CHAPTER III
SYSTEM ANALYSIS

3.1 The Existing System

The existing assessment system for the Information Technology subject at SPM level is divided into two categories. Paper 1 is a centralized examination conducted by the Examination Syndicate of Malaysia. Paper 2, on the other hand, is a school-based assessment managed by teachers teaching the Information Subject in schools. It is an on-going evaluation process of students’ knowledge, skills and norms in the Information Technology subject.

3.1.1 Examination overview

The Paper 1 for Information Technology subject has three sections, namely, Section A, Section B and Section C. Section A consist typical structured examination question that uses paper and pencil. It includes 10 multiple-choice questions plus a few fill-in the blanks questions that need to be answered in an answer booklet during stipulated examination time period. The section B and C is a computer-aided examination. The candidates use computer application and facilities to answer the given examination question. The response of each student will be saved on individual diskettes, which will then be collected by a Chief Invigilator and forwarded to The Examination Syndicate office for scoring and marking via the State Education Department.
3.1.2 Examination Management

Managing the existing system requires a lot of administrative tasks to be done manually by the examination center’s Chief Invigilator and a group of his assistants. Their job starts two weeks before the examination day. They have to reset and prepare the school computer lab for the test according to requirements set by the Examination Syndicate.

As such, the school computer lab must meet the Examination Syndicate regulations and requirements upon approval to the computer lab as an examination center for the Information Technology subject. The requirements stipulate that the lab must have at least 25 sets of multimedia personal computers connected by Local Area Network, a dedicated server and a personal computer for administrative purpose, and a Public Switched Telephone Network (PSTN) or Integrated Services Digital Network (ISDN) Internet connection. The school must also provide a licensed operating system and application software.

The examination invigilators comprise a Chief Invigilator, an Assistant Chief Invigilator and another invigilator. All of them come from neighboring schools and the Examination Section of the State Education Department assigns them. The school must also provide a technical assistant staff to help. Their initial duty is to reformat the entire computer in the lab and reestablish Local Area Network and Internet Connection. The reason for the reformatting is to prevent candidates from
storing and hiding notes, ensure computers are free from virus and minimize the possibility of computer failure during the examination.

On the examination day, the Chief Invigilator must get the examination question papers from the State Education Department. Normally, the State Education officer has earlier sent the questions to be kept safely under tight security at a nearby school. The Chief Invigilator will take the papers to his examination center early in the morning of the examination day. Candidates may be allowed to enter the examination center at 8.00 a.m. and will be seated randomly. The examination will begin according to the Examination Timetable provided by the Examination Syndicate. When the candidates are ready, and as scheduled, Section A of the Paper 1 booklet will be distributed. It is an objective-type question with 10 multiple-choice questions, followed by a number of a filling-in-the-blanks type of question. Candidates would be required to complete the examination on that booklet. After half an hour, the question booklet with candidates responses duly filled will be collected and packed by the invigilators.

The examination will proceed with Section B and section C. Before the question papers are delivered, the candidates are required to boot the computer and log in as a client to the server that runs on Windows NT version 4 platform. If the login is successful, candidates will gain access to their folder in the server. Candidates must use the software that is specified in the question paper to response to the question. Software that are used are Microsoft Word, Microsoft PowerPoint and chosen web editor such as Netscape Navigator or Microsoft FrontPage to response to the
question that requires developing a web page. All responses must be saved in the server under the candidates' individual folder.

When the examination time is up, one of the invigilators would distribute diskettes to the candidates. Candidates would have to save a copy of their responses in the given diskettes and submit it to the invigilator in charge. These diskettes will be forwarded to the Examination Syndicate office through the State Education Department. A compressed copy of the entire candidates' responses would be transferred to the Examination Syndicate server via FTP from the examination center.

