Security Protocol for Delay Tolerant Networks

A dissertation submitted for the Degree of Master of Information Security

S.M. Danishka Navin
University of Colombo School of Computing
Sri Lanka
November 2020

DECLARATION

The thesis is my original work and has not been submitted previously for a degree at this or any other university/institute. To the best of my knowledge it does not contain any material published or written by another person, except as acknowledged in the text.

Student‘s Name : **S.M. Danishka Navin**
Registration Number : **2017/MIS/005**
Index Number : **17770051**

$Student‘sSignature$: ..... $Date$: .....

This is to certify that this thesis is based on the work of **Mr. S.M Danishka Navin** Under my supervision. The thesis has been prepared according to the format stipulated and is of acceptable standard.

Certified by :
Supervisor’s Name : **Dr. Kasun De Zoysa**

$Supervisor‘sSignature$: ..... $Date$: .....

ACKNOWLEDGMENT

As a student of the Master of Information Security degree program, University of Colombo School of Computing, Sri Lanka, I am taking this occasion to express my gratitude to the University of Colombo School of Computing and also the people who helped to be a success with this project.

I wish to express my sincere appreciation to my supervisor, Dr.Kasun De Zoysa , Senior Lecturer at University of Colombo School of Computing, the advisor Dr. Damith Karunaratne, Senior Lecturer at University of Colombo School of Computing and Prof. Christian Rohner of the Uppsala University. They have convincingly guided and encouraged me.

Contribution of the Department of Examinations, Sri Lanka, is genuinely appreciated. Especially the Commissioner of the General Department of Examinations, Sri Lanka and his team.

I wish to acknowledge the support and love my family, including my late father, gave me to successfully complete the dissertation. Unwavering support of Dr. Buddy Liyanage, Mr. Susil Maduwage, Mr. Vincent Halahakone and Ms. Deepani Jayantha kept me going on and this work would not have been possible without their input.

ABSTRACT

Examinations are a great way to access what the students have learned with regards to a particular subject. Traditional mechanism of delivering an examination is paper-based but it has been adopted over the years to digital form. The transition from pen and paper-based examination model digitized examination has several requirements including composing questions in digital format and delivering them securely. Despite the last mile access of the candidate, examination should be equal and available to all the candidates to have a fair examination.

This research addresses the requirement of providing security to deliver complete digitized examination, including the evaluation process, to be conducted over a disrupted and disconnected environment. A new Security Protocol is introduced by this research using physical, administrative and technical controls.

The related community projects and solutions, security aspects, legal background are considered in designing the proposed protocol. Moreover, the protocol designed followed the principle of "Secure by Design", which included Threat Modelling followed by a Risk Assessment.

Several iterations of examinations were conducted to find the most appropriate solution and each iteration was tested with the participation of teachers and students. A secure protocol was implemented and it was successfully facilitated to conduct a computer-based examination with the participation of over 180,000 candidates, hundreds of teachers and other authorized officials under the Ministry of Education.

Evaluation was conducted in two methods. Firstly, each development iteration evaluated with user feedback using user surveys. Moreover, evaluation of the proposed protocol is presented through State Transition Diagrams.

This study conclude that , with the use of the physical, administrative and technical controls a computer-based examination can be securely delivered and execute in a disrupted and disconnected environment while maintaining Confidentiality, Integrity and Availability.

Contents

List of Figures

List of Abbreviations

2G	Second Generation
3G	Third Generation
4G	Fourth Generation
5G	Fifth Generation
ACK	Acknowledgement
AES	Advanced Encryption Standard
AP	Access Point
ARP	Address Resolution Protocol
ARQ	Automated Repeat Request
CPU	Central Processing Unit
CFDP	CCSDS File Delivery Protocol
CSSDS	Consultative Committee for Space Data Systems
DHCP	Dynamic Host Configuration Protocol
DoE	Departent of Examination
DoS	Denial of service attack
DDoS	Distributed denial-of-service attack
DNS	Domain Name System
DNSSEC	Domain Name System Security Extensions
DTB	Delay Tolerant Bulk
DTN	Delay Tolerant Network

DTNRG	Delay Tolerant Networking Research Group
DVD	Digital Versatile Disc
EVM	Electronic Voting Machine
GPG	GNU Privacy Guard
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IOPS	Input/Output Operations Per Second
IP	Internet Protocol
IPV4	Internet Protocol Version 4
IPV6	Internet Protocol Version 6
ITIL	Information Technology Infrastructure Library
ITU	International Telecommunication Union
NASA	The National Aeronautics and Space Administration
OSI	Open Systems Interconnection
PII	Personally Identifiable Information
PKI	Public Key Infrastructure
RAM	Random Access Memory
RSA	Rivest-Shamir-Adleman Algorith
SNC	Saami Network Connectivity
SSL	Secure Sockets Layer
SYN	Synchronize
TCP	Transmission Control Protocol
TLS	Transport Layer Security
UDP	User Datagram Protocol
USB	Universal Serial Bus
VPN	Virtual Private Network

Wi-Fi	IEEE 802.11 standards (Wi-Fi Technology)

Chapter 1

INTRODUCTION

1.1 Overview

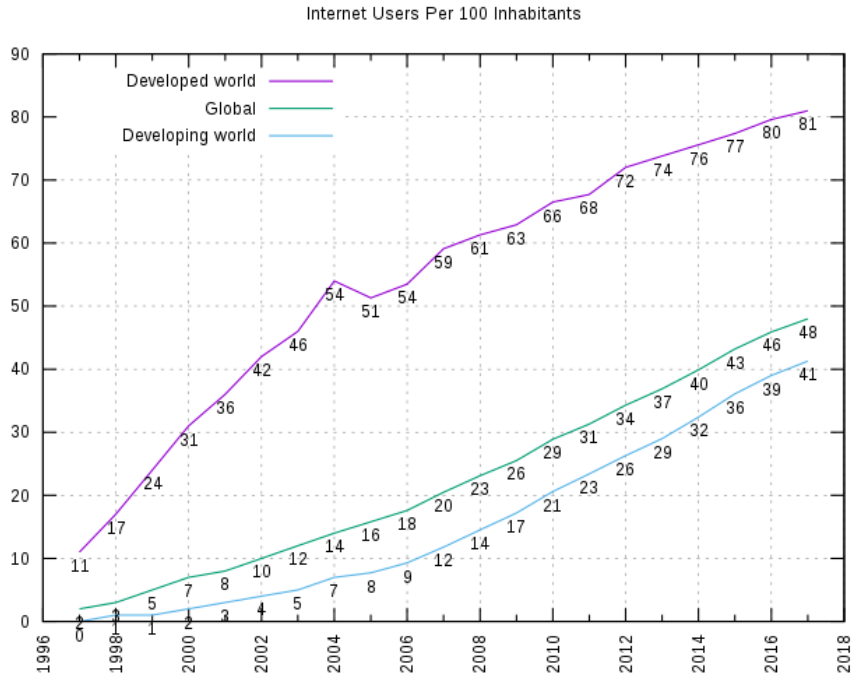
In this chapter, the background to the research, the motivation, problem, objectives and the scope as well as the limitations are outlined. An introduction to this thesis forms the concluding section of this chapter.

1.2 Background to the Research Study

Since the workable prototype on the Internet was released as the Advanced Research Projects Agency Network (ARPANET) in 1969, the Internet has evolved rapidly [1]. Global Internet usage is still under 50% [2] even though half a century has passed since the very first message was sent in ARPANET. As shown in figure: 1.1, more than 50% of the world is either offline or under disrupted connectivity. This could be due to either technical or geographical issues.

Any country or region can be offline at any time due to natural disasters such as tsunami. For example, In 2004, communication network in coastal areas of Sri Lanka badly damaged, and it took several days to recover the telecommunication. Replacement of the access network delayed till the transport network repaired [3]. It is highly essential to find a secure solution to establish communication within a disrupted and disconnected environment.

Delay Tolerant Network (DTN) provides connectivity with characteristics of disconnections, disruption and large delays to areas where no proper conventional connectivity infrastructure such as ADSL, Fiber, Wi-Fi, 2G, 3G, etc. are available. For any given pair of nodes, the round trip time is higher and thus there is a high chance of packet loss as there is no end to end connectivity between all nodes in the DTN.



Source: https://en.wikipedia.org/wiki/Global_Internet_usage

Figure 1.1: Internet users per 100 inhabitants

1.3 Motivation

1.3.1 Process of Online Examination in remote regions

Conducting an online examination and evaluation in a remote area, especially in a totally offline situation or with disrupted communication is a challenge. For example, conducting an online examination in a situation where the examination paper originates (Department of Examinations), examination centers and evaluation centers are not connected through regular communication media such as copper or fiber cables, Wi-Fi, microwave, is further challengeable.

As depicted in Figure: 1.2, during an island-wide examination there are multiple examination centers across the country. In order to conduct the examination, each examination center should receive examination papers in (digital format) and guidelines securely from the origin, and once the examination is successfully conducted examination data (questions, answers, etc) should be securely transferred to an evaluation center. Logical representation of the mobility of nodes depicted in Figure: 1.3.

Once the evaluation process is completed at evaluation centers, the evaluation center will then securely transfer its data i.e: examination papers, answers and results back to the Department of Examination. As both examination centers and evaluation centers are in a disconnected network, where remote back-up over the network is not available, it is necessary to look for alternative

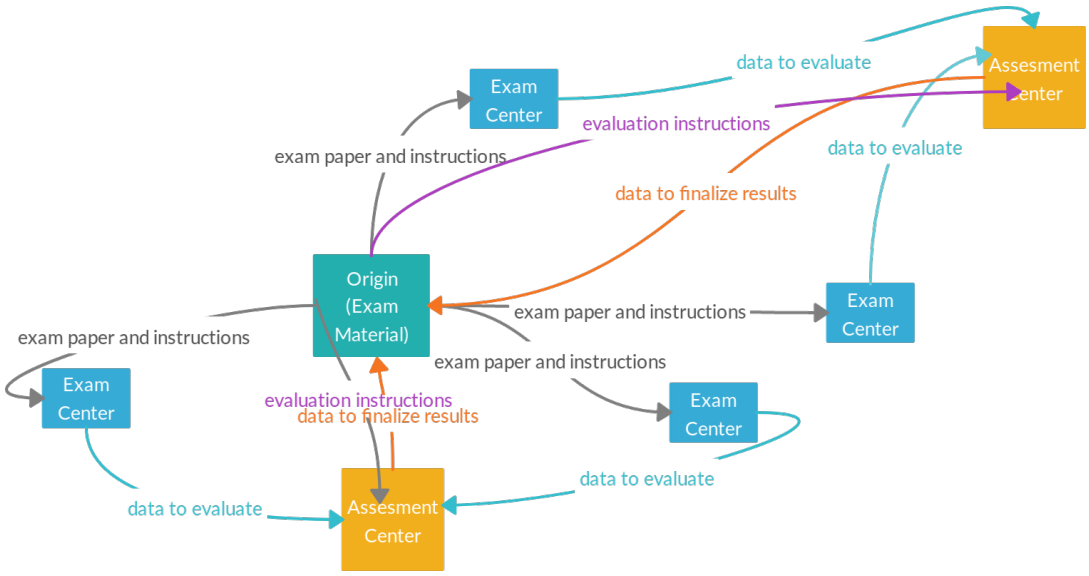


Figure 1.2: Examination and evaluation process of Department of Examination

options such as physical data transfer between the given two centers.

The backing up to a portable storage device and physically transferring is extremely faster compared to the backing up over regular networks. In case of a disaster situation, resuming the operation in different examination centers is possible. Moreover, candidates will be redirected to the nearest examination center in case of a full malfunction at a particular examination center.

As given in the Figure: 1.3, mobility of the examination related data transmit from one node to another. The examination papers (digitized) and guidelines move from the origin (DoE) to examination center and then examinations papers along with answers transmit to assessment centers.

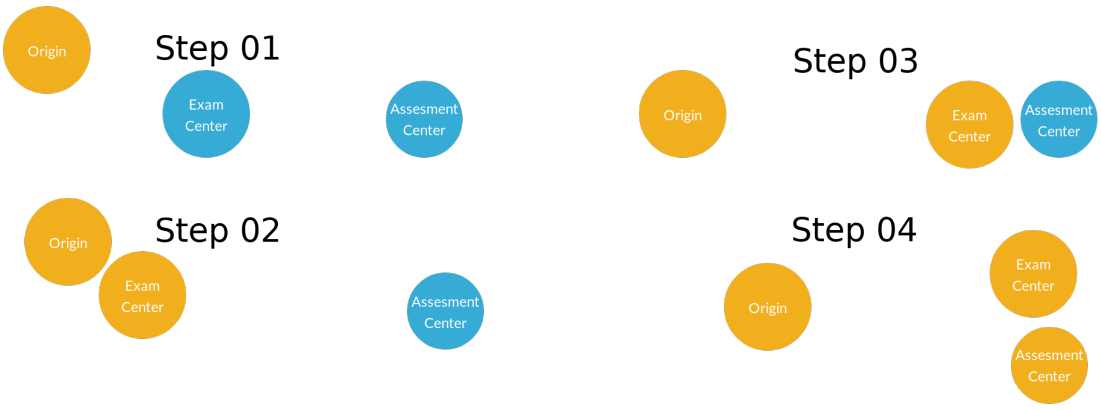


Figure 1.3: Mobility of the Nodes

1.3.2 Deploying and Running Disaster Management System in Remote Area under Disrupted Connectivity

During a disaster, it is obvious that a community can be isolated from the rest of the world but still different kinds of supportive services are required to run until the situation settles down. Supportive services include,

- Keeping track of casualties, deaths, and citizens with special attention or medial requirements.
- Keep track of medical supplies including medicine.
- Keep track of human resource as well as relief items and vehicles.
- Tracking daily status in the environment and the community for future requirements.
- Keep track of food and sanitary requirements.

The above-listed activities can be handled using a Disaster Management System which runs on top of Delay Tolerant Network (DTN). Even though the community is isolated due to a disaster or naturally isolated from the rest of the world, still the data/information in the Disaster Management System can be synced to another location leveraging DTN capabilities.

1.3.3 Deploy Health System to Support Remote Health Camps

Many governments and non-government organizations host health camps in remote areas across the country during a disaster. These camps can be either temporary or permanent depending on the situation. Secured Delay Tolerant Networks are still the best call to maintain sensitive data of both patients and staff while synchronizing data periodically with the Ministry of Health or relevant organizations.

1.3.4 Conducting an Election in Remote Areas Using Information System

Similarly, an automated election voting system can be deployed to run and return election results from a particular community back to the Election Commission Office. In addition to counting of votes, it will also enable systems such as election supportive activities. For example, logging online complaints by end-users and managing assets related to the voting center.

1.3.5 Public Administration System for Isolated Rural Communities

Public administration is one of the most useful services just like education and health services. In order to engage rural communities with efficient public administration, it requires the release of e-Services where remote communities are able to leverage Delay Tolerant Networks to experience the service at doorstep.

1.3.6 Military Intelligence Systems

Military units can be operated remotely to gather both intelligence and classified information. This requires feeding into an Intelligence Management System which usually is hosted at a different location. There is a high risk of transferring sensitive data over the public internet. To send any kind of data between two locations, source and destination should have end-to-end connectivity, but there is a greater risk that the remote location will be out of regular connectivity.

Intelligence data can be audio, video, detailed maps, images, or text files and total size can be very large. During a secret mission, it is highly critical to send this information without compromising confidentiality, integrity and authenticity. Above mentioned issues can be overcome by leveraging Delay Tolerant Networks to secure transmission of huge discrete data sets.

1.3.7 Systems for Irrigation, Power, Agriculture Stations

Due to the availability of cheap lands or safety concerns, most of the projects such as Irrigation, Power and Agriculture usually operate in remote areas where regular communication may not be available at all. But still, project progress may be required to update their respective zonal level office. Delay Tolerant Networks is still a valid option as long as real-time synchronization of information is not required. However, these applications require security, but existing Delay Tolerant Networks require adequate security to achieve confidentiality, authenticity and integrity.

However these applications require security but existing Delay Tolerant Networks require adequate security to achieve confidentiality, authenticity, authentication, integrity. Out of above listed examples, the main motivation to conduct a secure Opportunistic Network to run an online examination which can have a huge impact on the community in terms of faster result release while preserving the secrecy of the examination.

But its really worth to build a generic secure protocol that can be use to achieve any of the above listed use-case while achieving confidentiality, integrity, availability.

1.4 Research Problem

How to provide Confidentiality, Integrity, Availability to conduct an examination in a fully disconnected and disrupted environment.

1.5 Objective

Propose a security protocol to mitigate security issues using necessary and appropriate physical, administrative and technical controls to deliver an examination in a disrupted and disconnected environment.

1.6 Scope and Limitation

The system will be designed for an environment which completely offline or with disrupted Internet connectivity. The protocol will be design to support an unlimited number of nodes connect in different routing levels. However, the initial system will be tested for 10 nodes operating in 3 routing levels.

1.7 Overview of the Thesis

Chapter 1 INTRODUCTION This chapter introduces the motivation, problem, objectives and the scope as well as the limitations.

Chapter 2 LITERATURE REVIEW This chapter describes the related researches, technologies, procedures, as well as existing products solutions. Moreover, secure implementations of services in similar solutions from the different domains (Electronic Voting Machine in India) also captured in chapter 2.

CHAPTER 3 METHODOLOGY This chapter outlines the methods adopted in this study. There were three pilot examinations followed by user feedback are detailed in this chapter.

CHAPTER 4 PROTOCOL DESIGN The design chapter discusses the protocol design. This chapter includes secure design concepts such as Threat Modelling, Level 3 Data Flow Diagram, Risk Assessment. Moreover, this chapter describes the detailed design of the proposed secure protocol.

CHAPTER 5 IMPLEMENTATION Under the implementation, the chapter discusses the implementation, which has been already done to test the proposed solution.

CHAPTER 6 EVALUATION In order to ensure the quality and functionality of the proposed approach, testing of the protocol is most important. The purpose of having testing is to make sure that the proposed solution works as expected.

CHAPTER 7 CONCLUSION AND FUTURE WORK This chapter describes the results of the proposed solution and future enhancements that can be done.

1.8 Summary

Global internet usage is still under 50% even though half a century has passed since the introduction of ARPANET. Delay Tolerant Network provides is an alternative to conventional communication method. DTN provides connectivity to with characteristics of disconnections, disruptions and large delays to areas where Fiber, ADSL, Wi-Fi does not available.

There is a need to conduct computer-based examinations and no one should left behind due to issues with the last mile access. It is necessary to have a secure protocol to deliver an examination confidentially with integrity and availability.

In the next chapter, Chapter 2, researcher will review the literature related to computer-based examinations and security aspects. Further, next chapter discuss about legal background for computer-based examination.

Chapter 2

LITERATURE REVIEW

2.1 Overview

This chapter discusses the background and aspects related to conducting online examinations over a disconnected or disrupted network. Initially, it provides an overview of the Internet communication followed by communication technologies used, related issues and community projects of disrupted networks. The next section discusses the storage media and data security requirements for confidentiality and integrity. Then the following section focuses on conducting an online examination, storage solutions and electronic voting machine used in India under existing solutions. The final section of this chapter discusses related laws and regulations.

2.2 Internet

Internet and digital communication continued to grow with the introduction of Transport Control Protocol and Internet Protocol (TCP/IP) by Robert Kahn and Vinton Cerf in 1970 [4]. The TCP leads to communication among the devices across the regions and the growth of communication among different communities. Communication of the Internet powered by packet switching where the individual packet can be routed from the source to destination independent of the route of each packet.

The following are the characteristics of usable Internet [5] as given by the figure: 2.1 there are several reasons to not being able to access usable internet.

1. End-to-end connectivity

2. Short round trips

3. Symmetric data rates

4. Low error rates

To conduct an online examination, we need to consider the connectivity between the online examination server to the student system and make sure there won't be any connectivity interruptions during the examination period. As most of the remote school labs experience connectivity issues, especially good internet access, it is highly essential to find out possible options for conducting an examination where conventional communication technologies does not exist or are not affordable.

2.3 Challenges in Accessing Internet

As mentioned in the introduction chapter, 1.1, over 50% of the world population or around 4 billion people [6] is still having connectivity issues and it has been confirmed in a press release of the International Telecommunication Union (ITU) in early 2018. Moreover, in the same press release, it has been mentioned that the United Nations Broadband Commission for Sustainable Development has set seven ambitious targets in support of "Connecting the Other Half" of the world's population [7] .

As per a white paper by the World Economic Forum under the title of "Internet for All, A Framework for Accelerating Internet Access and Adoption" which focuses on addressing barriers on providing internet for all and also discusses developing replicable and scalable models. So, it is evident that internet access is not available for all, and it has been acknowledged by the global community, including responsible organizations such as the World Economic Forum. As depicted in the following diagram, the key issues affecting the access of the internet according to the white paper by World Economic Forum [8]are as follows. Among the list of the problems, infrastructure is one affecting about 4 billion people with regard to the internet accessibility given by the figure: 2.1.

2.4 Delay Tolerant/Disrupted Networks

Reliable data transmission is the key to the operation of most of the applications where all transmitted data should successfully be delivered to the destination. In the case of lost data Automated Repeat Request (ARQ) handles it which is supported by the Transport Control Protocol (TCP).

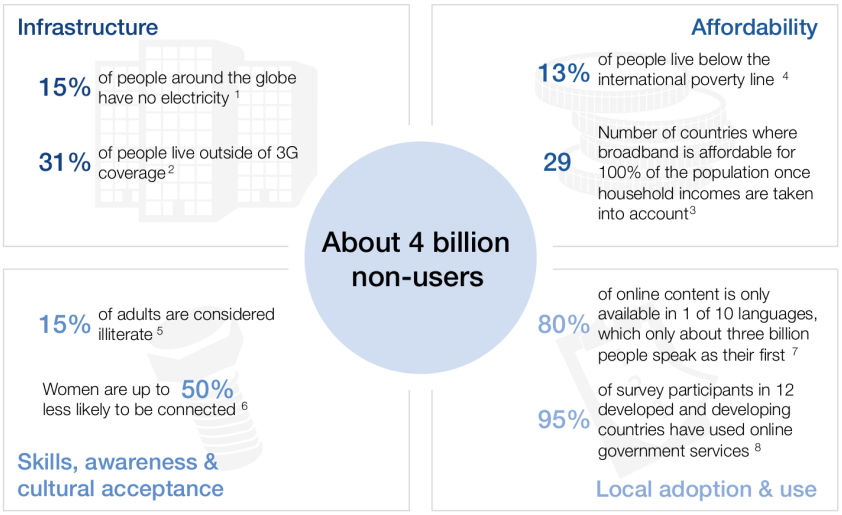


Figure 2.1: Internet Accessibility Challenges

Unfortunately, TCP is not suitable for communication over intermittent connections and with high propagation latency.

These issues have been considered when scientists were planning to take control of a robotic meteorological station on the planet Mars where the Interplanetary Internet originated [9].

Compared to conventional communication technology such as 2G, 3G, Optical Fiber, Wi-Fi, etc., the Delay-Tolerant Network has the several characteristics that explain under section 2.4.1.

2.4.1 Characteristics of Delay and Disruption Tolerant Networks

F Warthman [5], have discussed the following characteristics of the Delay Tolerant Networks in his tutorial about Delay and Disruption Tolerant Networks.

Intermittent Connectivity: In a situation where there is no proper end-to-end connectivity between source and destination (network partitioning), that makes the well-known TCP/IP protocol not exist.

Lengthy or Variable Latency: Internet protocols and applications that depend on the fast return of data or acknowledgement fail due to end-to-end path delays. Path delays consist of several latency issues, including propagation latency in between nodes and variable queuing latency.

Asymmetric Data Rates: There is moderate level support on Asymmetric Data Rates on the Internet. For example, ADSL and cable TV service provide asymmetric data rates, but it is at a moderate level. The TCP protocol is an interactive protocol that requires several signalling round-trips.

High Error Rates: In case of an error on links, it is required to either correction or retransmission of the complete packet. Error correction requires more processing and bits, and also

retransmission ended up with more network traffic. In DTN environment, less retransmission is required for hop-by-hop retransmission than for Internet type end-to-end retransmission.

2.4.2 Delay Tolerant Bulk (DTB) Data

N. Laoutaris et. al., have discussed Delay-Tolerant Bulk (DTB) data transfer over the Internet [10]. There are several factors considered including timezone differences. Concerning this research, there is a possibility of transferring bulk data over public Internet if the source (examination center server) able to find end-to-end connectivity with a server at the Department of Examinations. There are multiple possibilities of making a secure transmission from the remote server to the server at DoE. Sending encrypted data over VPN is the most secured approached or sending encrypted files using rsync over ssh is also possible. A scheduled job can handle this work when connectivity establishes between two ends. This solution can use as an add-on feature though it is not possible to implement in an entirely disconnected environment.

Many usable DTN based community projects out there and few of them discussed under next sub-section.

2.4.3 DTN Based Community Projects

There are several community projects deployed around the world by leveraging characteristics of Delay Tolerant Networks to connect disconnected communities with the rest of the world.

2.4.3.1 BusNet

KD Zoysa et. al., have discussed about a sensor network that build over a public transport system [11]. A few sensors mounted on top of public transport buses to monitor environmental pollution. Instead of using conventional sensor network that require, BusNet able to capture environmental pollution data using a few sensors. The BusNet research team claim that the solution is low cost and easy to manage. In away BusNet has transformed the public transport network into a communication network.

