><td><%Call initLink%></td></tr>
<tr><td><img border="0" src="sys_image/header.jpg" width="620"
height="80"></td></tr>
<tr><td height="200" background="sys_image/<%initColour%>"><%Call
initBody%></td></tr>
<tr><td>&gt;&gt; For any enquiries regarding the system, please contact 012 -
5335884</td></tr>
</table></div>
</body>
</html>
<%
```

```
Function initLink()

Dim SQL
SQL = "Select * From Link Where Active = 1"
RS.Open SQL, db
If Not RS.Bof Then
Response.Write "| "
While Not RS.Eof
        Response.Write "<a target=_blank href=" & chr(32) & RS("hyperlink") & chr(32)
& ">" & LCase(RS("link_view")) & "</a> | "
RS.MoveNext
Wend
Else
        Response.Write "...................."
End If
RS.Close
Response.Write "<a href=reg_.asp>new? view status here</a> | "
Response.Write "<a href=reg_.asp?_list=y>view waiting list</a> | "
End Function
Function initBody()
Response.Write "<form name=satu method=post
action=""sys_login/chklogin_.asp?_login=s_login"" onsubmit=""return chkLogin()"">"
Response.Write "<input type=hidden name=dua value=" & hexValue(10) & ">"
Response.Write "<div align=center>"
Response.Write "<table border=0 cellspacing=1 width=""50%"" id=table2>"
Response.Write "<tr><td width=100>STUDENT ID :</td><td>&nbsp;<input type=text
name=T1 size=30></td></tr>"
Response.Write "<tr><td width=100>PASSWORD :</td><td>&nbsp;<input
type=password name=T2 size=30></td></tr>"
Response.Write "<tr><td width=100>&nbsp;</td><td>&nbsp;<input type=""submit""
value=""     Login to System     "" name=""B1""></td></tr>"
Response.Write "</table></div></form>"
End Function
Function initColour()
Dim time
time = Second(Now)

If time Mod 3 = 0 Then
        Response.Write "Body1.jpg"
ElseIf time Mod 3 = 1 Then
        Response.Write "Body2.jpg"
Else
        Response.Write "Body3.jpg"
End if
End Function
%>
```

Coding for SMTP IP server

```
        Set db  = Server.CreateObject("ADODB.Connection")
        Set RS = Server.CreateObject("ADODB.Recordset")
        Set RS1         = Server.CreateObject("ADODB.Recordset")
        Set RS2         = Server.CreateObject("ADODB.Recordset")
        Set RS3         = Server.CreateObject("ADODB.Recordset")

   db.Open Connection
   smtp_IP = "xxx.x.x.x"
%>
```