3.2 Proposed System

3.2.1 Overview of the Proposed System

A web-based multiple-choice type of on-line examination using VPN is proposed in this paper to replace the existing system described above. By doing the examination on-line, examination management can be conducted more efficiently. A lot of trivial job such as storing the examination question paper, packing and forwarding candidates script are no longer needed.
3.2.2 VPN Establishment

A router-to-router VPN will be setup to connect the Examination Center LAN and the Examination Syndicate server. On the examination day, the Chief Invigilator of each Examination Center will connect their LAN to the Examination Syndicate server by login the given password to establish a PPTP connection, which enable a virtual private networking between his Examination Center and the dedicated server for the examination. Once the connection with the server is established, the candidates can start access the particular examination web page from their workstation.

3.2.3 The Examination Web Page

The Information Technology subject examination candidates will take their examination by interacting with the examination web page located at the Examination Syndicate server. On the main page of the examination web site, candidates have to login by keying in their user identity and password to gain access to the question page and to enable them to response/answer to the questions. The user identity keyed-in will be used to record the test score and to report the examination result.

After the candidates successfully log into system, they will be directed to the examination web page. If not, the candidate is required to do the login once more.
The Section A examination paper consist of multiple question with four choice of answer. Each question is displayed on a new page. Candidates must point his mouse pointer to the correct answer of his choice to response. Once the mouse is clicked, the response is selected and the second question page will be displayed consequently. Candidates can proceed until he has complete responding to the entire question as required. Should the candidates want to change their responses, they are free to browse back to the previous question and make changes to the response during the examination session. The candidate's can edit and make changes to the previous answers by clicking the back button on the browser.

A progress bar will show the number of question the candidates had responded. When the allocated time is up, the examination page will be disabled and the candidates results will be displayed.

3.2.4 Data Transfer

The transfer of data between the candidates’ machine and the Examination Syndicate Server will be carried on a VPN connecting the Examination Center and the Examination Syndicate server. The deployment of a VPN is essential to ensure a thorough security control over the data in transmission and the candidate's authentication process. The data packet transferred between the Examination Center and the Examination Syndicate server will be carried on a defined tunnel through the Internet. The packets are encrypted by the VPN protocol solution and encapsulated
in PPTP header to avoid eaves dropping. Those security features make certain the integrity of the examination session and the candidates' response.

3.2.5 Authentication

The examination web page is process by Active Server Page (ASP) server side scripting language. This server side scripting has the ability to authenticate user using challenge response technique. Candidates identity and password login by the candidates will be compared to the record that registered with the Examination Syndicate and stored in the Examination Syndicate database. If the identity and password matched with the record for that particular candidate's, he will be allowed to sit for the examination and the examination web page will be displayed on his workstation, else, he will not be able to access the page.

3.2.6 Multiple-delivery

The server side scripting will generate randomized question on the web page. These questions are obtained from the database bank-question that contain number of question. The candidates sitting side by side to each other will not necessary get the same set/item of questions. This feature prohibits identical question sets for two candidates. This feature ensures candidates unable to copy their friends' responses.
3.2.7 Scoring

The Active Server Page (ASP) server side scripting language will do the scoring of the examination automatically. The Examination Syndicate does not have to employ teachers to do the marking manually. The result can be produced once the candidates complete their response at the examination center itself. This feature enhanced the transparency of the examination and prevent human error during marking.

3.3 Requirement Definition

A requirement is a feature of the system or the description of something the system must do in order to achieve the objective of the system. It is essential to define system requirement by identifying services that the system will provide. Such system requirement can be divided into functional requirements and non-functional requirements.

3.3.1 Functional Requirements

Functional requirements are those tasks that the system must perform. The on-line examination through Virtual Private Network system will be developed to provide the following functional services:
a) **Examination Center Authentication**

The Chief Invigilator of an Examination Center will make a dial-up connection to The Examination Syndicate server for center authentication. After successful dialing up and authentication process, a tunnel will be established between the server and the member of the Local Area Network of the Examination Center. Data transferred between these two destinations will be encapsulated in PPTP protocol format. The packet will be routed in a defined path. Candidates can access the main page of the examination web site.