2.4.3.2 DakNet

DakNet [12] is founded by Richard Fletcher and Amir Alexander Hasson and which was transferring data via links in between portable storage known as Mobile Access Point (MAP), kiosks (interactive computer terminal). Mobile Access Point is mounted on a vehicle such as a bus, car,

or a two-wheeler such as a motorbike or a cycle. MAPs are supposed to physically move between communication devices, including kiosks where data moves along with the storage between two booths.

2.4.3.3 ZebraNet

ZebraNet [13][14] originated in Kenya to support Biologists in the Mpla Research Center the purpose of which was to track the position of a Zebra (in the sample) every 3 minutes and then transfer logs back to the base station via peer-to-peer connection among nodes (customized tracking collars). These customized collars consist of GPS, Small CPU, Flash Memory and Wireless Transceivers. Peer-to-peer communication overcomes the connectivity issue with conventional communication such as mobile networks within the area of extended animal migration monitors.

2.4.3.4 TurtleNet

TurtleNet [15] is a mobile sensor network based on DNT. It was deployed in August 2008 to study Gopher tortoises which are native to the Southeastern United States. A customized tracking device is placed on top of the tortoiseshell. This device consists of GPS, battery, solar panel, and communication devices to reach neighbour nodes as it is supposed to communicate opportunistically to transfer data between nodes instead of direct connection to the base station. In addition to tracking movements of Gopher tortoises, these devices have sensors which are capable of readings including GPS, temperature, battery consumption and solar energy harvest.

2.4.3.5 Saami Network Connectivity

Saami Network Connectivity (SNC) [16] was initiated to provide internet connectivity to the Saami Community of Reindeer Herders who are traditionally nomadic residents of Sąpmi. As the communication in northern regions where the Saami Reindeer herders occupied has intermittent connectivity leads to issues with a round-trip time of TCP. This project leveraged the benefit of the Delay-Tolerant Networking, which initially came from the Interplanetary Internet (IPN) Research Group.

2.4.3.6 Wizzy Digital Currier Service

In early 2003, Wizzy Digital Currier service was started to provide low-cost internet access in South Africa. The basic concept is to physically transfer data using USB sticks from a remote

school in a rural area to a city. Wizzy Digital Currier transports the USB storage using a motorbike which takes a few hours to reach the nearest town with high-speed internet. Even though it is possible to establish a satellite connection or microwave connection between a rural school and the city, it is more expensive than transporting a USB storage by motorbike. This solution is acceptable as long as the school can tolerate the delay of a few hours of transport time. In the case of corrupted data in the USB storage, the motorbike has to ride back to the city and return with a new copy of the data.

2.4.4 Bundle Protocol

The Delay Tolerant Network Research Group (DTNRG) has developed the Delay Tolerant Network Bundle protocol architecture given in figure: 2.2. DTNRG originated in discussions surrounding the inadequacies of TCP/IP for deep-space and interplanetary communications. Still, it has become a focal point for standardizing overlay technologies that address disconnected network environments on Earth as well. Internet's packet-based communication assembles data into packets, separates them, and transmits them to an endpoint that the protocol assumes is always connected.

The bundle layer is the overlay layer that DTNRG's Fall references. It sits between the transport layer and application layer of the various discrete networks the DTN bridges.

Since this solution is focusing on an entirely disconnected network, there is no use of the usual system, transport, and link-layer. Still, we use the physical layer via the Universal Serial Bus (BUS) port. Bundling everything all together makes it possible to transfer data between different entities during an exam. This is a possible solution that can be implemented with added security by enabling encryption and signature.

Marcin Nagy has discussed a protocol stack in his doctoral dissertation under the title of "Secure and Usable Services in Opportunistic Networks" [17].

2.5 Portable Storage Options (USB Storage Device)

In 2000 Ishrali company [18] introduced the USB memory device which was based on the floating-gate transistor. Over the years significant advancement has led to produce a USB device

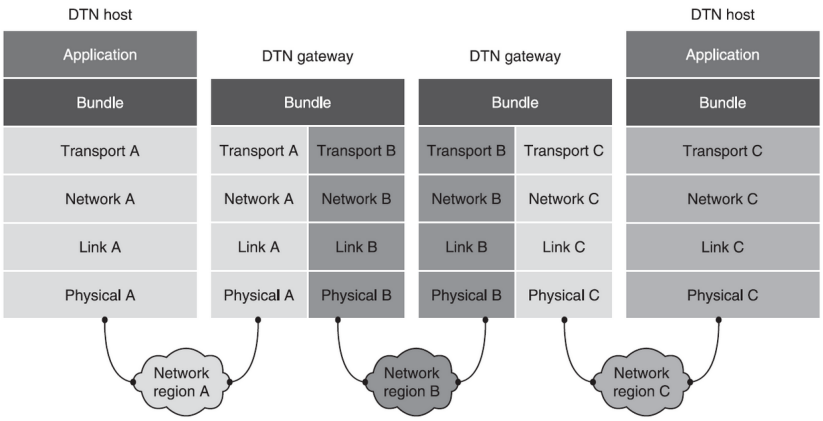


Figure 2.2: Bundle Protocol by Delay Tolerant Network Research Group (DTNRG)

which is pretty easy to handle including plug and play nature, read and write data, faster data transfer and the portability. All of these features, including high portability, are the reason for USB storage devices becoming the most widely used storage solution [19].

The USB drive is capable of storing different types of data, and it mainly uses data storage, data backup and live booting of Operating Systems too.

Handling of USB devices (pen drives) is more convenient due to its portability and it is even suitable when distributing to remote areas where no proper transportation is available. Since a USB device is a commodity product as well as an affordable solution, it is feasible to use the additional USB device in case a particular USB device is lost during the operation or in other words as a stand by the device.

A couple of conference papers acknowledged the possibility of use of USB devices as a communication technologies under DNT environment. Back in 2004, A South Africa based the Wizzy Digital Courier service (explained above) used to connect remote village schools using a portable USB storage device [20]. The USB storage device which has been carried physically to the student terminals [21].

2.5.1 Security of Content in an USB Device

To secure the content within the USB storage, data can be compressed and then encrypted before transferring data into the USB storage device. Both encryption and decryption can be implemented in either the Operating System level or Application level.

In a situation where USB devices are used to store and transfer sensitive data, it is highly essential to maintain the confidentiality, integrity and authenticity. It is necessary to keep the content stored in the USB device as encrypted, signed and hashed.

2.5.2 USBs with Hardware Encryption

Hardware encrypted USB drives are available in the market with military-grade encryption standards. USBs with built-in Hardware encryption release the burden of handling encryption and decryption at either Operating System-level or Application level. It can be plugged into any device and used as long as encryption-key is remembered but no need to maintain specific applications to handle the encryption and decryption.

On the other hand hardware, encrypted USBs are not widely used and not affordable.

Source: https://static.bhphoto.com

Figure 2.3: Hardware Encrypted USB

2.5.3 Dissimilar Redundancy

It is always good to have redundancy to minimize the risk by having a failover option. Despite the nonrecurring costs, having redundancy with diversifying devices is further reduced by mitigating the risk related to the failure of both options due to a similar fault (common-mode failures) in both primary and failover options [22].

Having USB storage devices with different chipset is much better than having the same type of USB storage devices. When backing up data as either failure to write the backup files into devices or failure to read from the devices is critical to the examination process as well as an evaluation process.

2.5.4 Data Retention Policy

Generally available USB storage devices are cheaper and able to be re-used in the long run under proper data retention policy where previously-stored content should be safely wiped out from the device after copying into secure archive storage.

Generally, examination answer papers should be available for a five year period. An online examination has to follow general examination guidelines and that demands a secure archive to maintain a given data set for at least a five year time period. Based on this requirement, it is essential to estimate how much secure archive storage is required and the cost incurred.

2.6 Data, Data Life Cycle and Data Security

The data is one of the critical assets of an organization; it is highly essential to safeguard data from all kinds of threats using suitable countermeasures. Protecting Organization's data has a direct impact on intellectual property, customer information, Organization's brand, etc. Besides, regulations and laws demand data security such as General Data Protection Regulation (GDPR) security requirements, that went in the European Economic Area (EEA) in 2018, to make the privacy rights of the residents in the European Economic Area [23].

Data classification is also essential when it comes to Data Security, Risk Management and Compliance. Data classification can be done based on several levels of sensitivity, value, criticality and impact to the Organization. Moreover, the classification of data is helping to define what baseline security controls are necessary, adequate and appropriate to safeguard given data. It is essential to classify all organization data into one of the following sensitivity levels listed below.

1. Restricted Data

   Restricted data can be classified as data that has "High Level" of impact which results from unauthorized disclosure, modification or deletion of data in an organization. For example, unauthorized modification of an examination paper or disclosure of personal information of a candidate has an impact on the restricted data of the examination system.

2. Private Data

   Private data can be classified as data that has a "Moderate level" of impact to an organization which results from unauthorized disclosure, modification or deletion of a data. Most of the time, private data belongs to the Organization itself and does not classify under restricted or public data. Still, a considerable level of security countermeasures applies to safeguard private data.

3. Public Data

Public data can be classified as data that has a “Low level” of risk to an organization which results from unauthorized disclosure, modification or deletion of data. Still, there is a possibility for the public image of an Organization to be damaged by any alteration or deletion of publicly available data. For example, in case of an intruder deleting or modifying publicly available examination results can cause an availability and integrity issue with respect to the examination results respectively. Confidentiality, Integrity and Availability are the essential security triad required for any system (including online examination system) that demands information security. There should be necessary and adequate protection required to safeguard public data.

As explained above, it is essential to protect all three classified types of data within an organization with the use of relevant countermeasures.

2.6.1 Data Life Cycle

The Data Life Cycle is a sequence of stages that the data unit goes through from its initial stage to final stage. It is essential to get a better understanding of the Data Life Cycle to find out necessary and adequate countermeasures at each stage of a data unit to confirm integrity, confidentiality and availability of data is preserved.

Figure 2.4: Data Life Cycle

2.6.2 Data Security

Qionglu Zhang et. al., has discussed achieving the data confidentiality and security using plausible deniability and securing deletion within a single system. Despite the usage of plausibly deniable encryption within an online examination, that paper has been highlighted the importance of maintaining confidentiality with encryption along with secure deletion. There is no point in secure deletion of data if the confidentiality been compromised before the secure deletion takes place. Similarly, there is no point in putting efforts to secure confidentially of the data if an advisory can be able to recover deleted data.

It is highly relevant to consider data security during each stage of the data life cycle as much as possible to safeguard sensitive data. All sensitive data should be encrypted during the creation, storage, use, transfer and archive while secure deletion should be guaranteed at the end [24].

2.7 Existing Solutions

There are several existing solutions are discussed under this section including AWS Snowball (under sub-section 2.7.1), Electronic Voting Machine (EVM) of India (under sub-section 2.7.2) is a solution that leverage the benefit of physical, administrative and technical controls. Under sub-section 2.7.3, benefit of the Moodle is discuss, which is an existing software solution to assessing and evaluation of learning. Last sub-section 2.7.4, discusses about the Safe Examination Browser.

2.7.1 Transfer Bulk Data with AWS Snowball

Amazon Web Service Snowball [25][26] is a secure method to migrate bulk data from one place to another which has several variants listed below.

1. AWS Snowball
2. AWS Snowball Edge
3. AWS Snowmobile

Unfortunately, this solution is not a generic solution and expensive for transferring data sets which is less than 100GB. When considering the physical size of the storage to be moved from one location to another, especially from one examination center to another, it won't be scalable with hundreds of examination centers. Moreover, this could be even difficult with a redundant

Figure 2.5: AWS Snowball

copy for each examination center. Further this solution is not cost-effective, and the size of the minimum data set is beyond the requirement as well.

2.7.2 Electronic Voting Machine (EVM) of India

Even though the Examination and Election process is under different domains, the implementation of the Electronic Voting Machine system across India is somewhat relevant. Electronic Voting Machine is a transformation from paper-based voting in the traditional ballot system to Electronic Voting Machine based system is worth studying as it also uses a mix of physical, administrative and technical controls to ensure confidentiality, integrity and availability of the election voting machine. Electronic Voting Machine is more convenient to deploy across the country including remote areas as a standalone system without conventional communication technologies.

Having the second highest world population, 1.42bn, India is the largest democracy in the world so their election process is worth studying under the current context. Citizens above 18 years old are eligible to vote, but they should have their names listed under the electoral roll prepared by the Election Commission, India. Making this electoral roll at national level is a tedious process and requires door to door enumeration visits. The Election Commission has the authority to schedule the election eventually. Registered voters are supposed to turn up at centres on the day, prove their identity before casting their vote. Once done, they are marked with a colored finger tip. Casted vote is recorded on the balloting unit of Electronic Voting Machines (EVM). Casting the vote is by pressing a button in an electronic voting machine against an identified or chosed candidate. [27].

According to S. Chauhan et.al., the EVM currently used in India was developed in 1990.

Figure 2.6: Electronic Voting Machine in India

Likewise, EVM was introduced to the nation in 1998 and it has been used in all the state and national elections since then. Indian authorities observe higher rates of voter participation, reduced cost of production and better accessibility to remote communities following the introduction of EVMs to the country. They produce faster results too[27].

Properties of the Electronic Voting Machines of India discuss under section 2.7.2.1.

2.7.2.1 Properties of EVM

Electronic Voting Machines have several notable properties that are listed below [28].

1. Accuracy

   Accuracy in EVM means that it should be impossible to change a casting vote, remove a validated vote from the final count or count an invalid vote into the final result

2. Authentication

   Only legit (users who are eligible to vote) voters can vote and make sure they can vote only once.

3. Privacy

   Privacy is one of the critical aspects of an election voting system. Nobody can map a given vote (ballot) to a voter and also voters not able to prove to whom s/he voted.

4. Verifiability

It is possible to verify all votes have been counted correctly, and this can be independently verified by anyone.

5. Availability

   The EVM system should be up and running throughout the voting period without any disruption, and the voter can access the system during any given time within the time of poll stands.

6. Resume Ability

   The EVM system is allowing to resume voting for those who had interruptions during the voting time as long as the voting period still valid.

The Election Commission of India has been published a broucher of the EVM [29] with details of it's components, Countermeasures and how the randomization of the process.

2.7.2.2 Components

Electronic Voting Machines of India has three components, shown in the figure: 2.6. The Control Unit (CU) is used by the presiding officer and the rest of the two components, Ballot Unit (BU) and the Voter Verifiable Paper Audit Trail (VVPAT) kept in the voting compartment.

The VVPAT has been introduced to add an additional level of transparency and credibility by letting voters verify their votes are cast as expected. The VVPAT is printed and displays a slip for about 7 seconds which includes the serial number, name and symbol of the candidate. After 7 seconds slip falls into the sealed box in VVPAT. This slip remains sealed and it can be audited by the court. Generally during each election these slips from 5 polling stations are randomly selected to count and match with the EVM count [28].

2.7.2.3 Randomization

The EVMs and VVPATs are allocated randomly to Assembly Constituencies and to polling stations through EVM Management System developed by Election Commission of India (ECI). This process is done in the presence of political parties and candidates [28].

2.7.2.4 Witnessed by Stakeholders

One of the best aspects of the EVM system is that stakeholders such as political parties and candidates take part in the commissioning process by participating at the first level of checking the EVM and VVPAT [28].

2.7.3 Moodle for Online examinations

Examinations play a major role in assessing and evaluation of learning. It is a great way to assess what students have learned, as well as the strengths and weaknesses of individual students. Besides, teachers can evaluate for themselves the interest and remembered parts of the lesson, since examinations are conducted in an environment where students attempt individually, it's a better way to discover how students think to argue and think logically under pressure. Moreover, teachers can use assessments and evaluations as feedback to improve their own teaching methods [30].

2.7.3.1 Powered by Open Source Community

Moodle is an Open Source Software (released under GPLv3+) [31] which was originally developed by Martin Dougiamas. A recent stable release (Moodle 3.8) recorded nearly 400,000 downloads [32]. Moodle also ships with major Linux distributions such as Fedora, Debian, Ubuntu and CentOS. Moodle can be deployed with major Open Source web servers, i.e. Apache httpd or Nginx and with major Open Source database servers such as MySQL, MariaDB and PostgreSQL and PHP. As of now, over 1600 plugins have been developed by the Moodle plugin development community of nearly 1000 contributors. Nearly 700,000 total number of plugins which have been downloaded as per the Moodle plugin portal [33].

Ria Mae H. Borromeo has done a study on the use of Moodle for Online examinations for distance educators [34]. As per the results of his research, several types of questions have been identified as suitable for examination and also teachers were interested in security features such as session locking where the user is lockdown into the browser and not able to use other applications. In the later part of this chapter, this feature is described under section 2.7.4. Moreover, identification of students as well as proctoring them has been highlighted in the results of the study. In case of examination is conducted in an examination center where the candidate has to be there in person physically, both identification and proctoring can execute accurately and efficiently. During a connectivity outage, its impossible to monitor activities of the candidate but physical proctoring has no such interruptions.

As a product which widely used, stable and vibrant community support, Moodle is well suitable for conducting Online Exam.

2.7.3.2 Assessment with Moodle

Online Assessment should have primary components listed below [35].

1. **Question bank**

   Question banks consist of question definitions and contexts. Those question definitions have been organized into categories.

2. **Question engine**

   A question engine is a subsystem to manage the execution of question definitions. When some attempt a question definitions in the question bank turn in to an interactive experience.

3. **Quiz, and other activities**

   To teach and assess students, particular activity is required. Activity use questions from the question bank while executed by the question engine.

2.7.3.3 Moodle Question Types

As mentioned below, there are standard question types in Moodle. For additional requirements its possible to create a question type plugin.

- Calculated question types:
  - Calculated
  - Calculated multi-choice
  - Calculated simple
- Drag and drop question types:
  - Drag and drop into text
  - Drag and drop markers
  - Drag and drop onto image
- Other question types:
  - Description
  - Essay
  - Matching
  - Embedded Answers (Cloze Test / Gap Fill)
  - Multiple choice

- Short Answer
- Numerical
- Random short-answer matching
- Select missing words
- True/False

2.7.3.4 User Study on Moodle

Based on a study using civil engineering, it has been found that Moodle quizzes are able to transfer and assess engineering knowledge [36].

2.7.4 Safe Examination Browser

Safe Examination Browser (SEB) [37] is an Open Source Software (released under Mozilla Public License) [38] being developed and maintained by the Educational Development and Technology unit of ETH Zurich. This web browser enables a safe environment for online examinations. In other words, this software is capable of converting any computer system into a secure and examination friendly system on a temporary basis.

Safe examination Browser has several features, including the ability to disable shortcuts and Operating System functions such as Task Manager. It prevents accessing the internet during an examination and controls the use of additional applications from the base Operating System. SET browser is able to integrate with Moodle

Next section is discusses about the legal background for the conduct a computer based examination in the context of Sri Lankan law.

2.8 Legal Background

The legal background of the public examinations in Sri Lanka dates back to the year 1968. The public examinations act No 2 of 1968, is an act to make more effective provisions for the proper conduct of public examinations, for the punishment of offences committed in connection with such public examinations, and for all matters connected therewith or incidental thereto according to its long title[39]. It establishes a “Commissioner of Examination” and an “Advisory Committee”. It has also created examination related offences and provided for the penalties. Section 6 of the Act provided the question papers to be “Secret Documents”, and that status

prevails until the lapse of a half an hour for the scheduled time of the commencement of the examination. In this context, any examination related system, whether manual or "digital" needs to be capable of maintaining the "Secret" status of the document. The divulging of information related to examinations is also an offence under section 7 of the Act, and the theft or disposal of such secret documents is presented from section 8. Although it was enacted for non-digital methods, the most important sections for the "digital" examination systems would be the section 9 and 10 where it deals with the instances of Destruction or tampering with secret document and the Fraudulent misdelivery of secret documents. Use of fake documents is also an offence under section 14. Divulging of information relating to examiners, and dishonest transmission of answer scripts was made offences under section 13. Additionally, section 18 provides those offences to be cognizable offences, which means that peace officers can arrest the offenders without a warrant.

In summary, any digital system deals with a public examination in Sri Lanka need to adhere to the Public Examinations Act, No. 25 of 1968. The system must be capable of maintaining the confidentiality and integrity of the examination related information and the aspects such as network, operating system and application security need to be maintained. However, the "documents" defined in the Public Examinations Act, No. 25 of 1968 refers to "hard copy", "tangible" documents and, whether the digital documents, information and data messages are fallen within this definition needed to be sorted out.

The Evidence (Special Provisions) Act of 1995[40] and Chapter V of the Electronic Transactions Act of 2006[41] provides the legal basis to the reception of electronic and computer evidence in civil and criminal proceedings. Therefore, the provisions of those acts make the digital information related to public examinations to be interpreted as "Secret documents" in Public Examinations Act, No. 25 of 1968. Electronic Transactions Act did not repeal any provision of the Evidence (Special Provisions) Act and it is expressly mentioned that nothing contained in the Evidence (Special Provisions) Act "shall apply to and in relation to any data message, electronic document, electronic record or other documents" to which the provisions of this Act applies.[42].

Marsoof[42] explains that the Evidence (Special Provisions) Act of 1995 and Chapter V of the Electronic Transactions Act have facilitated the reception of electronic and computer evidence by removing or modifying obstacles and difficulties which hitherto prevented the admission of such evidence. However, he further argues that the most crucial issue is whether the recording was altered or tampered with in any manner to affect its authenticity and reliability. Marsoof[42] establishes that, in the case of computer evidence, the issue that is vital is whether

the information supplied to the computer was accurate and whether the statement produced by the computer is derived from such information. Therefore, the examination related "digital" systems need to take care of those aspects. Marsoof[42] argues that It is vital to develop the necessary skills among the relevant professionals and necessary equipment and infrastructure when it comes to electronic evidence in the legal world.

According to the literature, although there are unresolved minor issues in the information communication technology-related legal system in Sri Lanka [42], the existing legal framework is sufficient to implement the provisions of, the public examinations act No 2 of 1968, for establishing any "digital" system for examination in Sri Lanka.

The Personal Data Protection Act is not available as of now, but the bill is yet to be passed by the Parliament of Sri Lanka. Once the Act is operational, it should be applied when the Department of Examination is keeping personal data of candidates, examiners and any other party [43].

In case of misconduct or criminal case related to a computer based examination, digital evidence is highly essential when in reconstructing information in a manner that ensures the admissibility of collected evidence in a court of law. Next section discusses about the importance of a computer-based examination.

2.9 Forensic Readiness

Digital forensics is a subset or a branch of forensic science where recovery and investigation of digital material found in digital devices such as computers, mobiles, routers, storage devices. A forensic investigation takes place after a serious information security incident as a post-event response to support a legal process. Ability to gather evidence and securely preserve them with standards of admissibility before an incident is a definite advance for an organization.

Digital evidence play a major role in following list of scenarios [44]:

- Disputed transactions
- Allegations of employee misconduct
- Legal and regulatory compliance
- Avoidance of negligence and breach-of-contract charges
- Assisting law enforcement investigations

- Meeting disclosure requirements in civil claims
- Supporting insurance claims after a loss occurs

Forensics readiness is about the ability to use legally admissible digital evidence when required by targeting increasing the possibilities of collect and preserve digital evidence with a minimum investigation cost. Robert Rowlingson has been discussed ten steps process for forensic readiness along with cost and benefits [45].

It is highly essential to enable digital forensic readiness for digital examination environment despite the communication technologies used within the system. Both conventional and delay-tolerant systems should enable forensics readiness. There are several activities to convert an organization to a digital forensics ready environment. Create and enforce related policies including data retention policies, and enable them with standards, guidelines and best practices. Provide adequate training for the relevant staff, identify and capture relevant logs with correct timestamps and time zones, maintain access logs are some tasks required to follow when initiating a forensics ready environment.

2.9.1 Operating System

Ewa Huebner et. al, has discussed how the Operating System deals with computer forensics. For example, Linux file systems with Journaling feature make a fast recovery in the event of a system or power failure. Data acquisition and analysis is another area in which the Operating System supports in computer forensics. [46]

2.9.2 Logs

Logs are one of the most essential and critical parts of a system and enable the forensics ready of the system. It is required to identify required logs for the running system in order to provide technical support as well as, for investigations at the post-event stage.

There are different logs available and some of them automatically generated by the Operating System, Application and some of them required to generate by the customized processes or cron jobs.

- User logins
- System start, shutdown and reboots
- Backup logs

- Web server (apache httpd) logs
- Database server (mariadb) logs
- Application server (moodle) logs
- Audit/Security logs
- Health checks

Both the timestamp of the log and as well as the system time should be set with the correct local time zone. Since the examination server is supposed to run independently in a remote station as the server, it is essential to set log to rotate in a manner that excess logs won't fill the disk. Disk capacity plan requires to consider the size of total logs and plan ahead. Moreover, it is important to avoid accidental deletion of sensitive or critical logs.

2.9.3 Host Based Intrusion Detection (HIDS)

Despite the fact that the system is running in a remote location, it is required to monitor and log the malicious behaviour of the server. An Intrusion Detection System (IDS) can detect changes and threats to the system. A host-based IDS is an IDS that monitors the server on which it is installed.

2.10 Incident Management

Incident Management is a day to day process that targets to manage the Life Cycle of all incidents, including unplanned interruptions. Incident Management restores an acceptable service with a minimal impact to the business after an incident occurred. Dr B.C. Potgieter et. al, have discussed that Information Technology Infrastructure Library (ITIL) framework has an impact on both customer satisfaction and operational performance [47].

An examination should deliver with no or minimum interruptions to stakeholders, including candidates and examiners. It is highly essential to have a mechanism to minimize all kinds of incidents that occur during the examination period.

2.11 Social Engineering Attacks

Social Engineering attacks are one of the most dangerous attacks in the world as they can threaten all systems and networks. Despite the technology used to secure intrusion detection systems,

anti-virus, firewalls and cryptography solutions, Social Engineering uses the weakest link "Humans". Due to the nature of humans tend to trust other humans which is less with technology. It is possible to divulge confidential information or bypass security measures by influence a person psychologically but not so with technology.

Fatima Salahdine et. al., have discussed the above-mentioned issue providing a detailed survey about social engineering along with classifications, detection strategies, and prevention procedures [48].

An online examination has higher participation of humans as well as the system has sensitive assets such as examination paper and examination results and Personally Identifiable Information (PII) to protect. So there is a high possibility of social engineering attacks during the entire process of the examination, and it is essential to use security measures to protect sensitive data even after the exam.

Personally Identifiable Information (PII) to protect, it is highly essential to take necessary actions to prevent social engineering attacks during the entire process of the examination as well as the organization should use security measures to protect sensitive data even after the exam.

There are a lot of Social Engineering attacks, and few of them are discussed below.

Unwanted tech support: Attacker trick the victim into divulging their login information by posing as a tech support person.

Pretexting Attack uses a fabricated scenario or good pretext to trick victim's personal information and use it to commit identity theft.

Vishing attack are about the use of Social Engineering over voice calls to collect personal or financial information. This attack can be used as attackers for reconnaissance purposes.

Smishing attack is a portmanteau of the Short Message Services (SMS). In Smishing attacks victim is tricked into downloading malware or a Trojan horse into mobile.

Tailgating Attacks tricks an employee into gaining access to unauthorized premises by following behind authorized people. For example, the unauthorized person accesses the restricted area of an organization by following an authorized officer.

2.12 Zero Trust

Zero Trust is a security concept, and it is about "Never Trust, Always Verify". In 2010, John Kindervag created the Zero Trust, which is a strategic initiative to leverage micro-segmentation and granular perimeter enforcement to prevent data breaches. In the Zero Trust architecture model, organizations never trust anything either within or outside its perimeters. Instead, it

continues to verify everything that connects to the system.

Andreas Gutmann et. al., have discussed ZeTA protocol for the Zero Trust Authentication. The Zeta protocol is about challenging people to either confirm or deny related attributes of their secrets, instead of challenging them to remember long secrets or conduct mathematical operations [49].

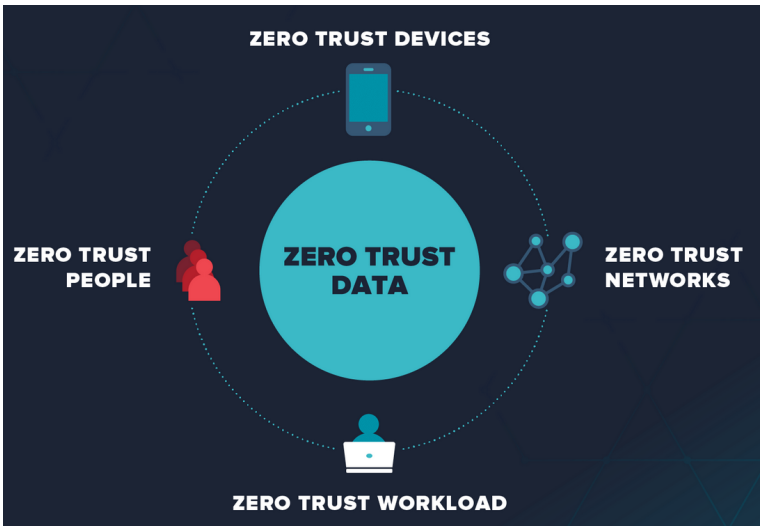


Figure 2.7: Zero Trust

2.13 Secure Code Review

Secure code review is about auditing the source code of an application. The main objective is to verify if the application has been implemented proper security controls and working as intended. Moreover, security controls have been implemented or invoked in all the right places. Secure code review is how we can ensure that the application has been developed in a way that "self-defending" in its given environment.

There should be a mechanism to assure that developers are following secure development practices and techniques. Security Code Review is the best method to assure if security application developers are following secure development techniques. Once we do proper secure code review, a penetration test should not discover any additional application vulnerabilities relating to the developed code.

Fixing application vulnerabilities after releasing make total cost ownership higher as well as it will poorly reflect the product brand image in case of severe impact due to the exploitation of such vulnerability. Secure Code Review reduce the risk of failing the application, damage to organization business, loss of data such as either PII, examination paper or examination results.

2.14 Towards a Secure Protocol to Conduct an Online examination in Disrupted and Disconnected Environment

Education is a human right [50] and reflected in international law in Article 26 of the Universal Declaration of Human Rights and Articles 13 and 14 of the International Covenant on Economic, Social and Cultural Rights. Examinations are a great way to access what the students have learned with regards to a particular subject. Traditional mechanism of delivering an examination is paper-based but it has been adopted over the years to digital form. The transition from pen and paper-based examination model digitized examination has several requirements including composing questions in digital format and delivering them securely. Despite the last mile access of the candidate, examination should be equal and available to all the candidates to have a fair examination.

As mentioned in the Section: 2.4.1, DTN characteristics well fit with conducting of an examination in a remote area. If a single examination backup file corrupted, they were only required to re-transmit a new backup file from the origin of the corrupted file. Alternatively, if a server crashed or an examination was being disrupted, only the particular examination center has to re-schedule the examination.

The reviewed literature provides knowledge of Delay Tolerance Environments and possible and affordable solutions to transmit data securely. Moreover, the literature on Electronic Voting Machines in India provides in-depth knowledge on how to leverage the physical, administrative and technological controls in order to keep the confidentiality, integrity and availability of a system which operate in parallel in remote areas without conventional communication. Further, this literature also provides the classification of data and security measures to protect sensitive data.

2.15 Summary

Challenges of accessing Internet and alternative solution which is DNT have been discussed. Further, discussed DTN based community projects, possible solutions to data transfer and data security. The EVM of India have been discussed in detail as the EVM project provides mixture of administrative, physical and technical controls to conduct an election. Legal background about conducting a computer-based examination highly essential and discussed in this chapter. This chapter ends with a need for a secure protocol to conduct online examination in disconnected and disrupted environment.

In the next chapter, Chapter 3, the methodology used to conduct the research study are discussed in detail.s

Chapter 3

METHODOLOGY AND APPROACHES

3.1 Overview

This chapter discusses an overview of the stages of the research. It also provides a detailed discussion on how the research was conducted.

3.2 Purpose of the research

The purpose of this research is to propose a security protocol to mitigate security issues using necessary and appropriate physical, administrative and technical controls to deliver an examination in a disrupted and disconnected environment

3.3 Action Research

Action Research is well suitable to solve real-world problems while observing the experience of solving the problem [51] and improve it simultaneously. Till it reaches the most appropriate solution, n number of iterations of the action research cycle was continued. It has several stages including planning, acting, observing, improving and reflecting.

3.3.1 Iteration I

Initial iteration started with setting up an online examination (first pilot test) and letting the students and teachers to get connected to a central server over the Internet. The assessment questions including MCQ and structured questions, have been created confidentially and securely loaded to a Moodle server. Candidates had no time limitations or session restrictions during this iter-

ation as the main objective was to identify if they had any connectivity issues with the central server.

At the end of the first pilot exam, a survey was carried out among teachers who participated as examination staff as well as the representatives of their students. Survey questions available under Appendix:B and related results are discussed in the Chapter 6-Evaluation.

3.3.2 Iteration II

During the first iteration, disruptions were observed, and it was decided to build a standalone server which runs locally in each school. The primary purpose of this standalone server is to authenticate users and run the Moodle application locally where no internet connection is required to conduct the examination.

Purchasing several hundred of servers is not affordable to the Department of Examinations while distributing them across the country is a complicated task for each examination. Converting existing infrastructure into a standalone server is pretty much convenient to teachers if they have a customized operating system with all required applications/packages and services.

A customized Linux ISO created including all required applications and a mock exam. Installation DVDs were shared with teachers across the country. Around 2000 DVDs have been distributed (in addition to hosted ISO files) along with an installation guide in English medium.

At the end of the second iteration, a survey was carried out among ICT teachers as the representative of their students. Survey questions available under Appendix:B and related results are discussed in the Chapter 6-Evaluation. Considering the results of the survey and the observations of the second iteration, the third iteration is planned and executed as explained in the next sub-section.

3.3.3 Iteration III

During the second iteration, disruptions and performance were observed. Moreover, a survey has been conducted among ICT teachers who involved with the second iteration.

The third iteration was planned with added security controls to the standalone server. To address the power outage issue, which was caused due to regional scheduled maintenance of the National Power Grid, the responsibility was given to the Coordination Center/Zonal Education Office to communicate with the supplier and reschedule maintenance.

The significant change of the 3rd iteration was the introduction of physical, administrative and technical control to the standalone server to maintain confidentiality, integrity and availabil-

ity. In the previous iteration, students connected to a server were deployed at their school ICT lab and they conducted the examination under the supervision of their class teacher. The 3rd iteration was almost similar to an official exam. Admissions were issued to students for the 3rd iteration and official examiners conducted the examinations during the scheduled examination period.

This iteration consists with two parts namely Iteration III - A and Iteration III - B. During the third iteration it was observed initial approach was not appropriate due to the performance issues and then switched to an alternative approach (Iteration III - B). Both approaches described below.

Iteration III - A

At the early stage of the third iteration, it was planned to use a USB Pen drive as the standalone server storage disk in order to avoid the difficulties of installation of customized GNU/Linux systems. The USB drive was plugged into a computer and installed the examination server Operating System into the USB drive (using USB drive as the storage disk). After creation of the USB drive as the storage drive of the server, it can easily convert any computer as the examination server. It was a matter of plugin the USB drive into any computer and reboot it. There was no requirement as such of installing hundreds of servers across the country.

Iteration III - B

After observing the Iteration - III-A, it was found a performance issue that discussed under the Evaluation Chapter.

Considering the technical difficulties and the high chances of human error, it was continued to seek an appropriate method. It was decided to replace the use of the in-memory system by installing each local server using an installation media (Install DVD or USB) with the help of a technical team.

At the end of the third iteration, a survey was carried out among teachers who participated as examination staff as well as the representatives of their students. Survey questions available under Appendix:C and related results are discussed in the Chapter 6-Evaluation.

Technical Support

Technical Support included in the third iteration as well to make sure any technical issues are sorted out as soon as possible. This technical support is in addition to the installation of the local servers.

3.4 Secure by Design

Protocol design was started with the principle of "Secure by Design", which includes Keep security simple, Defence in-depth, The Least privilege, Secure defaults, Fail securely, minimize the attack surface area, Fix security issues correctly, Separation of duties and avoid security by obscurity. Moreover, Threat Modelling was done to identify and understand potential threats related to the design and prioritize mitigation actions.

Next chapter will discuss the design in more details including successful attempts to meet the Principal of secure by design.

3.5 Threat Modelling

Threat Modelling is used to identify and understand threats as well as the mitigation options to secure digital assets. It also facilitates prioritizing security solutions. Moreover, it helps reduce the overhead to the QA team by reducing the number of development related bugs in advance. Major concern here is to reduce the total cost of development as fixing bugs after project release is expensive than fixing them at the early stage.

Since the examination centers located across the country it take time to distribute software security fixes after initial release. On going examinations should not disrupted due to security updates or any fixes. Level 3 DFD diagram have used to Threat Model with STRIDE and discussed under Section: 4.3.2 in Chapter 4-Protocol Design.

3.6 Risk Assessment

Risk Assessment is one of the vital methods that identifies and assesses vulnerabilities and threats against assets. One must ensure that necessary and appropriate risk treatment options should be implemented using administrative, physical and technical controls in order to mitigate identified risks. Verification of no missing necessary control is still available.

In other words, Risk Assessment facilitates to understand the risk and its potential impact upon objectives of designing the protocol. It is essential to determine and agree on which assets and threats to consider which determines the scope of the protocol.

A Risk Assessment has been conducted against this system and results of the Risk Assessment is discussed under the Chapter 4-Protocol Design and the Risk Assessment table is available under the Section: 4.3.3.

3.7 Interviews

In order to acquire domain knowledge, a series of face-to-face interviews conducted with relevant staff of the Department of Examinations. The main intention was to understand the operation of related processes, associated risks and process owners.

3.8 Surveys

Several surveys were conducted at the end of each iteration mentioned in the section: 3.3.1 as well as after the final implementation. As the users are located across the country, surveys were conducted using Google Forms. Survey questions are available under Appendix:A, Appendix:B, Appendix:C and Appendix:D.

3.9 Journaling

The researcher used several types of journaling methods throughout the research and each is described below.

3.9.1 Notebook

A notebook was used to sketch ideas and make notes during the meetings, interviews. Later, important issues, ideas, solutions were transferred to related tools such as Trello, code repository and issue tracker.

3.9.2 Audio Notes

Most of the interviews and discussions were recorded and kept as audio notes under pre-approvals and consents of the other party. Discussions with the project supervisor and consultant, interviews with stakeholders of the GIT online examination were recorded for the ease of reference during the research project.

3.9.3 Trello

In 2011, Trello has been created by Fog Creek Software, which is now a subsidiary of well known Atlassian. Trello is a Kanban-style web-based application. Very early in the research project, Trello was introduced to the Department of Examinations, to have better project management and

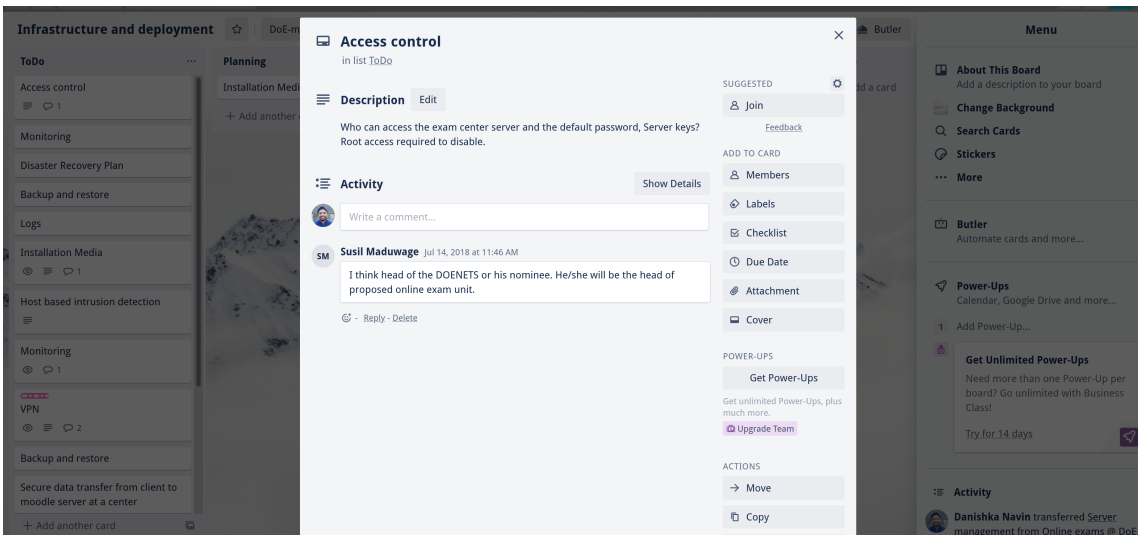


Figure 3.1: Trello for Project Management and Task Management

task management during GIT Online Examination. Just like the Department of Examinations, the researcher continued to use the Trello throughout this research project.

3.9.4 Bitbucket Repository and Issue Tracking

Issues (1–25 of 49)

Title	T	P	Status	Votes	Assignee	Created	Updated
#53: Restore process			NEW		Danishka Navin	2019-12-24	2019-12-24
#2: Backup moodle database			OPEN		Danishka Navin	2018-10-29	2019-10-08
#3: Backup moodle server			OPEN		Danishka Navin	2018-11-10	2019-10-08
#52: Authenticate backup files			NEW		Danishka Navin	2019-08-09	2019-08-09
#51: Server hardening			NEW		Danishka Navin	2019-08-06	2019-08-06
#50: Passwordless encryption for disks			NEW			2019-07-29	2019-07-29
#49: Encrypt USB with LUKS			NEW		Danishka Navin	2019-07-29	2019-07-29
#48: Auto backup in to USB storage			OPEN		Danishka Navin	2019-05-02	2019-05-09
#39: Timeouts in moodle			OPEN		Danishka Navin	2019-01-14	2019-01-31
#46: Capacity planning, tuning MariaDB			OPEN		Danishka Navin	2019-01-21	2019-01-27
#45: Harden httpd and mariadb			OPEN		Danishka Navin	2019-01-18	2019-01-27
#27: httpd and moodle performance tuning			OPEN		Danishka Navin	2018-12-21	2019-01-27
#47: MachineID and BootID			NEW		Danishka Navin	2019-01-25	2019-01-25
#8: Verify synchronized content			NEW		Danishka Navin	2018-11-10	2019-01-18
#28: Mariadb errors and warnings			OPEN		Danishka Navin	2018-12-24	2019-01-18
#44: Collect logs in remote serers			NEW		Danishka Navin	2019-01-15	2019-01-15
#43: Create sanity script to finalize			NEW		Danishka Navin	2019-01-15	2019-01-15
#42: Enable Log Rotate			NEW		Danishka Navin	2019-01-15	2019-01-15
#41: Setup LB and Backup Servers			NEW		Danishka Navin	2019-01-15	2019-01-15

Figure 3.2: Repository

The researcher managed his development work at Bitbucket private repository. Moreover, it used to maintain issues related to the development work under the Bitbucket Issues. As the researcher has already signed a non-disclosure agreement with the Department of the Examina-

tions, the code repository and created issues are left in the private repository.

3.10 Ethics

The researcher does not expose any Personally Identifiable Information of any person or a team during this research and no information will be exposed in the future. He respects the anonymity of all the parties. In the Chapter 6-Evaluation, the researcher discusses survey results by respecting the anonymity of participants. The same principle applies to the development and implementation stages as well.

3.11 Summary

Action research with several iterations followed by a user experience survey used. Information security principals, concepts discussed in this chapter. Further, interviews and risk assessment were also included in the methodology is this research.

In the next chapter, Chapter 4, researcher will discuss the design of the proposed protocol in detail. Level 3 Data Flow Diagram created and used for Treat Modelling prior to the designing of the proposed protocol.

Chapter 4

PROTOCOL DESIGN

4.1 Overview

This chapter presents the design of the security protocol used to conduct online examinations in disrupted and disconnected environments. The design followed the Secure by Design principal. Level Three Data Flow Diagram was used to model the design, and then Threat Modelling was conducted based on the DFD. Then Risk Assessment was conducted to ensure appropriate and necessary security controls used to mitigate identified risks.

4.2 Secure by Design

The protocol design was initiated with the principle of "Secure by Design". The proposed design was modelled using Data Flow Diagram (Level Three) and is discussed under Section: 4.3.1. After modelling the design, the next question was 'What can go wrong? '. Based on the level three Data Flow Diagram, STRIDE based Threat Modelling was done to identify related threats.

4.3 Data Flow Diagram and Threat Modelling

4.3.1 Data Flow Diagram with Trust Boundaries

The Data Flow Diagram represents the processes and functions that create, store, modify and share data through the system. Level Three Data Flow Diagram (DFD) is given in Figure: 4.1. For easy understanding, the main DFD diagram is split into three sections, namely the Department of Examinations (Section A), examination Center (Section B) and Evaluation Center (Section C).

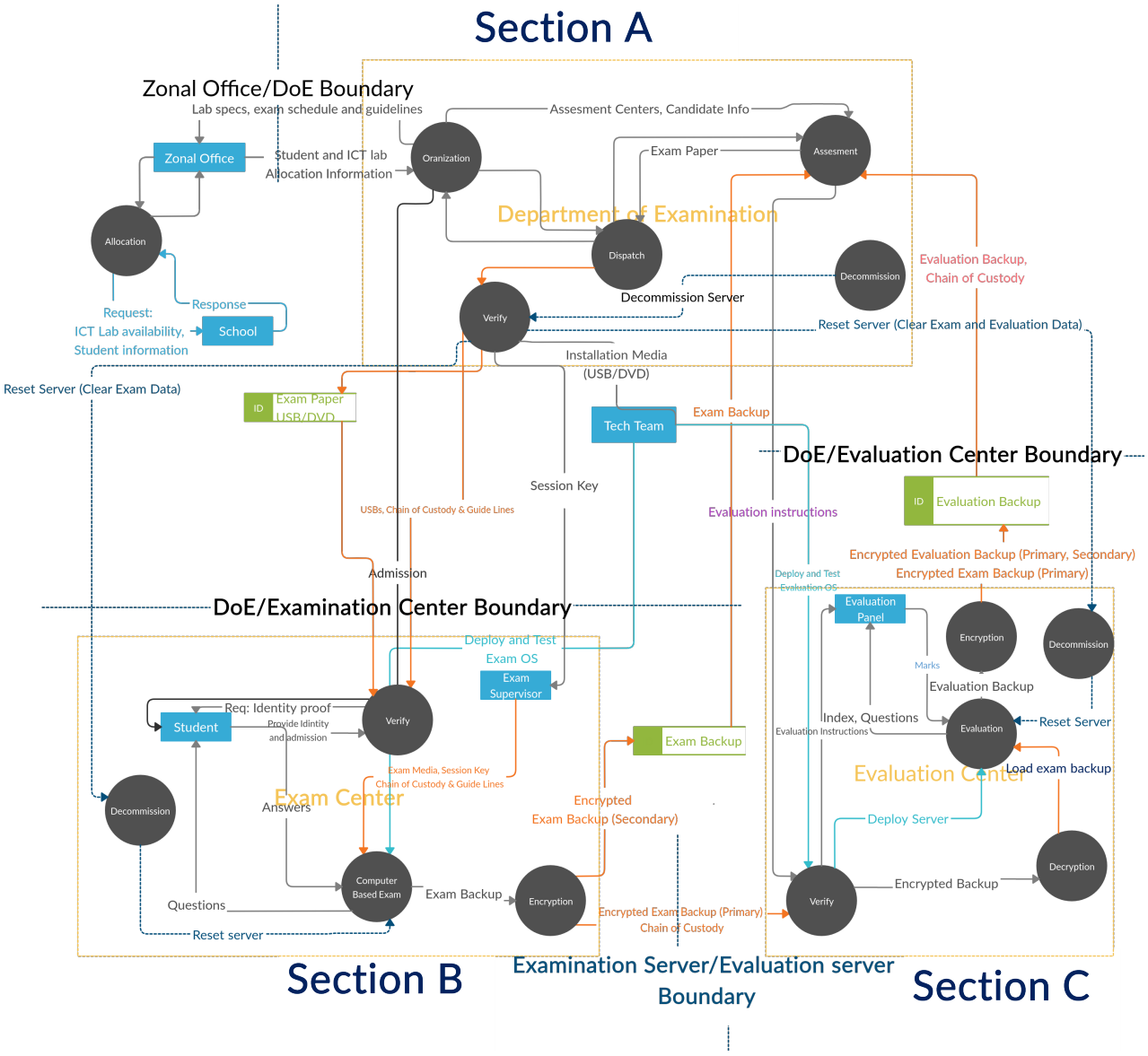


Figure 4.1: Level 3 Data Flow Diagram

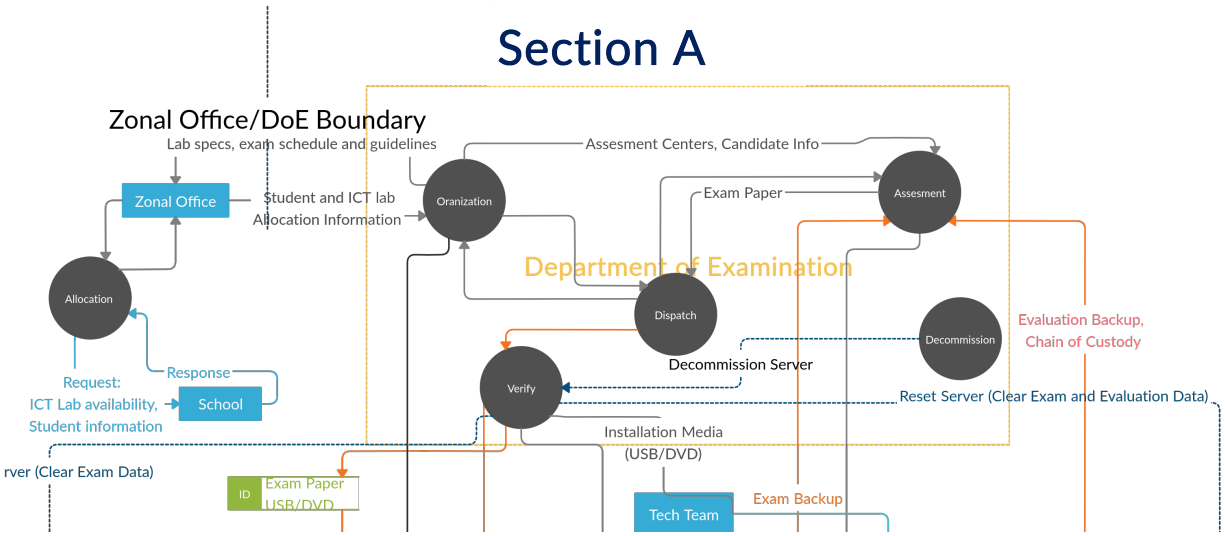


Figure 4.2: Level 3 Data Flow Diagram: Section A

As given in Figure: 4.2, section A represents the Department of Examination and its processes within the DoE 's boundary. The organization, Assessment, Dispatch, Decommission and Verifying processes are within the DoE trust boundary. All the other processes connect to verify processes which play a significant part of the examination as each information sent and received must be verified. In case of verification failure, the other party has to resend or retransmit the information. This process acts as the error checking but not error-correcting. Each process within the DoE trust boundary operates under existing security controls. Organization process handles the allocation of students to examination centers and lists eligible examination centers. Dispatch process is responsible for delivering information securely out of the DoE after verifying the delivery. Assessment process coordinates the entire examination assessment, and it collects the evaluation center and staff information from the organization process. The assessment process is responsible for collecting examination backups from the evaluation centers. And then deliver examination backups to respective evaluation centers after swapping examination backups randomly. After completion of data archival at either examination center or evaluation center, the decommissioning process reset the server. Cancellation of either examination or evaluation is demanded to decommission an examination center. It is also required to decommission a server if it is no longer required due to no further DoE activities to be done in the future.