b) **Candidate authentication and registration**

Before the examination takes place, the candidates will be provided with a password and user name by the invigilators. The candidates will then key-in the user name and password into the main page of the examination web examination site and thus registered into the examination database on the Examination Syndicate server. Their user name and password will actually be matched the registered Information Technology student database.
c) **Question Navigation.**

Question navigation enables candidates to browse through the questions set. The candidates are free to answer any questions or skip the questions that they feel difficult and need further thinking, or go back to any question that they think need to be revised.

d) **Scoring**

Scoring interface is only available to users who login is assigned as Examination Syndicate officer. Scoring is done automatically by the system. The result will be saved on.

e) **Random generator**

A random generator coding on the system will ensure the implementation of multiple deliveries of sets of questions to be answered by candidates in each session. This prevents them copying answers from the other candidates.
f) **Progress indicator.**

A progress indicator located at the top of the page will show the number of the question answered. A progress bar will advance as the candidates proceed to the next question. It gives a visual indicator to the candidates of the progress they are making.

### 3.3.2 Non-functional Requirement

Non-functional requirements are those requirements that are not directly needed but are equally important in implementing the system. In this system, security, user friendliness and latency were identified as part of non-functional requirements.

a) **Security**

SPM is one of the most important examinations in the Malaysian schooling system. It is an established evaluation system recognized by many academic institutions throughout the world as a valid and reliable evidence of academic performance of the candidates. If examination security is compromised, the validity of the examination may be affected. Consequently, SPM’s credibility as a national standard evaluation tool can be questioned.
b) **User Friendliness**

One of the purposes of having an on-line assessment is to assure that the examination is managed efficiently at the management site, as well as at the candidates' site. Candidates as the users of the system should not be the victims of technological confusion. Therefore, the system to be developed must not burden the candidates that could add stress during the examination. A proper interface design with user friendly approach is one of the critical aspect to the success of the system to be developed.

c) **Speed**

Speed is one of the critical factors in the implementation of an on-line assessment. It is beneficial to have a system that requires minimum computing power to run that system to avoid latency. A very strong encryption algorithm needs more computing process. As a result, it may reduce data transmission speed. Another factor that needs consideration is multiple accesses to the Examination Syndicate's server in an examination session. As many candidates will take the examination from different schools at the same time, heavy traffic and congestion is predicted. Proper choice of server machine, medium of data transfer and proper system configuration may help to minimize latency.
3.4 Consideration on VPN Implementation

VPN can be implemented using software solution or a dedicated hardware device. Cisco, one of the pioneer player in the network security offers wide range of hardware to support VPN implementation, while Microsoft, the dominant operating system vendor offers free solution of VPN ship with Microsoft Windows 98, Windows NT and Windows 2000 server operating system for their clients. There are also a number of third party solution provider promoting VPN software and hardware as one of their network security product.

3.4.1 Why Microsoft VPN?

System compatibility with the existing software and hard requirement for an examination center to organize the Information Technology examination is the main reason for choosing the Microsoft VPN. As the Examination Syndicate has regulated the entire examination center to use Windows NT as the center server operating system during the SPM Information Technology subject examination session and Windows 98 for the client machine, it is fair to suggest that Microsoft Point-To-Point Tunneling (PPTP) protocol VPN solution as a solution to be implemented in this web-based online examination. Microsoft offers free VPN solution through the implementation of Point-To-Point Tunneling Protocol, which is supported by Windows 98, Windows NT and Windows 2000 server.
Another reason for choosing Microsoft VPN solution is that it is the solution is available for free. One of the problems faces by the school offering Information Technology subject for their student is financial constrain. The Ministry of Education provides a very limited grant to the school. Each school gets RM60.00 per head grant (according to the number of student taking Information Technology Subject). The amount is far from enough to maintain the computer in the lab. Implementations of an on-line examination require purchasing of a new hardware thus adding financial burden to the school.