As per the Figure: 4.3, section B represents processes within the examination center boundary. Several processes within the trust boundary of examination center include verifying, Computer-based examination, Encryption and Decommission. The verification process verifies each information sent and received, and it also verifies human interaction. Students and staff must be

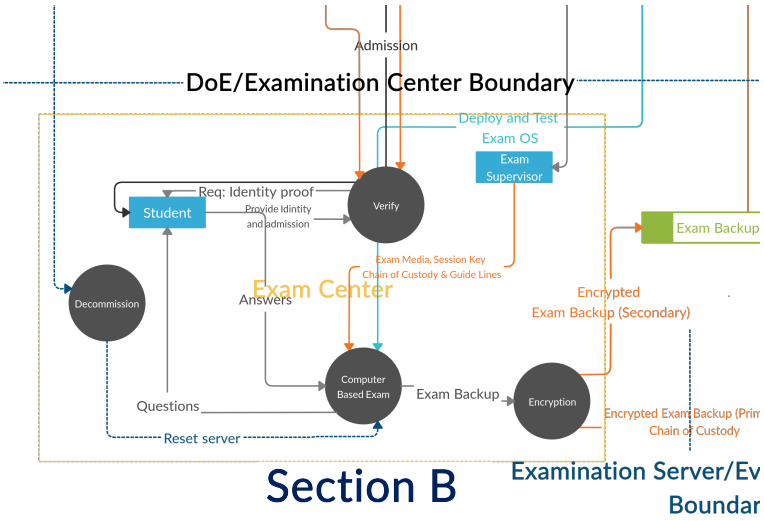


Figure 4.3: Level 3 Data Flow Diagram: Section B

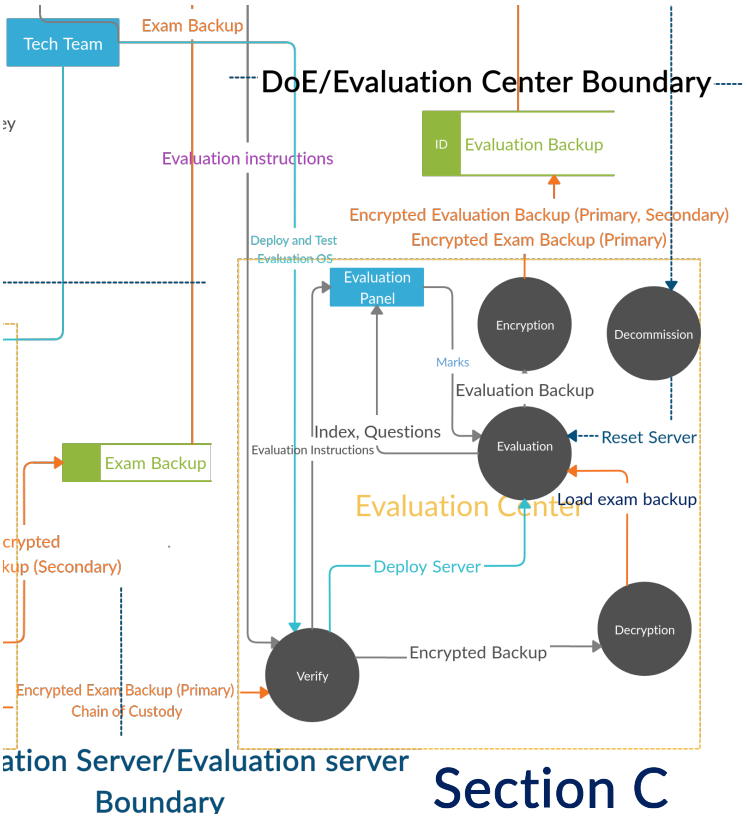


Figure 4.4: Level 3 Data Flow Diagram: Section C

verified before entering into the premises and operating the computers. Examination supervisors use the session key that was received securely via DoE secure delivery to start each examination session. Students must present with a valid admission card and a NIC. Examination server installation media and media with the examination paper must be verified. After completion of the examination, backup is encrypted and sent to the assessment process under the DoE trust boundary.

As given in Figure: 4.4, Similarly the section C, visualizes the processes within the evaluation center boundary. Several processes included within the evaluation center trust boundary including Verify, Evaluation, Encryption, Decryption and Decommission. Every human and information move in and out of the evaluation center trust boundary verified. The examination backup is received from the assessment process of DoE, required to restore after verification. After completion of the evaluation, an encrypted backup (results) is sent back to the DoE. A successful secure data archival required to decommission the evaluation server.

4.3.2 Threat Modelling

Threat modelling was conducted to answer the following questions. The Table: 4.1 represents the result of the Threat Modelling with STRIDE.

1. What are the threats we face?
2. Who are our likely threat actors?
    (a) What are their likely motivations?
    (b) What are their capabilities?
3. What are our vulnerabilities?

Then a Risk Assessment was conducted to identify risk factors, evaluating any associated risks, implementing appropriate and necessary controls to either reduce or remove risks. Despite the time and effort on Threat Modelling and Risk Assessment, it had a high impact on reducing the overall software development process cost. The Secure by Design principle leads to reducing the number of bugs, issues found after the deployment of the project. Due to the nature of examinations, it is hard to fix issues during the examination or evaluation, which severely impact the operation of the examinations and disrupt stakeholders. So, identifying issues at the early stage of the development process was invaluable as it will reduce the disruptions due to the proposed solution and reduce the total cost of ownership.

Table 4.1: STRIDE: Threats and Mitigation Technology

Threat	**Mitigation Technology**	**Solution**
Spoofing	Authentication	Digital Signature, Admission card
Tampering	Integrity, permissions	Digital Signature, Access Control Encryption
Repudiation	Fraud prevention, signatures logging	Chain of Custody, Logging, Attendance Sheet
Information Disclosure	Encryption, separation of duties	OpenPGP
Denial of service	Availability	Stand by resources
Elevation of privilege	Authorization, isolation	separation of duties, privileges, minimum access to servers

4.3.3 Risk Assessment

As mentioned above, Risk Assessment was conducted before moving to further design and development of the proposed solution. Purpose of conducting Risk Assessment was to ensure that necessary and appropriate risk treatment options should be implemented using administrative, physical and technical controls in order to mitigate identified risks. Verification of no missing necessary control is still available. The results of the Risk Assessment is available in the Table: 4.2.

Threat	Vulnerability	Asset	Impact	Likelihood	Risk	Control
Hardware Failure	Aging H/W, non-serviced H/W, Unprotected software controlling H/W	Servers (Critical)	ExamEvaluation service will be unavailable for maximum 15min (Critical)	Low	re-schedule examination session	Use standby server
Power Outage	Lack of UPS, Power Generator	Servers (Critical)	ExamEvaluation service will be unavailable for maximum 15min (Low)	Low	re-schedule examination session	Use UPS system, Power generator, informed regional power distributors about examination schedules to avoid maintenance during exam/evaluation period.
Disk Failure	Old disks, Malware affecting H/W	Backup (Critical)	Cancellation of ongoing exam/evaluation (Low)	Low	re-schedule examination session	Use standby server
Natural Disaster (flood/fire)	System in floodplain, flammable material used inside	Servers (Critical)	Cancellation of ongoing exam/evaluation (Low)	Low	re-schedule examination session	Reschedule exam, evaluation at different center using backups

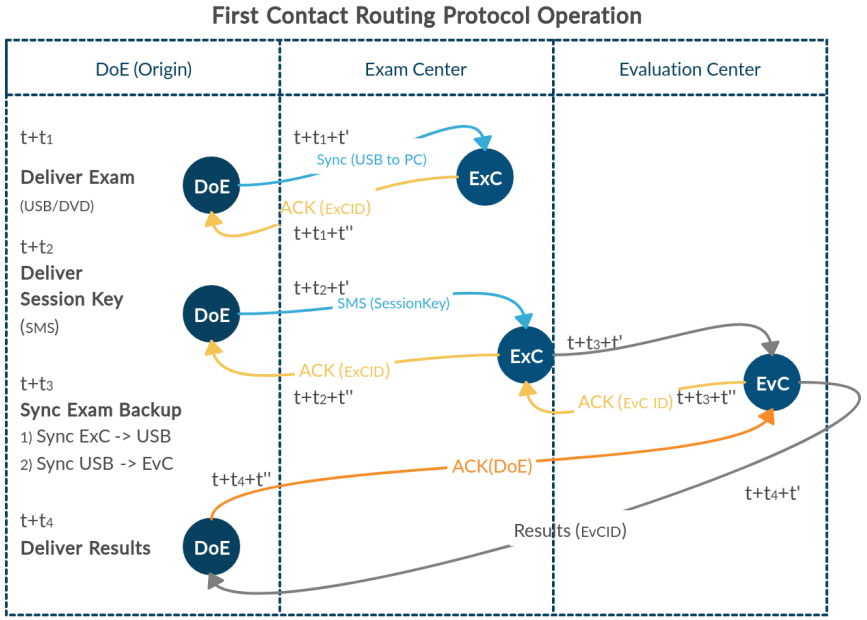


Table: 4.2 Risk Assessment

Threat	Vulnerability	Asset	Impact	Likelihood	Risk	Control
Data breach	Unpatched S/W, vulnerable unpatchable code, Badly written software	examination paper, examination marks (Critical)	examination declared null and void, Some material leaked out	Low	re-schedule examination session	Encryption, Access Control, Information deliver by trusted staff
Impersonate a candidate	Inadequate identity confirmation procedures and/or technology	examination paper (Critical)	Results awarded to wrong individual, fraud	Low	re-schedule examination session	Verify user identity at each stage
Accidental deletion of data	Software faults, Human Error	examination paper, examination marks (Critical)	examination results not available	Low	re-schedule examination session	Frequent Backups
Malicious human	Inadequate security assurance	Servers, LAN (Critical)	Disruption of exam, results collation, marking	Low	re-schedule examination session	Disable Wi-Fi in each exam/evaluation center
Lost Install media	Bad procedures	Encryption Keys (Critical)	Inability to start the paper on time	Low	extend or re-schedule examination session	Implement Chain of Custody, Deliver by trusted staff

Threat	Vulnerability	Asset	Impact	Likelihood	Risk	Control
Introduce fake exam-/evaluation center	Lack of proper assurance process	examination paper/-marks (Critical)	Deprive students of examination opportunity	Low	re-schedule examination session	Examination and evaluation center allocation initiated by the Zonal Education office and verification process exists to remove the threat.

4.4 Holistic View

When the holistic view of the entire examination process is considered, following areas are identified.

1. Recruit Individuals and Teams
2. Establish Trusted Environment
3. Dispatch
4. Preparation
5. Deliver Examination Paper
6. Conduct the Examination
7. Evaluation
8. Deliver Examination Results
9. Decommission

Apart from the areas listed above, Workflow Management was useful to keep track of the status of each activity to be completed in order to proceed at each stage. There were two routing protocols used to facilitate the examination process as well as the evaluation process, which explains in detail under the sub-section: 4.15.

4.5 Selection of Individuals and Establishing Teams

4.5.1 Creation of Roles

Multiple roles were created when considering the holistic view of the entire examination process. A team of several members was deployed for the smooth running of the process. Duties were well-defined and documented under each team member identifying his/her preferred skills.

Following are the list of roles created:

- Question Preparation
- Data Entry (Questions)
- Review Questions

- Bundle Questions to Moodle System
- Creating Packages, Build System, Create ISO, etc
- Examiner
- examination Supervisor
- Evaluation Panel
- Chief of Evaluation Panel
- Technical Team
- Technical Auditors
- Center Managers
- Security
- Courier/Transporter
- examination Organizer
- Dispatch Team
- Assessment Team
- Incident Response Team
- Regional Coordinator
- Service Providers
- Suppliers

In addition to the above-listed roles, the system focuses on the role of the examination candidates as they have physical access to the main examination center where the examination server is physically located.

4.5.2 Screening of Individuals

There was a proper recruitment process for the roles mentioned above, including the screening of individuals for highly confidential activities, and they were requested to sign a Non-Disclosure Agreement (NDA) with the Department of Examination. Each member of the team was equally responsible for assigned activities. However, only the head of the division was accountable for the process, and related activities conducted by his/her team.

Moreover, those who have to work on activities related to technical areas such as server deployment, technical support, including troubleshooting and incident response, were expected to have adequate skills and experience on the domain.

This screening process has a high impact on the authenticity of the examination process.

4.6 Review and Modify Service Level Agreements (SLA), Contracts, Memorandum of Understanding (MoU) and Laws and Regulations

There are multiple supporting services required to conduct a computer-based examination in order to make minimum disruption other than natural disasters. Electricity is a critical factor, and the Department of Examination should have an MoU with such stakeholders in order to minimize the impact on scheduled exams. School ICT labs running without the support of the national power grid (using alternative power sources such as solar power, power generator), are required to conduct proper maintenance in advance. Furthermore, review relevant SLA and MoU with respective parties.

Similarly, SLAs for digital equipment such as Routers, Switches, Uninterruptible Power Systems, PCs, Monitors should be enforced with vendors in advance to be repaired or replacing faulty items if and when necessary. Renting a portable power generator and having enough fuel reduces the risk of disruption of the examination or evaluation process.

Composing a list of contact channels and people is highly essential to respond to an incident during the examination. For example, how and who should be contacted in case of a power outage. The escalation procedure and the response time for such an incident should well be documented.

Moreover, related laws and regulations should be reviewed, and the necessary knowledge should be transferred to relevant teams by conducting workshops and awareness programs in

advance.

4.7 Establish Trusted Environment

4.7.1 Initialization : Selection of Exam/Evaluation Centers

This protocol is dedicated to establishing a trusted environment in order to conduct either examination or evaluation. Alternatively, both processes conducted by maintaining confidentiality, integrity and availability.

First, the Department of Examination should identify suitable examination centers (ICT labs) which already have basic requirements and capacity. For example, wired network connectivity to each PC/Laptop, power supply with USPs systems, number of client machines and servers including stand by systems. Other than the capacity requirement, the ICT lab should be available during the examination or evaluation period.

As depicted in the Figure: 4.5, the Department of Examination (DoE) sends a request to each lab along with an examination code, tentative schedule and the specs and guidelines. Each lab should send an ACK to the DoE with a Board Number (boardno) which is the examination Center ID, availability and status (**active** or **inactive**) of the lab. Once the Department of Examination has updated the received information, it sends an ACK to the examination center and based on the acknowledgement particular lab will be reserved for the upcoming examination using the examination Code (examcode) sent initially.

Specification include the following items:

1. Number of PCs available.
2. Number of Servers available.
3. Electricity Power
4. Capacity of PCs
5. Capacity of Servers
6. Number of UPS

Initialization Protocol supports the identification of available examination centers that fit with the specification provided by the Department of Examination. Next phase, the preparation of the exam, continues only with examination centers that match with given technical spec.

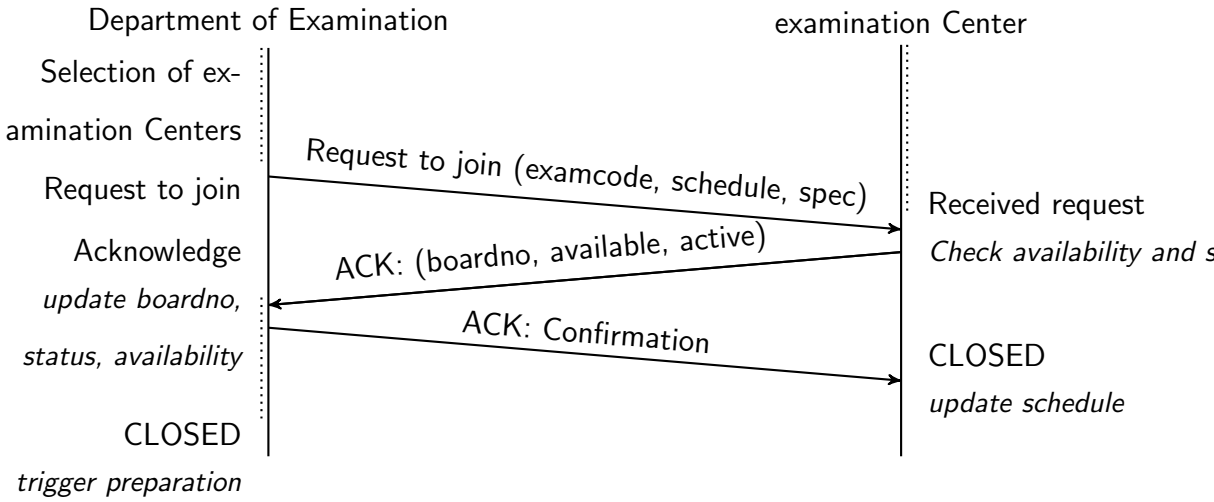


Figure 4.5: Initialization Protocol

4.8 Dispatch

4.8.1 Packaging, Build ISO

This process involves highly confidential work, and the DoE should handle it. All activities should be conducted under both physical and administrative controls in order to maintain the CIA Triad of Confidentiality, Integrity and Availability of the exam. A Senior Administrative Officer should always oversee the activities that take place in an isolated room, without internet access or connectivity to the local area network of the DoE, and only limited physical access is permitted. Physical access is allowed only to limited staff who have already been screened, with their role and access verified and a signed non-disclosure agreement. Each access attempt must be recorded in a logbook under the supervision of a senior officer.

The examination platform and required programs, scripts should be packaged. Packaging of software solutions makes it easier to distribute, update, remove and manage the software that creates specific Operating Systems, for example, Red Hat Enterprise Linux, CentOS, Fedora, Debian, Ubuntu. Moreover, after signing such customized packages, it is possible to verify the packages from the correct source.

Once packaging is done, it is required to build an ISO disk image which will be used to deploy an expected customized Operating System across several remote examination centers and evaluation centers. Since all required applications have been packaged, there will not be any manual installations, upgrades, removals or modifications at remote centers.

The checksum is created at the time of building the ISO image, and that checksum file keeps

the integrity of the DVD ISO image no matter how long it travelled or who keeps the image file or disk.

4.8.2 Compose policies, procedures, standards, guidelines and checklists

Based on the objectives of the Department of Examination, their existing policies should have necessary amendments in order to facilitate computer-based examinations as well as running it across the country in a fully or partially disconnected network. Based on the policies of the DoE, standards should be created or updated in order to implement the policies related to the computer-based exam. There are procedures which consist of detailed step-by-step instructions for a given task, which implements the policy. Guidelines are implementing procedures which consist of administrative instructions or recommendations. Checklists make specific requirements that have been met at a given point. It makes the verification process more manageable and avoids skipping any critical step in the process.

4.8.3 Packing

The staff of the examination Organization Branch plan the entire delivery roadmap and schedules. Following decisions to be made by the examination organization branch.

1. What to deliver?
2. On when it should deliver?
3. To whom it should deliver?
4. How to deliver?
5. When should it collect?
6. How should it collect?

For example, the installation media (DVD/USB) will not be sent early in the process, but it is more than enough for them to be sent after the completion of the initialization phase. The Technical Team should have both installation media and the list of the available exam/evaluation centers to visit in person and validate them. Then deploy the Operating System. Packaging includes security stickers to seal PCs and other required devices.

All the items are packed with waterproof material with a proper tag to identify destination and item code.

4.9 Preparation

After completion of the initialization phase, the DoE will know the number of examination and evaluation centers **available** to proceed with the particular exam. DoE will need to re-run the initialization phase in a set of new exam/evaluation centers or centers which initially failed but have been prepared up to the acceptable level. The latter will be handy in case there was a shortage of examination centers. DoE should always keep several exam/evaluation centers stand by in case of an emergency.

4.9.1 Preparation: Preparation of examination Center

Preparation of the examination center is the next step after the initialization phase. The DoE should send guidelines and a checklist to each examination center. In this stage, the manager of each Computer Center has to be involved in several activities that cover Network Security, Physical Security and Operating System Security of the PCs.

Operating System security includes installing and updating virus guard and OS update in client systems. In addition to updating systems, it is required to create local users and let the system clean up user directories after each reboot to remove any kind of examination materials remaining before the next session. It is about keeping the confidentiality of the exam. Disabling Wi-Fi is a must in order to avoid outsiders breaking into the local network via the Wi-Fi access point. Physical security is about providing security of assets in the examination center.

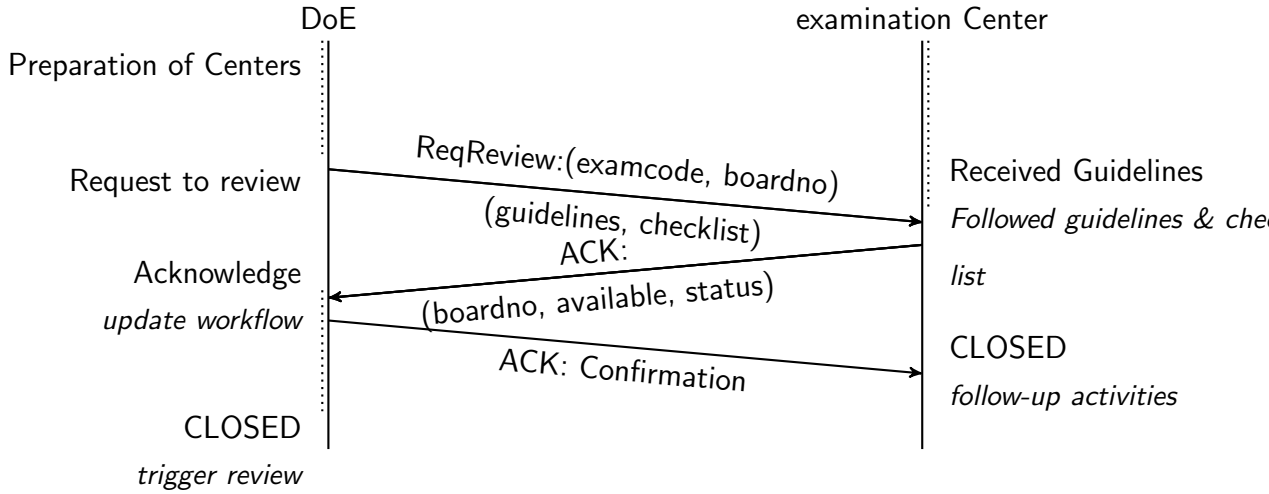


Figure 4.6: Preparation Protocol

4.9.2 Preparation: Review of examination Center and examination Server Deployment

Center Manager confirms the preparation of the examination center, based on given guidelines and review as per the given checklist. Then there will be a separate team that will be visiting the examination center in person to make sure if the manager has reported the actual situation and to find whether there are missing steps still. This is a kind of additional verification that count under administrative controls.

The Technical Team will deploy a customized Operating System (GNU/Linux) which acts as the platform for the questions. That is when the review is complete, and the examination center is maintaining up to given standards and guidelines.

At this phase, the technical team should conduct the following activities. Having a separate team to review and deploy the examination server, that respects the value of separation of duties is paramount. The Technical Team should be with a well-balanced composition of ICT teachers with Hardware, Network and GNU/Linux skills, In-Service Advisor (ISA), and also the Assistant Director in Education who has authority to make decisions.

4.9.2.1 Review the Examination Center

It needs a fresh review of the examination center against the given checklist. Finding any kind of missing physical, administrative or technical controls within the examination centers is vital.

Since this technical team has the authority to make decisions, they will act immediately to fulfil requirements or to sort out issues. In case of a worst-case scenario where they can not resolve the issue, they are supposed to inform the DoE. The Technical Team has the full authority to disqualify any examination center being a part of the examination with the given examination code. In such a scenario, they should immediately inform the DoE and change the status of the examination center into **disqualified**. Otherwise, examination center status is **qualified**. In the case of a disqualified exam/evaluation, there is a possibility of re-run the initialization phase after successful repair or avoiding risks detected during the review process.

4.9.2.2 Deploy the Operating System

A DVD/USB copy of the customized GNU/Linux Operating System must have been delivered to the Technical Team in advance. The Technical team should deploy the given Operating System into primary and stand servers in the examination center as well as the evaluation center. The Tech Team is responsible for labelling primary and secondary servers and sealed the casing using

the provided stickers from the DoE. The installation process is pretty much straightforward as it is only required to make partitions and set passwords. As a part of the post-installation, the Tech Team is supposed to run a script which reset both local and root (admin) user passwords and each password should be unique in all examination centers across the island. The DoE can regenerate these passwords if required, and this activity avoids the examination center manager or someone else knowing the password given at the installation time as a result of shoulder-surfing or any other mechanism.

No one supposed to open the casing or/and change peripherals in the server. Furthermore, to log into the server once the Tech team has confirmed its deployment. During the installation of the server, there will be additional software and services automatically installed which are required to run the examination platform up and running.

In the case of the system upgrade, the same process can be followed. For example, in case of security patches to be applied in order to mitigate the specific vulnerability, the Tech Team can use a customized GNU/Linux ISO that includes the examination platform as well as security patches.

4.9.3 Verify the Installation of Operating System

After completion of post-installation activities, the Tech Team is required to verify the server deployment against a given checklist. It includes accessing given services from client machines. Once the verification is successful, examination center status is changed to **Ready to Deploy**. Tech Team shutdown each server and isolate the secondary server (remove network cables) as both servers should not run at the same time. Once everything is done, the Tech team seals all USB ports using the given official stickers and updates their journals/logbooks.

There could be a scenario where selected server hardware failed during the installation or post-installation, though it is less probable. Replacing an entire server with quality hardware is highly recommended at this point considering minimizing the risk of failing the server during the examination or evaluation process.

4.10 Deliver Examination Paper

A couple of days before the actual exam, the Examiner should visit his examination center, which is under the status of **Ready to Deploy**. This means the examination center is ready to deploy the exam.

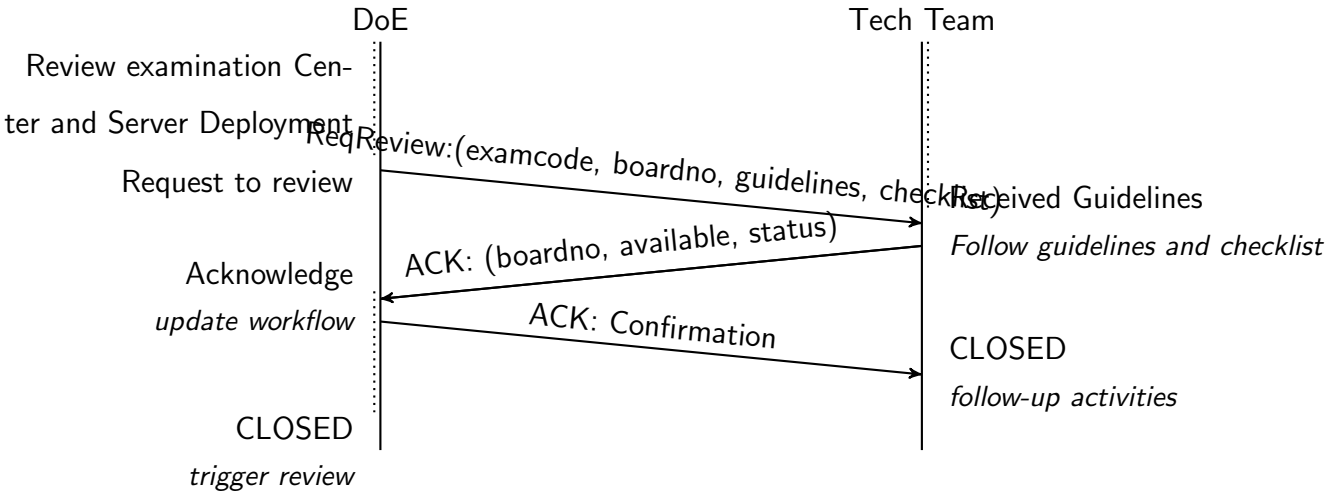


Figure 4.7: Review Protocol

Each Examiner will receive a portable USB storage, specifically USB pen drive with encrypted content from a Regional Coordinating Center one day in advance. Examiner should open the package in front of his assistant. Examiner boots the primary server and then waits till the system is ready to log in. Once the server is appropriately booted, the Examiner plugs the USB device sent from the Department of Examination via the regional center.

Role of the regional center is to keep a trusted space which enhances the communication between the DoE and the remote examination centers. For the exam, in case one of the USB is not working, Examiner has to wait for the round trip that takes to return the faulty device and to receive a new device. That impacts severely on the overall examination process.

The pre-installed Operating System is able to detect the USB that plugged in, transfer files in the USB, verify them, then extract it to required locations and reload or restart services accordingly. This process does not require anyone to log in to the system. So that chances of modifying the system are controlled. Examiner and the assistant will be there as a physical control to avoid such login attempts.

4.11 Conduct the Examination

Once the system is restored, Examiner can verify the restore process by accessing the server using the client system. It is a matter of browsing a given URL and seeing the test results. Moreover, the mock examination is given to verify the examination platform and questions are deployed. Now examination center status is switched to **Exam Ready** and this status should not

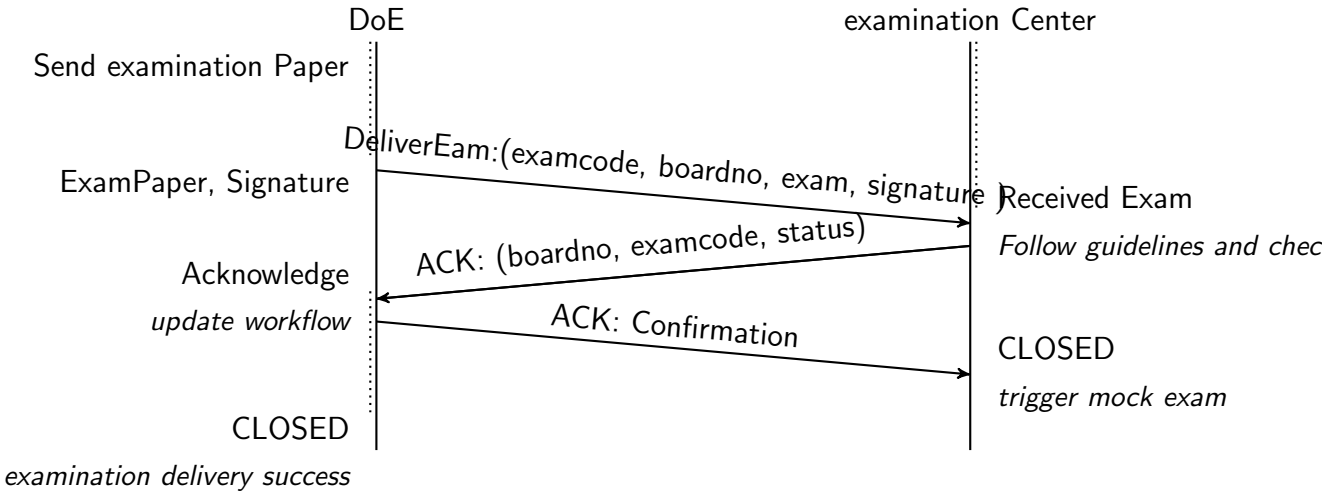


Figure 4.8: Deliver Exam

be maintained for a long time as the examination should be commenced in the examination center within a day or two. Once the examination is commenced, it should inform both the DoE and the regional center about the current status **Exam In Progress**. During the exam, examination center status can be switched to **Hold** if the examination Center operations are withheld due to technical or natural incident. The status changed to **Moved** if the examination center moved to a new location due to natural disaster **Exam Done** The same can be done once the examination was successfully ended.

After each session of the exam, Examiner should back up the examination center server into two USB devices given by the DoE. Backup is encrypted and hashed in order to verify integrity. This process should be continued till the final day, and there should be a log entry for each USB device when the Examiner is taking the backup. Log entry includes USB label, time, and officer 's signature and this document act as an administrative control which confirms who had taken the backup.

At the end of the last session of the last day of the exam, server shutdown and all opened ports should be sealed with the given security sticker in order to control reusing the server until the DoE requests to do so.

Both USB storage devices and log entry should be sealed into a wet-proof package and handed it over to the regional center. Scheduled transportation should reach the regional center along with an administrative officer to collect the package. Both USB devices and log sheets are used in the next stage of the examination process, which is evaluation.

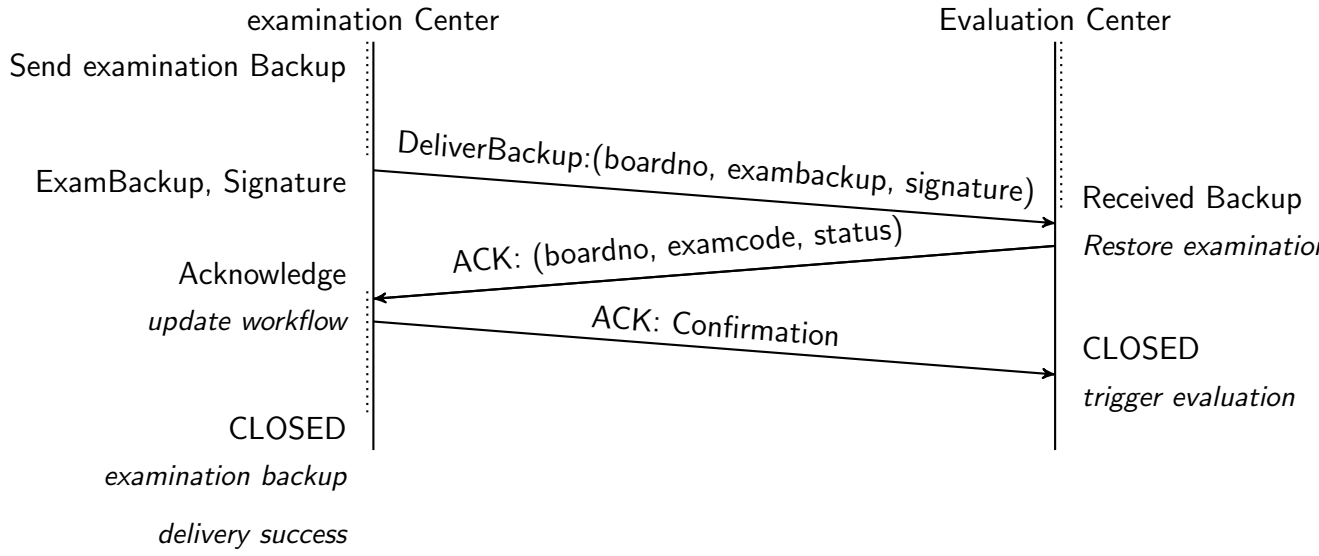


Figure 4.9: Deliver examination Back

4.12 Evaluation

The evaluation process is almost similar to the examination process in terms of generic operations. In terms of human involvement, a group of selected teachers is connected to a remote server located in an evaluation center instead of students. The Chief of the evaluation panel replaces the Examiner. The Examiner was selected after screening and all the stuff provided valid identification. Technical staff collects the USB devices along with the log sheet after verifying the person who delivered the package. Technical staff should provide his/her own identity to support verification of both parties and should then acknowledge receiving the package by signing the journal.

Once the server powered up, the USB ws plugged in and the technical team restores a backup as per the given guidelines. Tech team should use the log sheet to create a track of backups taken at each examination session in order to restore the correct session. Next step is to verify the restoration process by login into the examination system with a test account using the client machine. After confirmation from the tech team, teachers commence the evaluation process.

During the evaluation period, a daily backup will be generated automatically. After completion of the backup, the USB device is plugged into the system and lets the system synchronize the encrypted backup. Each backup should be recorded in the log sheet, including date and time, location (Evaluation Center ID), the signature of the officer who was involved with the backup process.

At the end of final evaluation day, once the completion of the backup server was shut down,

all opened ports should be sealed with the given security sticker in order to control reusing the server until the DoE requests to do so. The USB devices and the log sheet should be adequately sealed in a waterproof package.

4.13 Deliver Examination Results

The authorized officer should collect the properly sealed package from the evaluation center by producing an official identity card. It is also required to verify the person who delivers the package from the evaluation center. Then the package will be delivered to the DoE as the final stage of the examination process. At the DoE, the same verification process is repeated by checking the identity of both delivering and receiving parties and then the package is handed over to the Confidential Branch, which is supposed to pool results.

Once the package is received at the DoE, the package is safely opened, and then the log sheet is checked for any crucial comments or feedback. First, the signatures are verified. Then the received USB stick is plugged in to take a copy of the backup into secure storage at the DoE. The same activity should be repeated for the second USB as well. In the end, both USBs should have separate backups into secure storage if the signature is verified.

Once signature verification is successful, and the backup is completed, USBs should be kept in a safe locker along with a copy of the log sheet. Then the decryption process will use the backup copy and the log sheet. After the decryption is completed, results will be imported to a central server which processes examination results.

Now the acknowledgement required to send back to the evaluation center in order to wipe out evaluation servers.

4.14 Decommission

After considering the requirement of secure deletion of data, a decommissioning process was introduced. Authorized officers attend this task only on request in case the server is no longer in use due to hardware failure. Cancellation of the examination or evaluation also requires the decommissioning process. It is mandatory to perform data archival before each decommissioning process. The officer who attended the decommissioning process must produce a report on the way the decommissioning process was carried out. The decommissioning report includes information such as when it was done, where it was done, by whom it was down, how it was done and what tools used during the entire process.

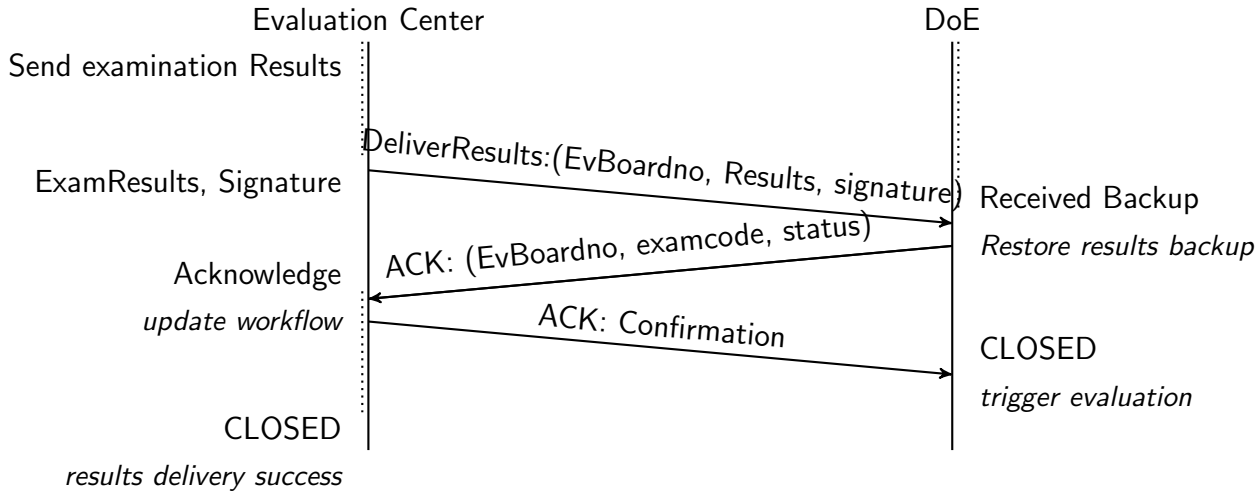


Figure 4.10: Deliver Results

4.15 Routing Protocols

4.15.1 Direct Contact Protocol Operation

In order to handle secure delivery of environment keys during the initial phase of setting up the environment at both examination Center (ExC) and Evaluation Center (EvC), two different installation media are directly distributed to each center via trusted transportation. Transportation should be hand-carried by a trusted official who already cleared the screening process and got authorized himself to distribute media from DoE to ExC and EvC accordingly. There are different keys available in each installation media which require to handle encryption, decryption, signature creation and verification at each stage. The person who delivers the media has no authority to install or keep them for personal usage.

It is mandatory to provide official identity at DoE before collecting the package as well as delivering it to each center. Similarly, the person who delivered the package shall verify the identity of receiving parties before handing it over. It is essential to maintain a log note to keep track of the collection and delivery of each media with correct date and time with the location (Center ID) and signature of relevant participants. This operation process is depicted in the figure:4.15.2.

4.15.2 First Contact Protocol Operation

Each examination Center should back up examination content and send them to an Evaluation Center via an authorized officer who is already screened. The officer should prove the identity

to the examination Center (ExC) and verify the person who is handing over the backup to make sure there will not be a third party involvement other than officials.

At the Evaluation Center (EvC), the identity validation process is repeated, and then the backup is handed over. During the collection and delivery, a backup name, hash, date and time (collection or deliver), location (Center ID) and replant participants are noted.

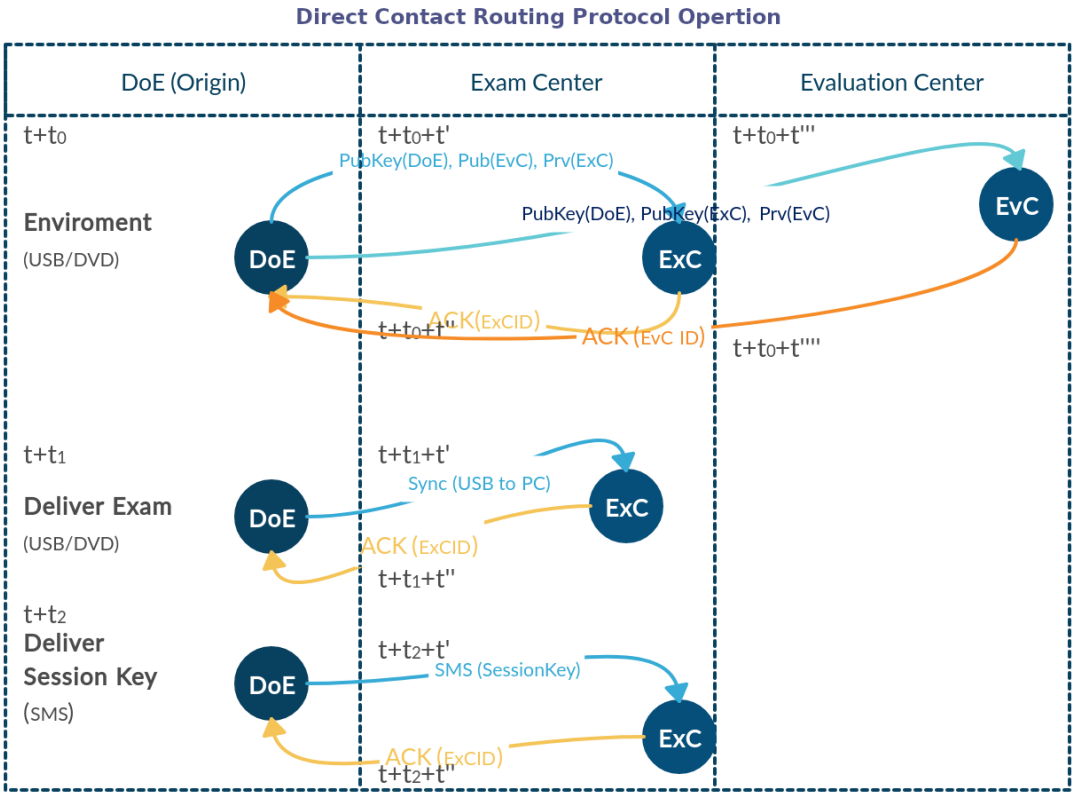


Figure 4.11: Direct Contact Protocol Operation During Environment Setup

4.15.3 Protocol Stack

Each of the protocols and sub-protocols described above form the protocol stack that provides the solution. The proposed protocol stack is given in Figure:4.15.3, which enables the confidentiality, integrity, availability and non-repudiation of the examination system. Foundation of this protocol stack is the trusted layer which builds during the initial phase of the process where the selection of trustworthy staff and initialization protocol is given in Figure:4.5. Then the main

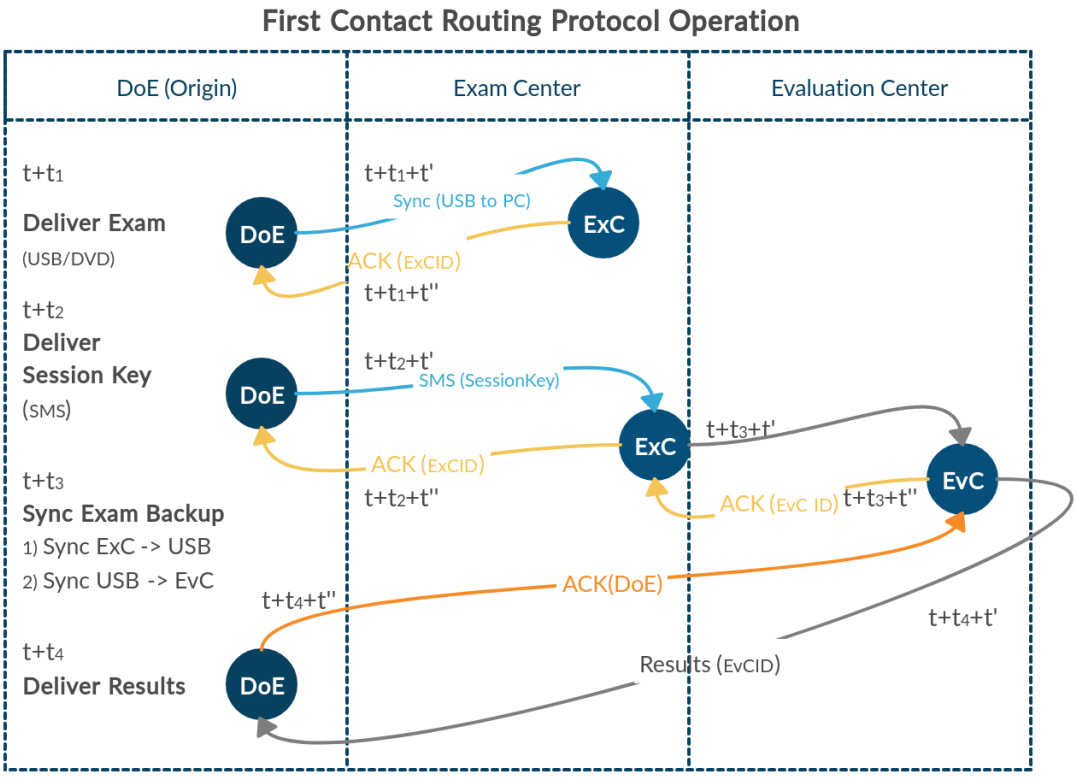


Figure 4.12: First Contact Protocol Operation During the examination and Evaluation

two protocols, First Contact Routing Protocol and Direct Contact Routing Protocol handle routing. Direct Routing Protocol is used to set up the environment and deliver session keys, which is required to start the exam.

First Contact Routing Protocol facilitates synchronization of exam, backup and results while Direct Contact Routing enables environment setup and session key. Sync Protocol enables secure synchronization of content from the server to USB and vice versa at both examination Center and Evaluation Center.

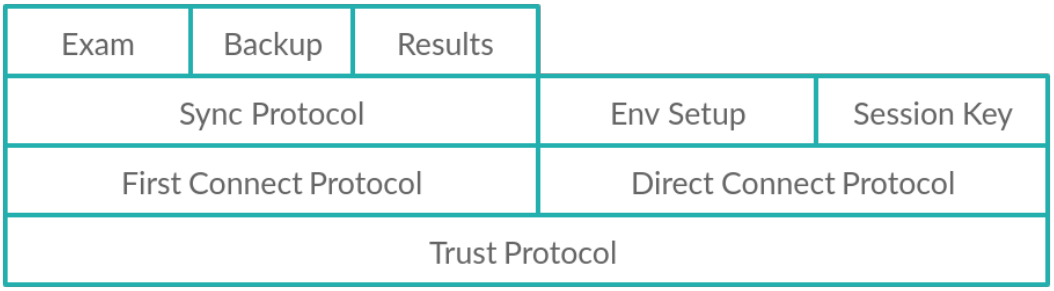


Figure 4.13: Protocol Stack

Even though this solution is missing AAA server such as RADIUS server which is used in conventional networks. The proposed solution provides similar capabilities by handling Authentication (Who you are?), Authorization (What you are allowed to do?) and Accounting (keeping records/Logging system) using physical, administrative and technical controls embedded into the solution.

Moreover, the proposed solution provides data security with respect to the Data Security Lifecycle listed below.

Create : create, update/modify data.

Store : Data at rest.

Use : Data in use.

Share : Data in transmit.

Archive : Backup, store in long term storage.

Destroy : Permanently destroying of data.

4.16 Summary

Design of the security protocol initiated with the idea of "Secure by Design" concept. So, a Level 3 Data Flow Diagram created against the proposed solution followed by a Threat Modelling.

In the next chapter, Chapter 5, the researcher will discuss in detail the implementation of the proposed protocol.

Chapter 5

IMPLEMENTATION

5.1 Overview

This chapter discusses the implementation of the proposed protocol design discussed in the previous chapter. The proof of concept prototype was developed using the proposed security protocol. Moreover, this chapter discusses how administrative, physical and technical controls were implemented to ensure confidentiality, integrity and availability of a computer-based examination which is capable of running in a delay tolerant environment.

5.2 Training and Awareness

Several training and awareness programs were conducted to address different stakeholders and scenarios. Firstly, a hands-on training session was conducted to the staff of examination and evaluation centers on the fundamentals of GNU/Linux and also on setting up a local network. Troubleshooting, monitoring exams and related formalities such as taking a secure backup and filling chain of custody were also included in the training process.

A separate session was conducted on security-related aspects, including Social Engineering attacks. These training sessions were provided to full staff in all administrative categories as security is everyone 's responsibility. Moreover, these training and awareness programs were conducted to prevent incidents related to human errors and also to provide better user experience with fast response to incidents. During the awareness programs, it was highlighted the importance of the security concepts (discussed in the Section: 2.12) such as Zero Trust. One such thing discussed was about dealing with a candidate who has already arrived in the examination centre after the identity validation procedure. There, we strongly instructed to the authorized

center staff to not let this candidate to approach the server computer or having try-outs to login with others credentials.