3.4.2 Microsoft VPN Implementation Consideration

To implement Microsoft PPTP VPN solution for the on-line examination, it is suggested that all client machines on the examination center use Windows 98 operating system to support the implementation of the VPN web-based on-line examination. The server machine in the Examination Center uses Windows NT 4.0 or Windows 2000 server as regulated by The Examination Syndicate. This is one of the requirement for any school to be approved as the center for Information Technology Examination Center. The Examination Syndicate server will also be running on Windows NT or Windows 2000 platform to enable the implementation of PPTP with the Examination Centers throughout the country.

Windows NT server operating system includes the 40-bit or 128-bit encryption keys that are automatically generated for every VPN session, allowing fast, strong data encryption using the RC4 encryption algorithm. In addition, Windows NT 4.0
provides system administrators with the additional tools necessary to secure their installations. This includes integrated user authentication and facilities for enforcing strong password security. For enhanced security, Microsoft recommends the deployment of the 128-bit key encryption. [14]

To enable VPN implementation for the on-line Information Technology examination, a few configurations must be done to the examination center workstations and server. The server at the Examination Syndicate of Malaysia need to be configured to accept VPN communications by acknowledging workstation IP after the examination center is authenticated. The examination web page is made available to those workstations and candidates can submit their response through these workstations. The candidates’ responses will be transmitted to the Examination Syndicate server in encrypted text.

It is also recommended that Windows NT Server Primary Domain Controller (PDC) to be setup at every State Education Department Examination Unit. PDC can authenticate user login. Establishing distributed PDC will speed up the authentication process and reduce congestion at the main server.
3.4.3 Microsoft VPN Security Features

Microsoft VPN relies on security features of the Point-to-Point Protocol (PPP) to provide user authentication and protect the confidentiality of user data. Point-To-Point is the protocol used to transport data within the PPTP tunnel. PPP authentication methods support Microsoft Windows 98 Dial-Up Networking and Windows NT 4.0.

Remote Access Server (RAS) service provided by Windows NT include Password Authentication Protocol (PAP), Shiva Password Authentication Protocol (SPAP), Challenge Handshake Authentication Protocol (CHAP), and Microsoft Challenge Handshake Authentication Protocol (MS-CHAP). Microsoft Point to Point Encryption (MPPE) is supported in Windows 9x Dial Up Networking and Windows NT 4.0 RAS. MPPE uses the RC4 stream cipher.

PPTP depends on two proprietary protocols to protect user data at the PPP level: MS-CHAP and MPPE. Due to strong critics on MS-CHAP, Microsoft releases a new version of MS-CHAP (MS-CHAP version 2), which provides mutual authentication, stronger initial data encryption keys, and separate encryption keys for the transmit and receive paths. [15]
Microsoft recently released an update to the PPTP client and server components for Windows NT that provides administrators with the ability to configure the PPTP server so that it will only accept the stronger Windows NT password authentication.

One of the threats in PPTP connection is the man-in-the-middle attack. If an attacker could position a machine between the client and their target server, the machine in the middle could attempt to impersonate the subject PPTP server and accept the traffic from the client. The vulnerability to "man-in-the-middle" attacks exists with any non-mutual challenge response authentication protocol, and is therefore not specific to Microsoft's products. However, in the case of Windows NT data encryption is simply enabled, communication between the client and the server is fully protected and cannot be read by the machine in the middle that lacks the necessary key to decrypt information transmitted.

PPTP uses the RSA RC4 encryption algorithm. To make things more difficult for an attacker, the encryption key is changed after every 256 packets delivered. In an upcoming release, Microsoft plan to enable key changing on every single packet will further enhance security. This makes even well resourced brute force attacks nearly impossible. [15]
3.5 Example of a Microsoft VPN Client Setup

To enable the client machine to establish a VPN connection with a VPN server, the Microsoft VPN communication component must first be installed to the server operating system at the Examination Center LAN. This can be done in the control panel by selecting the “Add and Remove Program” window. Then select the Windows setup tab and check the communication component. Double click the communication component and check the Virtual Private Networking Component.

![Microsoft VPN component selections](image)

*Figure 3.1: Microsoft VPN component selections*

Windows required the computer to restart to updates the configuration. After restarting, double click the network icon in the Control Panel and click the add
button. Then select adapter and pick Microsoft from the list and double click “Microsoft Virtual Private Networking Adapter” from the Network Adapters list.