5.3 Encryption

Despite the mode of the examination, examination papers and results should be transported securely from one location to another. It should remain safe when examination data is at rest (residing in a disk). Encryption plays a significant role here to ensure that confidentiality is not compromised and implemented encryption methods are further described here.

5.3.1 Encryption of Data on Transmit

Sensitive data such as examination paper should not transmit in plain text. Since the transmission medium is a generic USB drive (no built-in hardware encryption), sensitive content was encrypted before writing them into the USB drive.

Examination center servers were set up to generate encrypted backups automatically. Following that, the examination supervisor needs to trigger the backup via examination monitoring dashboard. Detailed explanation on the implementation of encrypted backups can be found under the Section: 5.16 Secure Backups.

5.3.2 Encryption of Data at Rest

The data that is stored physically in the disk is called Data-at-Rest. The encryption of data-at-rest is about encrypting the data in a server disk. During the deployment of the examination server, it is recommended to create disk encryption at the time of installation of the server by a Tech Team. Since there is no technical team available at an examination center permanently or full time (they are supposed to provide technical support to several examination centers in their education zone) passphrase should be kept only by the examination supervisor.

The Data-at-Rest Encryption has no protection over deletion of data in the encrypted disk or when formatting the encrypted disk. The risk of wiping out the entire encrypted disk is controlled by allowing access only to authorized examination staff of centers. Unauthorized access to the examination center is controlled by the security officers who are placed outside the examination center. Both the staff and examination candidates are authorized to access the examination center premises after the verification process. The staff has to provide both NIC/Passport and a valid appointment letter, but examination candidates should provide a valid admission card along with

their NICs. The supervisor of the examination center is responsible for avoiding unauthorized access to the server by any party, including students while it is being up and running. The security guard is responsible for securing the main entrance of the premises.

Moreover, Wi-Fi is disabled in order to avoid unauthorized remote access via the Wi-Fi routers available in examination centers. The technical team is supposed to review the availability of Wi-Fi access during their on-site pre-examination audit. The technical team should immediately disable Wi-Fi services attached to the internal network.

In the examination guidelines, it is mentioned that no electronic devices are permitted into the examination center. Neither storage device, nor communication device is allowed to bring into the examination center.

5.3.3 Key Infrastructure and Distribution

The examination process requires keys for encryption, decryption, signature creation and verification of the signature. Some cryptography-related activities were implemented as follows:

1. Encrypt examination paper at the Department of Examination
2. Sign the examination paper at the Department of Examination
3. Decrypt examination paper in the examination server
4. Verify the signature of the signed examination paper in the examination server
5. Encrypt examination backup in examination server
6. Sign the examination backup in examination server
7. Decrypt examination backup in evaluation server
8. Encrypt evaluation backup in evaluation server
9. Sign the examination backup in examination server
10. Decrypt evaluation backup at Department of Examination
11. Verify signature of the evaluation backup at Department of Examination

Above listed cryptography-related activities require different types of keys in different locations in order to transmit examination content confidentially. To make this possible, Key

Distribution is highly essential, and the proposed solution is capable of distributing keys to all examination centers across the country.

Required keys were added into the customized ISO image and required keys were copied into the server during the installation efficiently. There were two separate ISO files created to deploy examination server and evaluation server. It made it easier to distribute keys required for each server instead of having all keys in both types of servers.

The examination paper was decrypted only at examination server but it is impossible to decrypt at the evaluation server as the examination paper was encrypted using the public key of the examination server. Similarly, evaluation server backup could not decrypt using the examination server but at the Department of Examinations as the evaluated results are encrypted using the public key of the Department of Examinations. Purpose of this technical control was to enforce only the examination centers were able to retrieve the examination paper but not elsewhere. It enables confidentiality within the examination process.

5.3.4 Type of Encryption

Mainly there are two encryption types, namely, Symmetric Encryption and Asymmetric Encryption. There is an advantage of using symmetric encryption when dealing with large files. The idea was to first encrypt either examination paper or backups with symmetric encryption and then encrypt the symmetric key using public key encryption (asymmetric encryption). When transferring the encrypted file, the encrypted (using the public key of the destination) secret key of the symmetric encryption is also required to be sent to the destination.

Hybrid encryption is leveraging the performance of the symmetric encryption and the convince of secure key exchange of the public encryption. It is highly essential to encrypt and decrypt backup files efficiently and exchange keys with minimum effort over a secure mechanism.

5.3.5 GnuPG (GPG)

GnuPG (GPG) is a Hybrid Encryption solution. The GPG uses symmetric encryption using it 's default cipher of Advanced Encryption Standard (AES) and encrypts the session key with the public key. In addition to the encryption and decryption, GPG is able to handle signature creation and verification as well.

5.4 Local Configuration

The local server includes several configurations which are deployed for different requirements such as to enable service, forensic readiness, ease of technical support and to minimize accessing local server except via web server.

The technical team executed a separate script to manage local configurations. It is the responsibility of the technical team to verify setting under the supervision of the examination supervisor. Since the examination supervisor is responsible for all the activities conducted in the examination center, the supervisor must observe all activities with the help of the center assistant.

5.4.1 Network configuration

The examination server or the evaluation server is deployed in a school ICT lab before commencing the examination or the evaluation. Other than the server, client machines with either Linux or Windows Operating System, no change to the client OS is made but setting up /etc/hosts file to resolve local DNS is allowed. Each examination center and evaluation center is supposed to set the local network into a unique network address. The examination servers used a unique IP that each client machine can use to access the server during either examination. The similar environment was set up in each evaluation center, but the server had unique IP but different from the examination server.Client machines are required to set the server IP to resolve DNS locally using the “hosts” file.

Both primary and the standby server were configured with the same IP address but the standby machine supposed to power up only when the primary server is unavailable. In case of unavailability of the primary server, it is a must to remove it ’s network connectivity cable before connecting the standby server to avoid IP conflict.

5.4.1.1 Network Interface Card (NIC) Bonding

Network Interface Card (NIC) bonding implemented during the installation to support multiple NIC devices to serve with a single IP. It also enables fail-over in case of network interface failure or cable damage. As given in Figure: 5.1, NIC bonding implementation was automated to minimize human errors and easy deployment. Customized systemd service is created to regenerate the fresh nic bonding configuration after each system or service reboot. It makes the system automatically remove configurations of nic devices that no longer attached to the device.

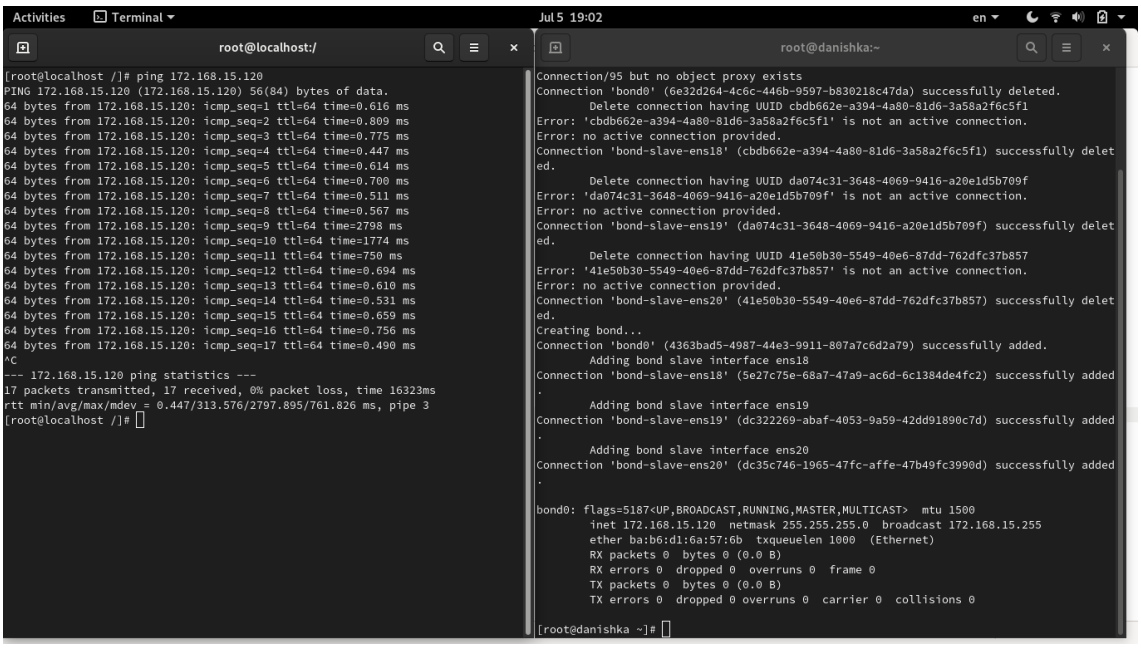


Figure 5.1: Automated NIC Bonding

Moreover, the above mentioned technical aspects were communicated to members of the technical teams during their hands on training sessions. Additionally, these instructions were included in the printed technical guidelines provided to each center.

5.4.2 Update Timezone

In order to retrieve useful logs with the correct timestamp, setting the Timezone to correct timezone is an essential task. Time-dependent activities such as scheduled jobs, application-related events (either activation or expiration of the examination) depend on the time zone. Importance of setting the correct timezone and the way set correct timezone during the installation was explained during the hands-on training session. A custom script that runs as the post-installation fix the timezone in case if it missed during the installation.

5.4.3 Enable Service

- Cronjobs for backups
- Firewalld
- httpd
- MariaDB
- Custom Service (i.e. synchronize secure backups to USB)

- Firewalld

5.5 Collecting Environment Information

Environment information is useful in case of an incident. It is highly essential to collect environment information, such as neighbouring devices to enable forensic readiness. Network scanning to find the number of devices attached to the network. ARP Scanner is one of the tools that can periodically scan the network to find connected devices. A number of connected devices to the examination network should not exceed the total number of computers approved to a given examination center. Similarly, the number of connected devices in the evaluation center network should be equal to the number of approved computers in the network of the evaluation center. The above-mentioned feature was implemented in both examination and evaluation center servers as a part of forensic readiness of the system.

5.5.1 Logs

Logs are one of the most essential and critical parts of a system and help the system to be a forensic-ready environment. It is required to identify required logs for the running system in order to provide technical support as well as for investigations at the post-event stage.

There are different logs available, and some of them automatically generated by the Operating System and Applications. Some of them are required to generate by the customized processes or scheduled jobs. Purpose of enabling logs effectively and securely collect them is highly useful for a forensics readiness of the system. In case of an incident, logs deliver exhaustive information on the either past or present situation.

- User logins
- System start, shutdown and reboots
- Backup logs
- Web server (apache httpd) logs
- Database server (mariadb) logs
- Application server (moodle) logs
- Audit/Security logs

- Health checks

There is no much use of logs without a proper timestamp, but the system time should be set to the local time zone. Since the system is supposed to run independently in a remote station as a server, it is essential to set log to rotate in a manner that excess logs will not fill the disk. Disk capacity planning requires considering the size of complete logs. Moreover, it is essential to avoid accidental deletion of sensitive or critical logs.

5.6 Server Hardening

Server hardening is about increasing the security of the operating system and its applications, service of a server. There are activities that can be done in order to harden a Linux server. A few of them listed below. During the installation of the customized Operating System, it automatically deploys the harden version of httpd configuration.

5.6.1 Update Kernel and install security updates

It is highly essential to keep the kernel up to date and install the latest security updates. All available updates bundle together during the ISO build process. There would be no need of separate package update if the server installation was done by the latest release of ISO from the Department of Examinations.

Technical Team able to deploy security updates with a pre-approval from the DoE in case of a critical security patch to deploy.

5.6.2 Minimal service and packages

Both examination and evaluation servers should have only httpd, MariaDB and firewalld service but not services such as samba, FTP rsh, telnet, rlogin, and mail services. The server should have only required packages. Minimum packages will reduce the risk of having vulnerable packages.

5.6.3 Verify no local user (non-root) accounts with UID set to 0

Only the root user account should have UID set to 0.

5.6.4 Verify no user accounts with empty passwords

User accounts with empty passwords should be a lock.

```
[danishka@danishka ~]$
[danishka@danishka ~]$  dnf list installed fire*
Installed Packages
firebird.x86_64                          3.0.4.33054-4.fc30              @updates
firebird-utils.x86_64                    3.0.4.33054-4.fc30              @updates
firefox.x86_64                           76.0-2.fc30                     @updates
firewalld.noarch                         0.6.6-1.fc30                    @updates
firewalld-filesystem.noarch              0.6.6-1.fc30                    @updates
[danishka@danishka ~]$
[danishka@danishka ~]$
```

Figure 5.2: Verify installed packages (package name start with 'fire')

```
[root@danishka ~]#
[root@danishka ~]# awk -F: '($3 == "0") {print}' /etc/passwd
root:x:0:0:root:/root:/bin/bash
[root@danishka ~]#
[root@danishka ~]#
```

Figure 5.3: Verify no local user (non-root) accounts with UID set to 0

A user account can be lock using the following command.

```
#passwd␣-l␣<user_name>
```

5.7 Host Based Intrusion Detection (HIDS)

Although the system is running in a remote location, it is required to monitor the malicious behaviour of the server. An Intrusion Detection System (IDS) can detect changes and threats to the system. A host-based IDS will monitor the server on which it is installed. There are several HIDS solutions out there, but the researcher deployed Advanced Intrusion Detection Environment (AIDE). The AIDE is an open-source HIDS solution that can scan file properties such as the content of the file, file creation and update time, file permission and inodes.

5.8 Packaging

- Udev rules
- Backup scripts
- Examination paper
- Encryption Keys

```
[root@danishka ~]#
[root@danishka ~]# awk -F: '($2 == "") {print}' /etc/shadow
[root@danishka ~]#
```

Figure 5.4: Find user accounts with empty passwords

5.8.1 Build ISO

ISO file was created using both official fedora packages and customized packages. This process was conducted under the observation of a senior officer.

Once the ISO was built, the verification process started at the Department of Examinations. All custom scripts and required functionality was there as expected. Then the ISO image was approved, and media (LiveUSB/LiveDVD) preparation started.

5.8.2 ISO Checksum

A checksum was created and signed with the private key of the Department of Examinations. At the receiving end, checksum was verified before the check the checksum of the received installation media.

5.8.3 Packaging DVD/USB

ISO files can be distributed across all the examination centers as LiveDVD or LiveUSB. After writing the ISO image into either DVD or USB as a live system, each media was verified by booting into login screen. Then the verified media was labelled with serial numbers for tracking purpose and carefully packed using a secure package.

5.9 Prepare Examination Center

5.9.1 Masking of Educational Material in the ICT Lab

Examination center was prepared as per guidelines provided by the Department of Examination. All kinds of educational materials have either been masked or removed. For example, educational banners, posters or any form of materials with the content that related to the subject of the examination.

5.9.2 Access Control

A security officer deployed at the main entrance of each examination center during the period of examination. The main door of the ICT lab was secured with a proper padlock and each client and server machines also locked with padlocks. The supervisor of the center is responsible to secure the machines and servers inside the center and keys of the padlock keys should be sealed and kept at the security office. The chief of the security accountable for the physical security of the premises.

5.9.3 Security Camera

Some of the examinations and evaluation centers consist of a security camera that operates throughout the entire day. Since the deployment of a security camera is not an affordable solution, it was not a mandatory requirement but considered as good to have an option.

5.9.4 Network Level Controls

Wi-Fi access disabled from the ADSL/4G routers to make sure that the local area network is accessed by only verified candidates and the supervisor who are physically present inside the examination center.

5.9.5 Client Systems

Anti-virus software updated in candidate 's and supervisor 's system. All devices tested including mouse, keyboard, UPS. The hard disk was cleaned up including the download directory. Verified available disk capacity, CPU and physical memory are up to the recommended capacity. For each session of this examination, there were two standby computers for candidates and a one standby machine for the server in school ICT labs.

5.10 Prepare Evaluation Center

Preparation of the evaluation center is almost similar to the preparation of the examination center that was described under Section: 5.9. All client machines treated as mentioned in Section: 5.9.5 and access controls were placed as mentioned in Section: 5.9.2, Section: 5.9.4.

5.11 Deploy Servers

The technical team confirmed that they had received the correct checksum of the ISO image by verifying the checksum. Then generated the checksum of the received ISO and matched with the received checksum. Once the checksum was matched, the technical team deployed examination servers and evaluation servers using corresponding ISO images.

Even though deployment of both examination server and evaluation server is straightforward and almost similar, priority is given to deploy the examination server. Both primary and standby server have deployed in each center. Successful deployment of the server reported back to the examination server that triggers the next step. Installed media kept securely with the technical team, but the examination supervisor had no access to the examination media.

There were two layers of security established while deploying the server by leveraging separation of duties. Each server deployed with disk-level encryption. Passphrase for the decryption of the disk, provided by the examination supervisor. However, root and local user (one single user created in each server) passwords were set by the technical team. During the examination period, the examination supervisor uses the passphrase during the boot-up of the server, but there was no such requirement to login to the server. The examination supervisor was only authorized to power on the server and provide the passphrase before the examination. After the examination server was just shutdown but no manual operations to be done directly in the server throughout the examination period. The similar procedure conducted at the evaluation center. The chief officer of the evaluation center was responsible to power-up the server and shutdown during the evaluation period.

5.12 Loading examination Paper

Once the examination server deployed, the examination paper would be received as a digital media (USB). After plugging the USB into the running examination server by the examination supervisor, the examination server automatically detected the attached USB and loaded the examination paper after verifying the decrypted content.

5.12.1 Verify examination server

A mock examination was given to verify the examination server. This is the very last step of a series of activities to make the examination server ready to run an online examination. After updating the status of the verification process, the session key was distributed to examination

centers which were successful with verification of the server. Otherwise, relevant support teams attend to rectify issues found during the verification process. A detailed description of the support teams available under the Section: 5.24.

5.13 Session Key

A session key is required to access each examination session. It was generated and securely delivered to the examination supervisor in advance. Delivery of the session key is separated from the delivery of the installation media (USB/DVD) and examination paper. During this process, the identity of the delivered person and the received person is verified.

5.14 Verify Candidate

Candidate verification is done in two stages. Security officers only allowed valid candidates to enter the examination center by verifying admission against the identification card/letter and checking their belongings. Valid candidates were allowed to enter the premises and did not allow any prohibited items, including any electronic devices mobile phone, storage devices). Then the supervisor has to verify the candidates against the list of valid candidates sent from the Department of Examinations along with the candidate 's admission and identity card/letter.

A notice was placed in both inside and outside of the examination center as a preventative security control. It was clearly mentioned that what should not bring into the examination center and what should not be done in the centers.

5.15 Conduct Online Examination

After the verification process, candidate 's filled the attendance sheet. Then the supervisor distributed login credentials to respective candidates and shared the session key. Candidates were logged in to the examination system, which was based on Moodle and provided session key to access the examination. During the examination, the supervisor was able to monitor the progress of each student using a separate dashboard. The supervisor was able to extend the examination session when there was a disruption with less than thirty minutes. For disruptions with more than thirty minutes had to be rescheduled, and each extension and reschedule were reported back to the Department of Examination and logged in the journal reports. In case, if an examination

was rescheduled due to a disruption, the rescheduled examination would be conducted after the examination.

5.16 Secure Backups

The system generates secure backups for sensitive data such as examination papers, answers and results. Sensitive content is compressed and then encrypted on the file with a signature to verify later.

5.17 Automated Secure Synchronization

The system was designed in a way that no operator is required to login to the Operating System either via Graphical User Interface or the Terminal (CLI). The examiner is supposed to plug one of the USB drives to the system after each examination session. Automated synchronization initiates once the USB device is plugged into the system without any other human interaction.

5.17.1 Identify USB

Udev is the Linux subsystem that supplies the Operating System with device events, for example, adding or removal of devices such as network card, external hard drives (including USB drives), mouses, keyboards, joysticks and DVD-ROM drives. Udev is a potentially useful utility that a standard user can manually script to perform specific tasks when a particular device is plugged in.

Udev rules recognize the way to identify attached devices and to assign a device name that is persistent through system reboots or disk changes. Once Udev receives a device event, it matches the pre-configured rules against the device attributes in sysfs to identify the device. In addition, Udev rules can specify additional scripts to execute as part of device event handling.

Udev recognizes devices by serial numbers and manufacturer, vendor product ID numbers. Though the mounting process can be restricted to a selected range of devices, Udev rules auto-mount any USB device as the synchronization process handles only encrypted data bundles.

5.17.2 Local Synchronization

Synchronization initiates once the USB device is mounted under the predefined location as per instructions given in the Udev rules. It is recommended to examiners to plug the primary USB

device and then the secondary device sequentially to avoid human errors such as removal of the wrong USB while backing up both devices at once.

It is possible to repeat the synchronization for any number of times for the same device. The Synchronization process also supports multiple devices, and it enables synchronization of standby USB devices in case one or both USBs are damaged or lost. This feature enables retrieving backup files until either the examination or evaluation server decommissioned. If the device is lost, nobody can use it as the content is already encrypted.

5.17.3 Chain of Custody

The examiner was supposed to have two backup copies after each session using both USB devices. It is recommended to maintain the chain of custody document during the examination period. Information maintained in this document includes Device ID (provided by the Department of Examination), backup time, date and user signature. In the case of missing backups, this document will be used for investigation purposes.

5.17.4 Authentication and Authorization of Synchronization

At this stage, the examiner is authorized to take backups under supervision of the chief examiner. The examination center staff are responsible for executing the backup process with the guidelines provided. Other than examination staff, no one else should operate the system and handle the backup process (students and the third party is strictly not allowed).

Any misbehaviour was followed with an official investigation and is bound to relevant consequences. Computer Crimes Act will apply to an online examination if any offences mentioned in the act are committed by an examination candidate, examination staff or third-party [52]. Since the examination papers are copyright materials of the Department of Examinations, Intellectual Property Act No.36 of 2003 is applicable in the case of misuse of examination papers or backups that includes examination papers [53]. Moreover, Public Examinations Act (no. 25 of 1968) [39] is also applicable here.

5.18 Post Examination Activities

After the examination, as mentioned above, secure backup (dual copies) was taken into provided USB storage drives, and the chain of custody was updated. Both secure backup and chain of custody were securely packed with a waterproof and damage proof package. After verifying the

receiver and sender, the package was handed over to secure delivery managed by the Department of Examination.

The next activity is to shut down the server and disconnect it from both the network and the power line. Then, all ports including USBs and power button, casing, power supply socket, network socket need to be sealed using a special sticker provided by the Department of Examinations. Moreover, padlocks to be used to secure the casing of the server machine.

5.19 Swapping

Collected backups were swapped before sending them to evaluation centers. Before the commencement of the examination, no one has the right to predict the evaluation center allocated to a given examination center.

5.20 Evaluation of Examination Papers

The evaluation center also had two levels of security where a security officer verified every person visiting the evaluation center by checking the appointment letter and the identity card/letter. The chief examiner of the evaluation panel also did a verification.

Once the evaluation center received the examination backup, it was logged in to a journal along with received time, delivered person and the signature of chief of the evaluation panel. Then the USB with the examination backup was plugged into the server and waited till it restored the examination backup. Only the evaluation server was able to decrypt the examination backup as it had keys to verify the signature of the examination server and decrypt the backup. After a successful backup restoring process, the USB and the examination backup were kept securely in a sealed secure enclosure. The evaluation panel was able to log into the system using the provided credentials.

After completion of the evaluation, the chief of the panel triggered the secure backup and plugged the USB into the system. As mentioned under Section: 5.17, secure backup was synchronized to the USB. The chain of custody was updated accordingly after the dual backup was completed.

5.21 Post Evaluation Activities

After the evaluation, secure backup (dual copies) was taken into provided USB storage drives, and the chain of custody was updated. Both, secure backup and chain of custody were securely packed with a waterproof and damage proof package. After verifying the receiver and sender, the package was handed over to secure delivery managed by the Department of Examination.

Evaluation server was shutting down and disconnected from both network and the power line. All ports including USBs and power button, casing, power supply socket, network socket were sealed using a special sticker provided by the Department of Examinations and padlocks used to secure the casing.

5.22 Data Archival

At the end of the entire examination process, each examination center and evaluation center delivered a couple of backups (two USBs). All logs and encrypted backups should be archived for a minimum of five years as per the data retention policy of the Department of Examination. All contents of USBs are copied to portable disks with high durability. It is highly recommended creating dual copies of the archive and sending them into two different safe lockers. The achieved data must be retrieved only on approval.

5.23 Secure Deletion and Decommission of Servers

Servers can be removed from the examination or evaluation process due to hardware failure or the examination center, or if the evaluation center is no longer in use. In such a situation, data belongs to the examinations should be securely wiped out. This process should be handled by a specific team from the Department of Examination. Who are authorized to make the necessary decision to ensure no examination related data can be recovered from the server.

5.24 Incident Response

Technical support is highly critical in an event where the malfunction is about to happen before the examination or while in progress and once the examination is already completed. Technical support split into several layers in order to provide efficient and quality technical support in order to maintain either no downtime or minimum.

Technical Support has been implemented in three different levels to make sure the availability of efficient technical support during the examination process.

5.24.1 Level I Support

Level I technical support is provided by examination staff at the examination center. It should be available on-site throughout the examination period. A similar should be available for the evaluation center as well. Level I technical issues should be reported back to the Department of Examination using log sheets (journals) provided and phone calls and emails can be used when it matters as per availability and severity of the incident. Level I support should escalate their issues to Level II support unless they can fix with given resources.