![Network Configuration Window](image)

*Figure 3.2: Microsoft VPN network configuration*

The client machine is now VPN enabled. Since PPTP encapsulates its data stream in the PPP protocol, the VPN requires a second dial-up adapter. This second dial-up adapter for VPN is added in addition to the first dial-up adapter that provides PPP support for the analog or ISDN modem. Selecting the “make new connection” icon in the “Dial Up Networking” window can do this. The purpose of this dial up is to
enable the client machine to make connection to remote server, in this case The Examination Syndicate server that stores the examination web page. The Examination Syndicate web server can control access to the examination folder and web page by limiting access to identified user only. The examination web page will not be open to public in the Internet. Despite, the user or candidates will use the Internet connection medium to enable communication to the Examination Syndicate server. The server on the other hand must be configured to accept VPN communication with the clients.

The figure below shows the first step to a new VPN connection. Microsoft VPN adapter was selected as the device to be used.

![VPN connection setup interface](image)

*Figure 3.3: VPN connection setup interface*
In the next screen, the dialog box will prompt for the Host name or IP address of the VPN-server. Key in the appropriate Host name or IP address of the server that will be connected to.

![Make New Connection](image)

*Figure 3.4: Defining the VPN host*

The next dialog box tells that the VPN dial up is successfully configured. The connection can be established once the Internet connection is available and the server is configured to accept the client.
3.6 Example of a Microsoft VPN Server Setup

Windows NT server operating system allows remote access to its resources by the user who has been granted a remote access dial up permission. PPTP is implemented to all remote access connecting to the server. [16] After authenticated, a remote user is allowed to access to the server resources as if they are in a LAN client/server relationship. In the Information Technology on-line Examination situation, candidates can access only to the subject examination folder. Once they access the examination folder, they will be directed to the login web page as a default page. The following is the procedure to configure a Windows NT server to enable virtual private networking.

In the Network property window, select the Protocols tab. Add Point To Point Tunneling Protocol as the network protocol.
Figure 3.6: Network Protocol Selections

A dialog box will appear with a prompt asking number of Virtual Private Networks to allow. Windows NT allows up to 256 number of VPN.

Figure 3.7: PPTP configurations
Figure 3.6: Network Protocol Selections

A dialog box will appear with a prompt asking number of Virtual Private Networks to allow. Windows NT allows up to 256 number of VPN.

Figure 3.7: PPTP configurations
Another dialog box will appear with a message for configuring PPTP ports in Remote Access Services setup.

![Setup Message]

*Figure 3.8: Setup message*

A remote access device must be added to the given port.

![Remote Access Setup]

*Figure 3.9: Remote access port setup*
After adding the entire RAS adapter, network configuration for dial out must be configured. Configure each VPN-adapter on the VPN-server to allow a dial in connection with to receive calls port usage.

Figure 3.10: Port usage configuration

3.7 Software Requirements

To develop the on-line Information System for SPM examination, the software’s listed below is needed:

a) Window 98- as operating system.

b) Macromedia Dream Weaver- for web page development.

c) Active Server Page (ASP)-as server side scripting language.
d) Visual InterDev- ASP page editor.

e) Microsoft Access- to develops and manage database.

f) Microsoft Word- for system documentation.

g) Personal Web Server- system testing.

h) Visio 2000- for chart and system design.

i) Microsoft NT 4 Server Operating System for VPN implementation testing.

3.8 Hardware Requirement

Massive progress in hardware development offers quality hardware with competitive price. Powerful processor and sufficient system memory will make the processing work efficient. Listed below were the hardware chosen to developed on-line examination software. They are:

a) Intel Pentium 400 MHz processor

b) 128 MB of RAM

c) 4 GB Hard disk

d) 1.44MB Floppy Disk Drive

e) 52 x CD ROM Drive

f) Keyboard

g) Mouse

h) SVGA Monitor