5.24.2 Level II Support

The technical support team of the zone provides Level II technical support which can be reached over the phone and if required, Level II technical support can reach an examination center in less than an hour. The technical team should escalate the issue to Level III Support when they are unable to resolve the issue. Level II Support has the authority to get the third-party support, such as calling a vendor and requesting to replace malfunctioning devices at an examination center or evaluation center. Since it is possible to reschedule a disrupted examination session, there will not be much impact on candidates other than reattempting the examination either after repairing the device or relocating to another examination center on a different date as per approval of the Department of Examination.

5.24.3 Level III Support

Level III Support is provided over the phone and via emails by a technical team who are based in the Department of Examinations. On-site support is also provided by the Level III team but only when there is a critical issue where the rest of the two teams can not rectify the issue or make a decision themselves. Level III Tech Support has the authority to cancel an ongoing examination session with or without a rescheduled session. Moreover, Level III support coordinates both Levels I and II teams when an issue occurs with the effects on all the centers around the country.

5.25 Security Controls

As given in Table: 5.1, there were several control measures implemented. Physical security implanted to avoid unauthorized physical access and, facility and infrastructure protection. Administrative controls included policies, standards and processes. Technical or logical controls included access controls, cryptography, intrusion prevention and backups.

Above mentioned controls represent five types of security controls or control functions, namely preventative, detective, deterrent, corrective and recovery.

	Control Functions				
	Preventative	Detective	Deterrent	Corrective	Recovery
Physical	Padlocks, Waterproof packing for USB drives and documents, Secure Packaging for DVD	CCTV, Security officers	Security officers, CCTV, Warnings	Repair physical damage	Stand by servers
Technical	Encryption, Firewall, Antivirus SW	IDS, Application and access logs	Warning messages in the system, Signature	Restore either OS or data, Install bug fix, replace faulty hardware	Stand by server, Dual backup, Power generator
Administrative	Separation of duties, Hiring and termination policy	Review access rights and journals, Screening, Verify candidates and staff	Non Disclosure Agreement (NDA), Exam guidelines for candidates	Inquires and investigations	Attendance sheet, Chain of custody, Reissue admission, Reschedule examination, Reschedule evaluation

Table 5.1: Control Functions and Control Types

5.26 Summary

A mixture of administrative, physical and technical controls was implemented to ensure confidentiality, integrity and availability of a computer-based examination which is capable of running in a disrupted and disconnected environment.

In the next chapter, Chapter 6, the researcher will provide a discussion about the evaluation of the research, including lessons learned in each stage. Moreover, the next chapter presents the evaluation of the proposed protocol through State Transition Diagrams.

Chapter 6

EVALUATION

6.1 Overview

In this chapter, discusses about the evaluation of the proposed protocol. Evaluation was conducted in two methods. Firstly, each development iteration evaluated with user feedback using user surveys. Moreover, evaluation of the proposed protocol is presented through State Transition Diagrams.

6.2 Results of the Iteration-I

The first iteration conducted as an online examination using a central examination server. As per the results of the servery, there was a high participation (see Figure: 6.1) and high satisfaction rate (see Figure: 6.2) among the participants. The high rate of user satisfaction implies that the provided Moodle based examination platform was up to the user satisfaction.

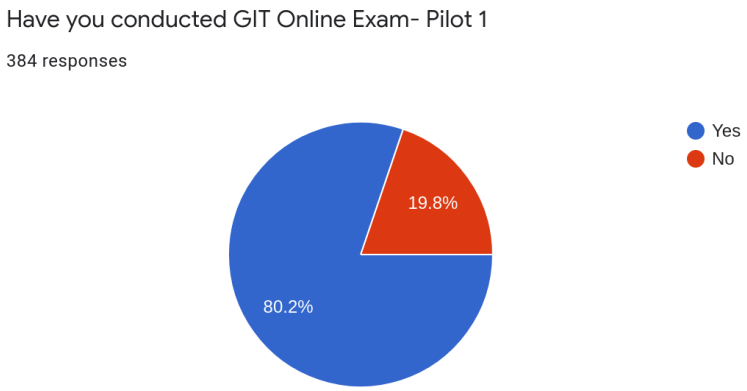


Figure 6.1: Participation of the First Iteration

As indicated in the Figure: 6.3, there were several issues. Around 30% of them had no

internet at school and 39% of them had poor connectivity. Around 34% of them having lack of resources (PCs) in the school ICT lab, which clearly justify the requirement on extra sessions. Since the number of usable ICT labs are less, each ICT lab has to conduct multiple sessions of the examination.

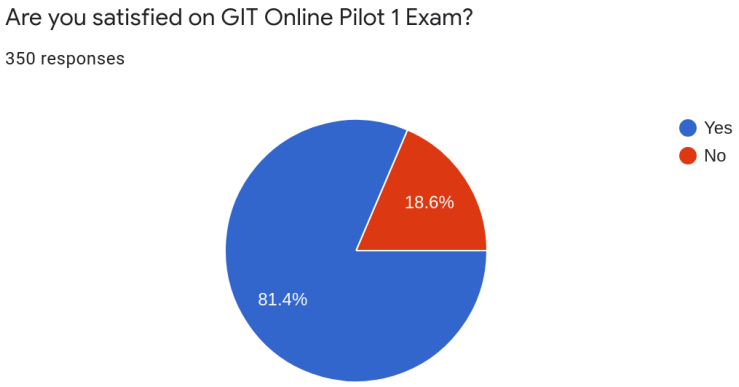


Figure 6.2: Satisfaction of the First Iteration

Over 20% of them experienced a disrupted power supply during the examination period of the first iteration. Moodle provides a feature to extend examination session time in case of such outage. It is not possible to handle extension of examination session time in several examination candidates due to multiple outages across the country. examination session extension is much easier when students connect to a local server instead central server. The examination supervisor can easily extent to examination session time in the local server.

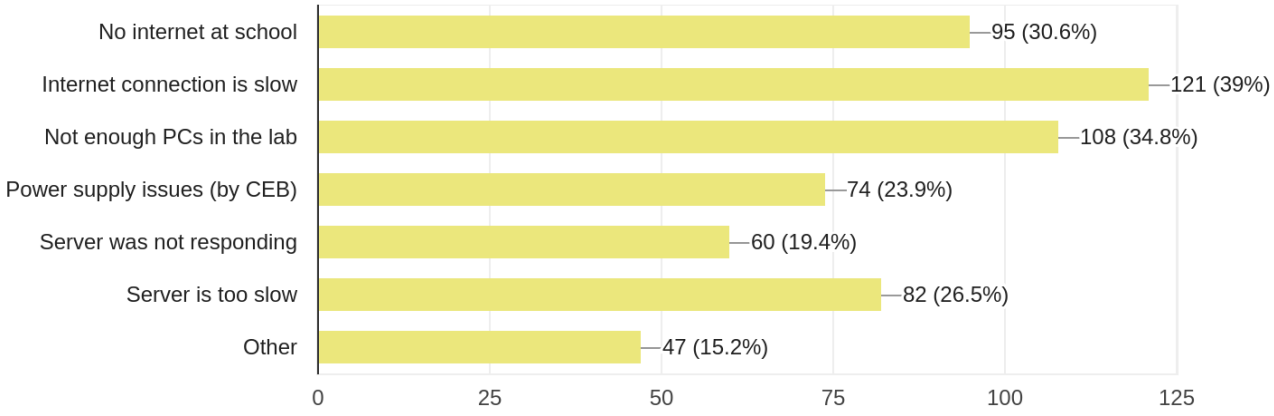


Figure 6.3: Issues of the First Iteration

Concerning above mentioned issues, second iteration planned to deploy a local server in the school ICT lab itself.

6.3 Results of the Iteration-II

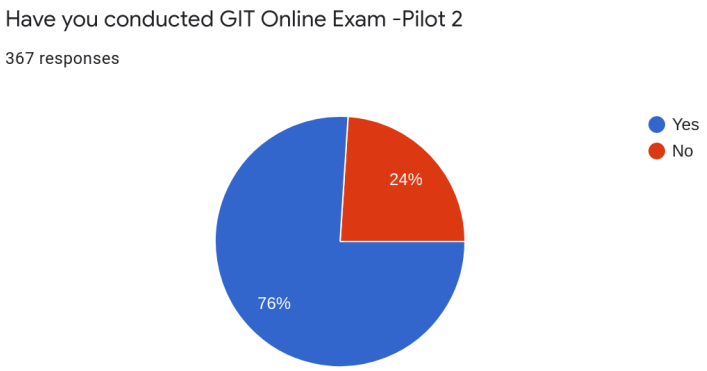


Figure 6.4: Participation of the Second Iteration

The results of the second iteration proved that a standalone server was available and operational throughout the examination period with few disruptions. During the second iteration, power outages and lightning caused disruptions to the standalone system and such factors were beyond anyone 's control. As per the results of the servery, there was a high participation (see Figure: 6.4) and high satisfaction rate (see Figure: 6.5) among the participants.

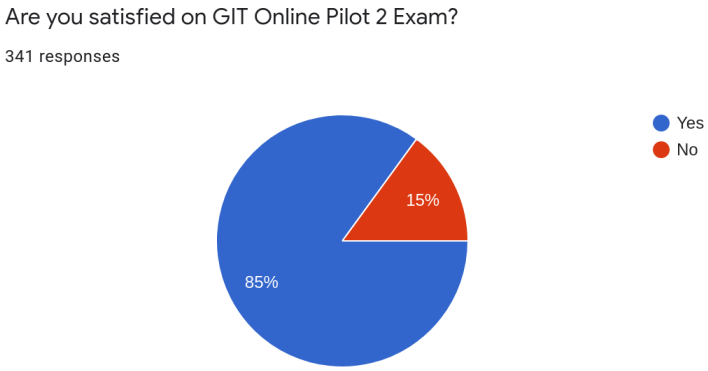


Figure 6.5: Satisfaction of the Second Iteration

6.4 Results of the Iteration-III

6.4.1 Results of the Iteration-III A

After observing the Iteration - III-A, it was found that the local server was not able to maintain the availability, and it started throwing timeout errors. Investigations found that the nature of Moodle, which is used as the examination platform, makes database writes when the user either switches to a new question or answers to the current question. This nature of Moodle creates many disk IO operations in addition to the IO operations generated by the operating system itself.

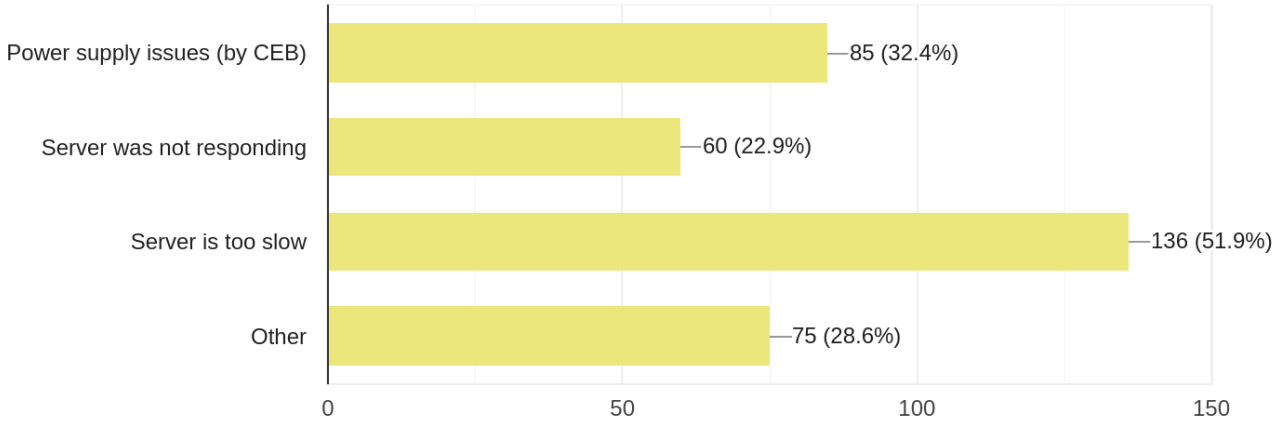


Figure 6.6: Issues of the Second Iteration

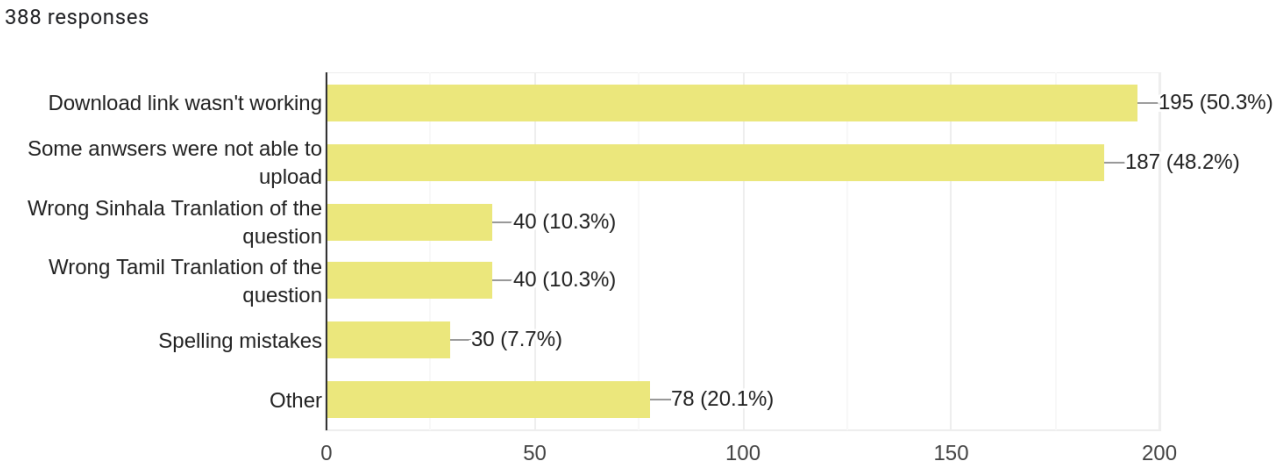


Figure 6.7: Third Iteration: Questions Related Issues

6.4.1.1 Boot into Volatile Memory

Then the same USB was tested with a specific boot option instead of default boot options. Entire Operating System was booted into volatile memory (RAM) and tested on the local examination server. The local server worked as expected but left the entire examination process in a high risk of losing data in case of system shutdown. It is possible to back up everything to another USB using the scheduled job, but there is a high chance of human error while handling two different types of USBs (one USB to boot the machine and another one to back up).

6.4.2 Results of the Iteration-III B

As given in the Figure: 6.8 during the third iteration over 60% of the participants were conducted the examination using local server.

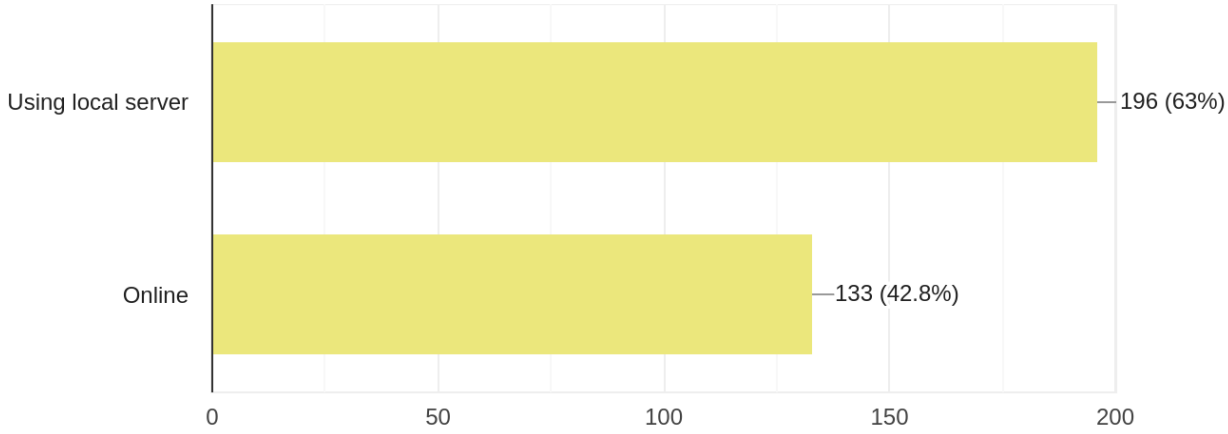


Figure 6.8: Third Iteration: Method used to conduct the examination

The next option was to deliver an installation DVD and deploy the server. As per Figure: 6.9, several issues reported and only 46.9% of them were able to start the examination on time.

Considering the results of the third iteration, following measures taken to avoid unnecessary delaying of the examination.

1. Introduced secure casing for installation media (DVD case)
2. Live USB option was discontinued
3. Advised service providers to review all hardware and repair them and produce a service report.

4. Requested examination centers to coordinate with regional power electricity suppliers and avoid their maintenance during the examination.

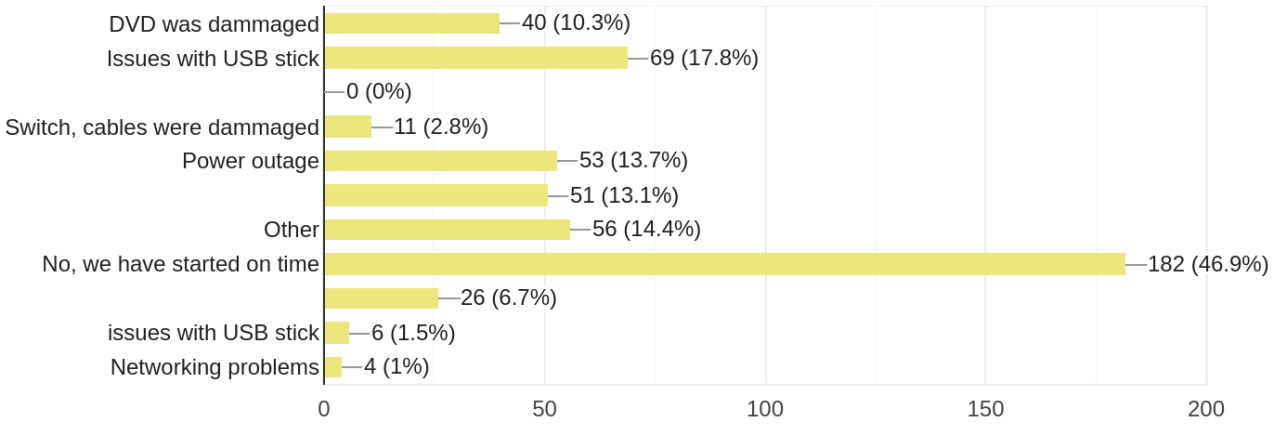


Figure 6.9: Third Iteration: Issues Impact on the Commence of the Examination

6.5 Evaluation Results of the Implementation

An online survey was conducted among examiners who involved with the implementation of the proposed solution. There were 242 officers were engaged with the survey by representing 242 out of 656 examination centers. Sample was distributed across the different districts in the country. Sample of the survey represent by the Figure: 6.10.

6.5.1 Installation of Local Server

Nearly 90% of participants were able to install the local server as given in the Figure: 6.11. This proves that given instructions in the installation guide and proved training programs were effective.

6.5.2 Usage of local server and online examination against the district

As given in the Figure: 6.12 and Figure: 6.13, other than Colombo district, there was high usage of the local server compared to the online examination server.

District

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Ampara	7	2.9	2.9	2.9
	Anuradhapura	20	8.3	8.3	11.2
	Badulla	13	5.4	5.4	16.5
	Batticaloa	2	.8	.8	17.4
	Colombo	35	14.5	14.5	31.8
	Galle	5	2.1	2.1	33.9
	Gampaha	15	6.2	6.2	40.1
	Hambantota	6	2.5	2.5	42.6
	Kalutara	5	2.1	2.1	44.6
	Kaluthara	1	.4	.4	45.0
	Kandy	17	7.0	7.0	52.1
	Kegalle	6	2.5	2.5	54.5
	Kilinochchi	1	.4	.4	55.0
	Kuliyapitiya	1	.4	.4	55.4
	Kurunegala	26	10.7	10.7	66.1
	Mannar	5	2.1	2.1	68.2
	Matale	11	4.5	4.5	72.7
	Matara	16	6.6	6.6	79.3
	Monaragala	7	2.9	2.9	82.2
	Nuwara Eliya	12	5.0	5.0	87.2
	Polonnaruwa	7	2.9	2.9	90.1
	Puttalam	2	.8	.8	90.9
	Ratnapura	16	6.6	6.6	97.5
	Trincomalee	5	2.1	2.1	99.6
	Vavuniya	1	.4	.4	100.0
	Total	242	100.0	100.0	

Figure 6.10: GIT2019: Selected sample of the survey

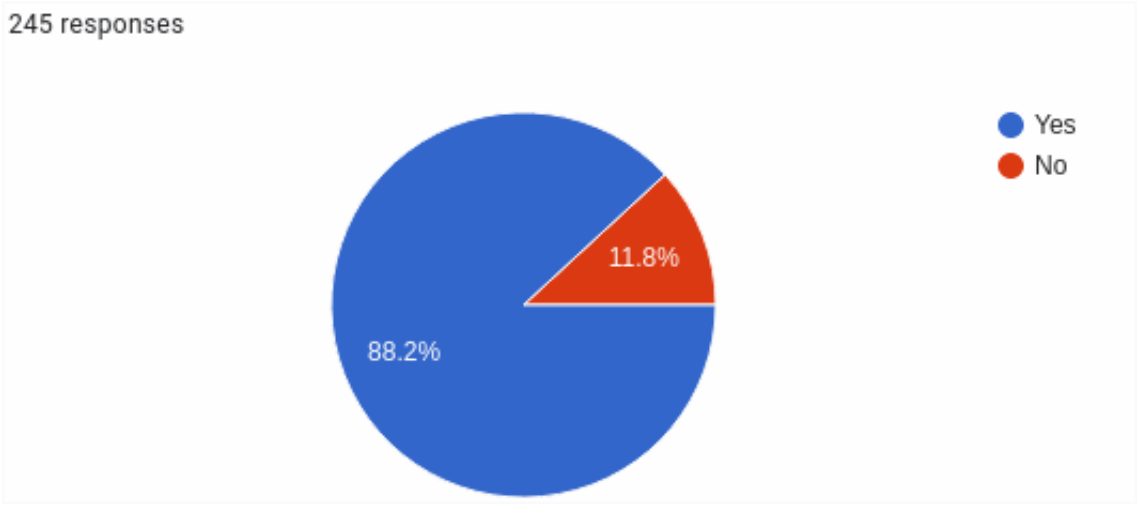


Figure 6.11: Ability to Install Local Server

		Local Server	Online	Total
District	Ampara	1	6	7
	Anuradhapura	19	1	20
	Badulla	10	3	13
	Batticaloa	2	0	2
	Colombo	17	18	35
	Galle	4	1	5
	Gampaha	11	4	15
	Hambantota	6	0	6
	Kalutara	4	1	5
	Kaluthara	1	0	1
	Kandy	12	5	17
	Kegalle	4	2	6
	Kilinochchi	1	0	1
	Kuliyapitiya	1	0	1
	Kurunegala	24	2	26
	Mannar	5	0	5
	Matale	9	2	11
	Matara	15	1	16
	Monaragala	7	0	7
	Nuwara Eliya	7	5	12
	Polonnaruwa	4	3	7
	Puttalam	2	0	2
	Ratnapura	13	3	16
	Trincomalee	5	0	5
	Vavuniya	1	0	1
Total		185	57	242

Figure 6.12: Usage of local server and online

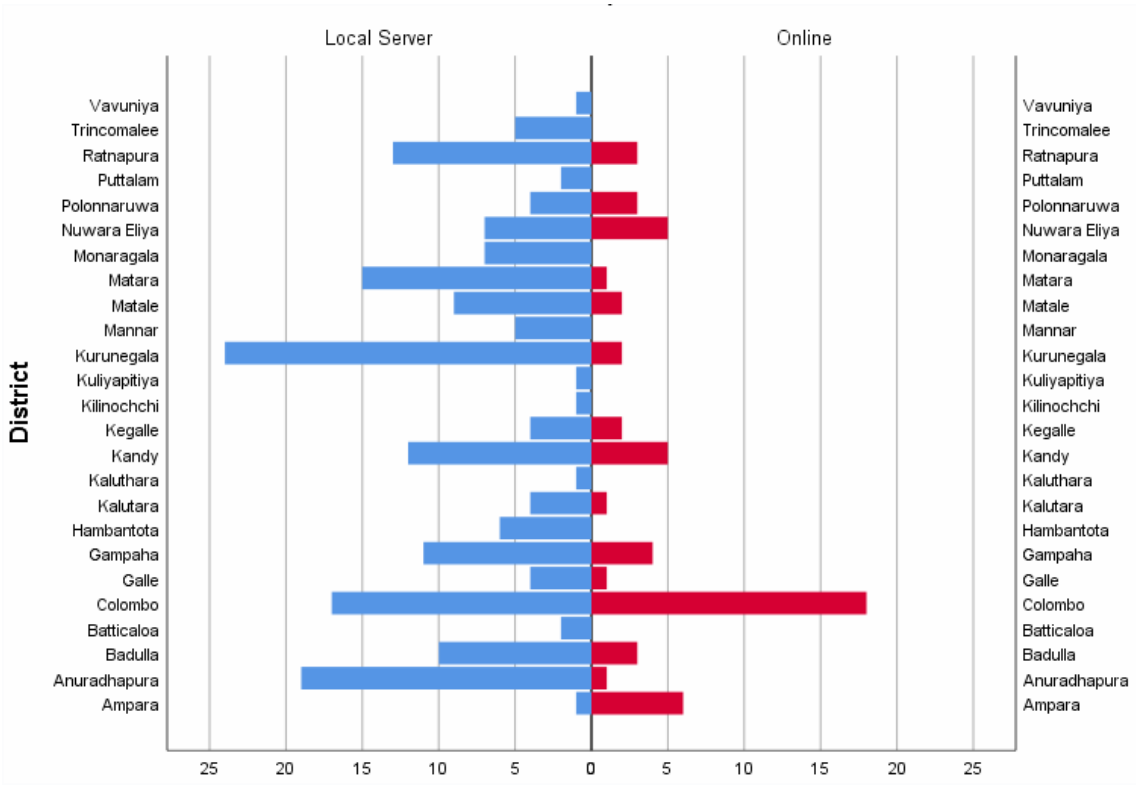


Figure 6.13: Usage of local server and online against the district

6.5.3 Ability to Reschedule an Examination

During the implementation, rescheduling of the examination was allowed under the approval of the Department of Examination. The examination centers, which were disrupted for more than 30 minutes, were allowed to reschedule the examination. As given in the Figure: 6.14, 39.2% of them conducted extra session due to the rescheduling of the examination session. This rescheduling of an examination proved that candidates have no risk of cancellation of examinations due to disruptions. Rescheduling of the examination in a center is independent of other centers.

6.5.4 Preference in the Next Examination

As a part of the same survey, users were able to mention there a preference in the next examination based on the previous experience they had. According to the Figure: 6.15 except Colombo district, many users prefer to use a local server compared to the online examination server.

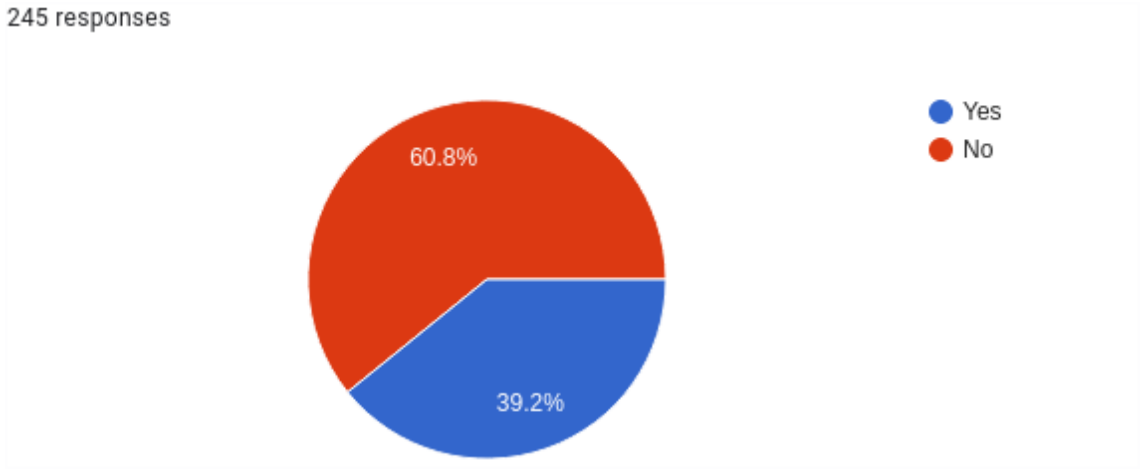


Figure 6.14: Rescheduling of Exams

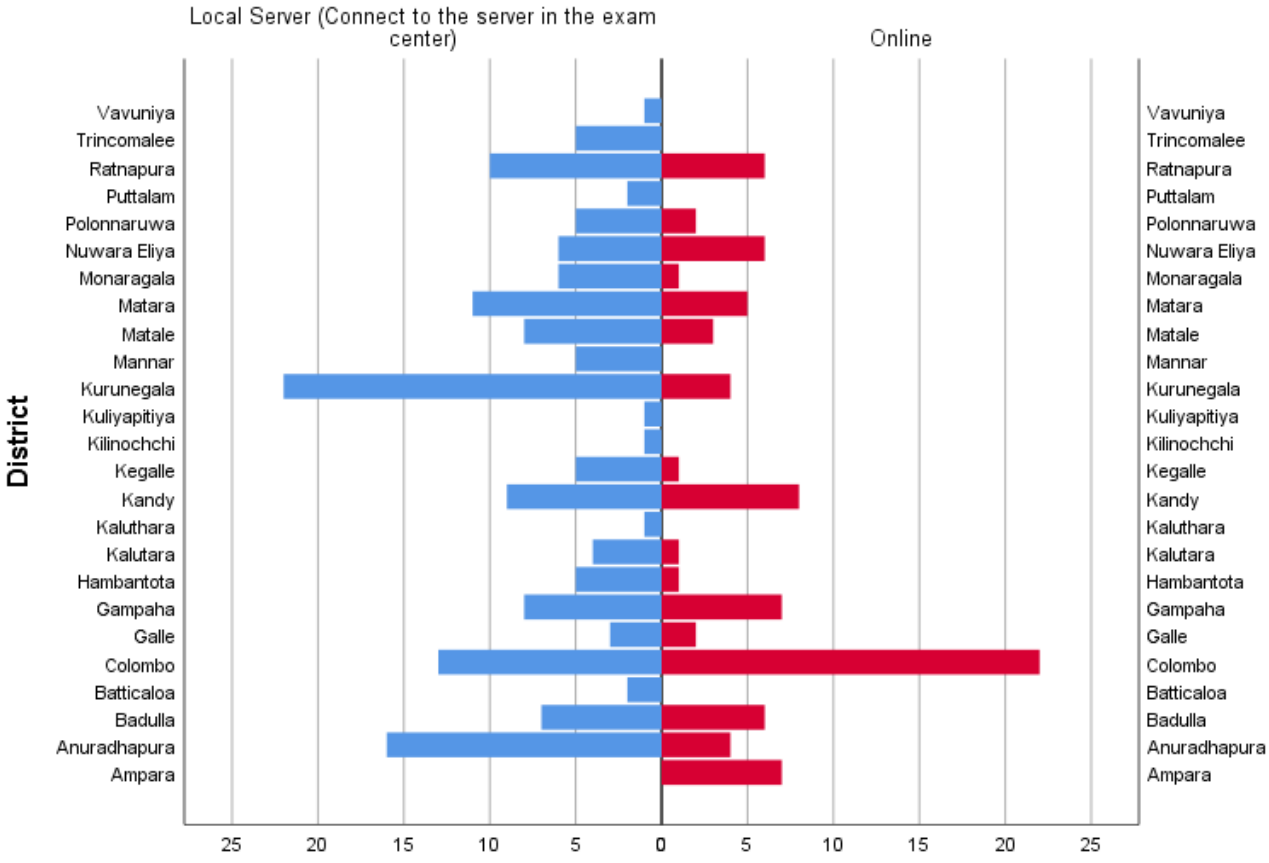


Figure 6.15: User preference for the next examination against the district

6.6 Administrative Incidents Reported During the Examination

As listed in the Appendix: E, administrative type incidents have reported during the examination and follow up investigations. The examiner should follow the standards, guidelines and recommendations to minimize administrative level incidents.

6.7 Other Factors Affecting to Success

Knowledge and skills of Supervisor who is the Level-I support in this examination system. S/he should have troubleshooting skills and escalate to relevant parties at the correct time. Especially supervisors should able to understand given instructions and follow guidelines and standards.

6.8 Synchronization Over the Internet

Both examination and Evaluation servers capable of Synchronized encrypted backups over the Internet. This feature was enabled by rsync over secure shell. This feature was appreciated as it provided additional method to synchronize secure backups directly into the Department of Examinations.

6.9 State Transition Diagram

The entire proposed protocol evaluated separately for the examination and evaluation. The protocol evaluated by state transition diagram.

6.9.1 Examination Module of the Secure Protocol

Examination module of the proposed protocol have evaluated by the State Transition Diagram as in Figure: 6.16. It includes all verification stages including checking availability of the ICT center, verification of the specification, installation media and the media transferring the examination paper.

According to the Figure: 6.16, there is a possibility of extending the if the examination is disrupted for less than 30 minutes. In case the disruption is more than 30 minutes, officials make a decision on re-scheduling the examination to a different examination session. Rescheduling of

an examination can be located to either on same examination center or a different examination center. As per the Figure: 6.14, over 39% of the examiners had to reschedule exams.

At the end of the examination, taking the backup in to two USB device (dual backup), update the chain of custody and hand them over to verified and authorized person to return them back to the Department of Examinations. Server data is securely wiped with an approval before ending the examination session.

6.9.2 Evaluation Module of the Secure Protocol

Evaluation module of the proposed protocol have evaluated by the State Transition Diagram as in Figure: 6.17. The evaluation process of the examination explained above in the Section: 6.9.1.

At the last stage of the evaluation, taking the backup in to two USB device (dual backup), update the chain of custody and hand them over to verified and authorized person to return them back to the Department of Examinations. Server data is securely wiped with an approval before ending the entire evaluation session.

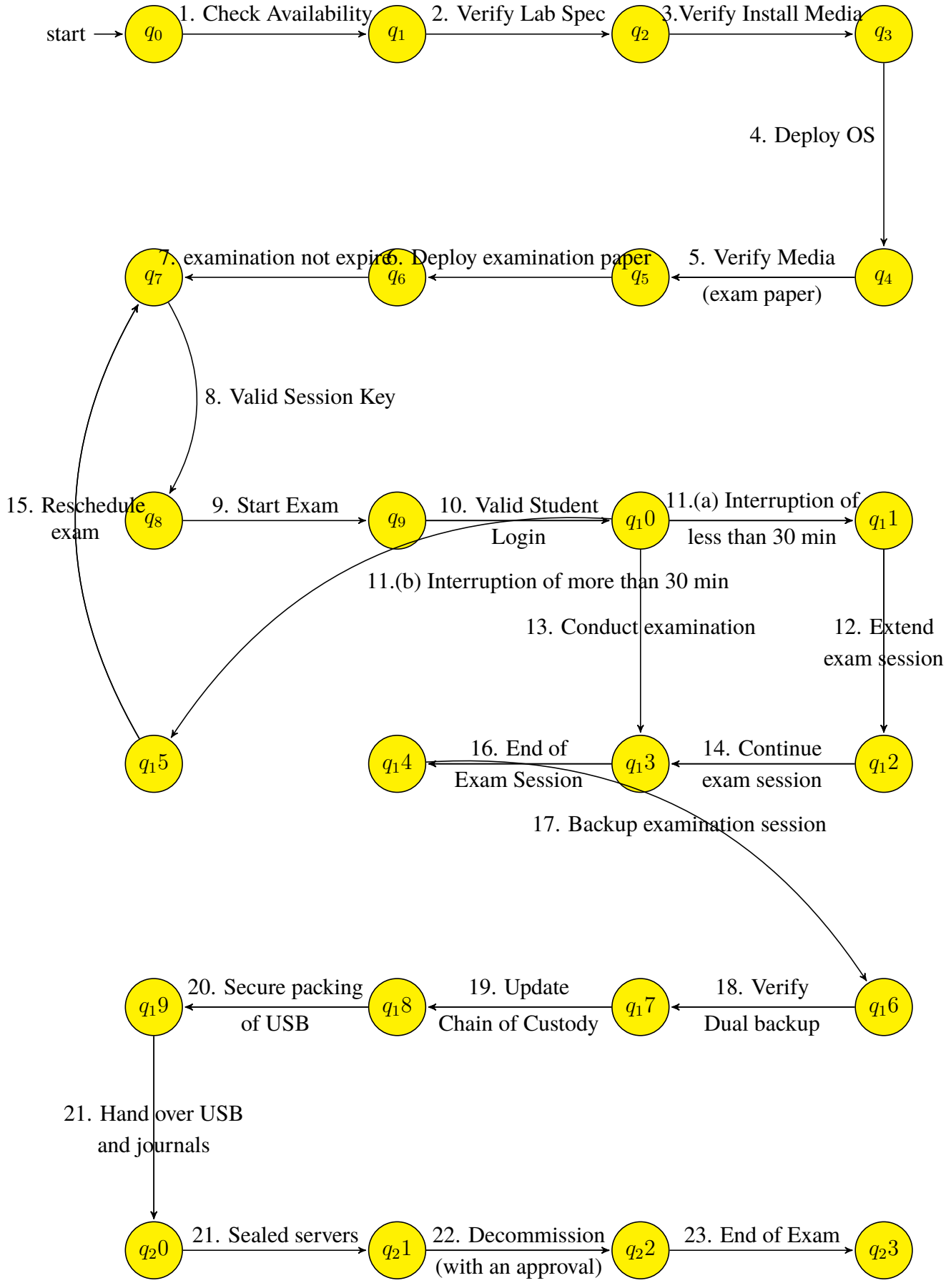


Figure 6.16: State Transition Diagram of the Examination

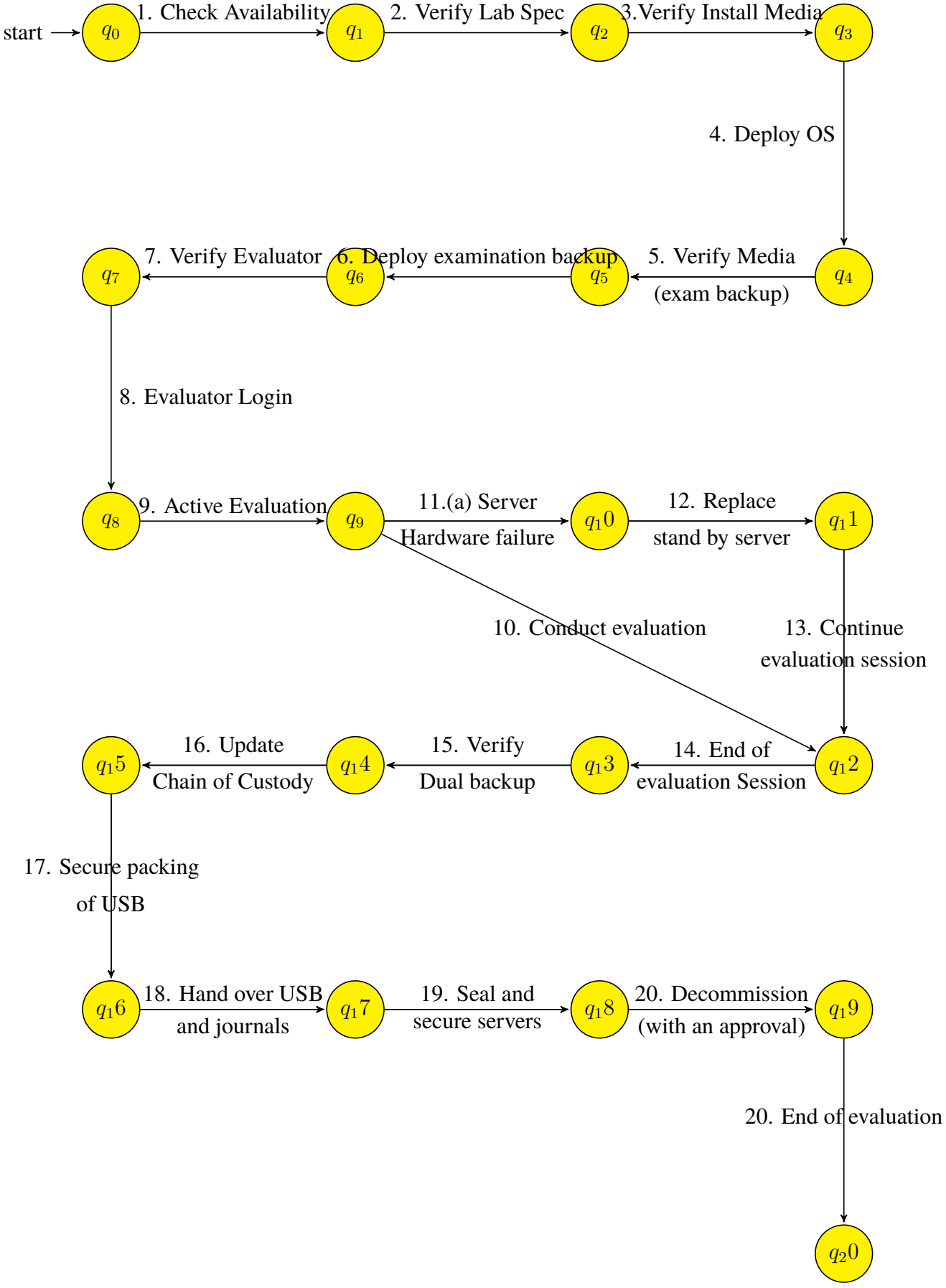


Figure 6.17: State Transition Diagram of the Evaluation

6.10 Summary

The results of this research indicated that it is practically possible to deliver online examination to disrupted and disconnected regions using the proposed security protocol.

The next chapter, Chapter 7, is the final chapter. Conclusion and future work are presented in the next chapter.

Chapter 7

CONCLUSION AND FUTURE WORK

7.1 Overview

The outcome of this research is summarized in this chapter. The first section of this chapter discusses the conclusion and followed by a separate section for future work.

7.2 Conclusion

The objective of this research was to propose a secure protocol to deliver a computer-based examinations in disrupted and disconnected regions. The security protocol use necessary and appropriate physical, administrative and technical controls.

The related technologies, solutions Delay Tolerant Networks based community projects, legal background and security requirements principals are considered in designing the proposed protocol. Especially, the protocol designed followed the principle of "Secure by Design", which included Threat Modelling followed by a Risk Assessment. The research methodology was a mixture of action research and survey.

There were several iterations of developments and observations conducted prior to finalizing the design. First iteration was conducted as an online examination using a central examination server. As per the results of the servery, there was a high participation and high satisfaction rate among the participants. The high rate of user satisfaction implied that the provided Moodle based examination platform was up to the user satisfaction.

As disruptions were observed during the first iteration, it was decided to conduct the second iteration using standalone server. A customized Linux ISO have been built and distributed 2000 DVD copies to selected school along with installation guide. Then the second iteration was

completed followed by a survey. Based on the survey results of second iteration, third iteration was planned and executed with two approaches. First approach was to use USB pen drives to boot the examination server where customized Linux Operating System installed in to the USB drive. In this approach Operating System load into in memory. Though this approach was operationally easier when booting the examination server but a performance issue observed. Second approach replaced the use of in-memory system by installing each local server using an installation media (Install DVD/USB) with the help of a technical team. Third iteration followed with a survey to observe issues during the examination process.

The implementation was evaluated using survey and the evaluation of proposed protocol was presented through State Transition Diagrams. However, the obtained results indicate that the implemented secure Delay Tolerance Protocol enabled to conduct an computer-based examination effectively and securely in a disrupted and disconnected environment.

Both the third iteration and the implementation of the secure protocol facilitated to conduct an online examination with over 180,000 candidates and hundreds of officials dispersed all over the island. The overall examination was conducted smoothly by the Department of Examination and it became the first-ever computer-based examination conducted in Sri Lanka with such a big number of candidates.

The sustainability of the process of conducting computer-based examinations is also a changeable task with the rapid advancement of the technologies. The organizations involving such tasks, therefore, needed to be proactive with their work and future developments.

7.3 Future Work

Risk Management is an ongoing activity that depends on how often the technology and architecture are changed within the organisation. It is highly essential to identify the people, process and technology that is critical to the computer-based examination process and help to assess the associated risk. Risk Management and Risk Assessment are essential parts of Information Security Management. A continuous Risk Assessment and Risk Management should be a part of future enhancement. Either the audit branch or the finance branch of the Department of Examinations should take ownership of the Risk Assessment process. Risk Assessment included identification of hazards, analysis of risks, and evaluate risks.

Moreover, paperless verification of identity would be a great value addition as all the candidates could attend the examination without official admission during a post-disaster situation or the department may not able to send admissions on time.

7.4 Concluding Remarks

This study has shown that, with the use of the physical, administrative and technical controls a computer-based examination can be securely delivered and execute in a disrupted and disconnected environment while maintaining Confidentiality, Integrity and Availability. Finally, research findings have been discussed with respect to the Department of Examination environment and local context.

Bibliography

[1] L. Kleinrock, "An early history of the internet [history of communications]." IEEE Communications Magazine, 2010, pp. 26–36, last accessed 20 June 2020. [Online]. Available: https://ieeexplore.ieee.org/document/5534584

[2] W. Foundation, "Half of the world 's people are still offline. how do we connect them as quickly as possible?" 2019, last accessed 20 June 2020. [Online]. Available: https://webfoundation.org/2019/02/half-of-the-worlds-people-are-still-offline-how-do-we-connect-them-as-quickly-as-possible/

[3] S. Jayasuriya, P. Steele, D. Weerakoon, M. Knight-John, and N. Arunatilake, "Post-tsunami recovery: Issues and challenges in sri lanka," 01 2005, last accessed 20 June 2020. [Online]. Available: https://www.adb.org/sites/default/files/publication/157220/adbi-rp71.pdf

[4] V. Cerf and R. Kahn, "A protocol for packet network intercommunication," *IEEE Transactions on Communications*, vol. 22, no. 5, pp. 637–648, 1974.

[5] W. Forrest, "Delay- and disruption-tolerant networks (dtns) a tutorial," 2015. [Online]. Available: http://ipnsig.org/wp-content/uploads/2015/09/DTN_Tutorial_v3.2.pdf

[6] A. Armbrecht, "4 reasons 4 billion people are still offline," last accessed 20 June 2020. [Online]. Available: https://www.weforum.org/agenda/2016/02/4-reasons-4-billion-people-are-still-offline/

[7] "UN broadband commission sets global broadband targets to bring online the worldâĂŹs 3.8 billion not connected to the internet," 2018, last accessed 20 June 2020. [Online]. Available: https://www.itu.int/en/mediacentre/Pages/2018-PR01.aspx

[8] "Internet for all, a framework for accelerating internet access and adoption," 2016. [Online]. Available: http://www3.weforum.org/docs/WEF_Internet_for_All_Framework_Accelerating_Internet_Access_Adoption_report_2016.pdf

[9] L. T. K. F. V. C. B. D. Scott Burleigh, Adrian Hooke, K. Scott, and H. Weiss, "Delay-tolerant networking: An approach to interplanetary internet," pp. 128–136, 2003. [Online]. Available: https://www.itu.int/en/mediacentre/Pages/2018-PR01.aspx

[10] R. S. P. R. NIKOLAOS L AOUTARIS, GEORGIOS SMARAGDAKIS and R. SUNDARAM, "Delay-tolerant bulk data transfers on the internet." IEEE, 2013, pp. 1852 – 1865.

[11] D. Z. Kasun and K. Chamath, "Busnet - a sensor network built over a public transport system," in *Proceedings of the 4th European conference on Wireless Sensor Networks*, 2007.

[12] R. F. Alex Pentland and A. Hasson, "Daknet: Rethinking connectivity in developing nations," 2004, p. 78.

[13] S. A. L. Pei Zhang, Christopher M. Sadler and M. Martonosi, "Hardware design experiences in zebranet," 2004. [Online]. Available: https://www.princeton.edu/~mrm/sensys04.pdf

[14] Y. W. M. M. L.-S. P. Philo Juang, Hidekazu Oki and D. Rubenstein, "Energy-efficient computing for wildlife tracking: Design tradeoffs and early experiences with zebranet." International Conference on Architectural Support for Programming Languages and Operating Systems (ASPLOS-X), San Jose, California, USA,, 2002, pp. 96–107. [Online]. Available: https://dl.acm.org/doi/pdf/10.1145/635508.605408

[15] M. D. C. J. E. Jacob Sorber, Aruna Balasubramanian and C. Qualls, "Tula: Balancing energy for sensing and communication in a perpetual mobile system." IEEE TRANSACTIONS ON MOBILE COMPUTING, 2013, pp. 804–816.

[16] M. U. Avri Doria and D. P. Pandey, "Providing connectivity to the saami nomadic community," vol. 7. ACM SIGMOBILE Mobile Computing and Communications Review, 2003, last accessed 20 June 2020. [Online]. Available: http://www.diva-portal.org/smash/get/diva2:1000353/FULLTEXT01.pdf

[17] M. Nagy, "Secure and usable services in opportunistic networks," PhD dissertation, Aalto University, School of Electrical Engineering, 2019. [Online]. Available: https://aaltodoc.aalto.fi/handle/123456789/38783

[18] D. M. Inventor: Amir Ban and O. Ogdan, "Architecture for a usb-based pc flash disk storage card," Patent, 1999. [Online]. Available: https://patents.google.com/patent/DE60043623D1/en

[19] C. F. Dominique BriÃÍre and P. Traverse, "A study on a secure usb mechanism that prevents the exposure of authentication information for smart human care services," vol. 2001, 2001. [Online]. Available: https://davi.ws/avionics/TheAvionicsHandbook_Cap_12.pdf

[20] K. F. Sushant Jain and R. Patra, "Routing in a delay tolerant network." ACM SIGCOMM Computer Communication Review 34(4), 2004, pp. 145–158.

[21] H. C. Mohammed Al-Siyabi and Z. Sun, "Delay/disruption tolerant network architecture for aircrafts datalink on scheduled routes." Personal Satellite Services - Second International ICST Conference, PSATS 2010, Rome, Italy, 2010, pp. 235–248.

[22] Y. L. H. L. K. Y. Kyungroul Lee, Insu Oh and J. Seo, "Electrical flight controls, from airbus a320/330/340 to future military transport aircraft: A family of fault-tolerant systems," 2000. [Online]. Available: https://davi.ws/avionics/TheAvionicsHandbook_Cap_12.pdf

[23] "General data protection regulation(gdpr)," last accessed 20 June 2020. [Online]. Available: https://gdpr-info.eu/

[24] B. C. Qionglu Zhang, Shijie Jia and B. Chen, "Ensuring data confidentiality via plausibly deniable encryption and secure deletion âĂŞ a survey."

[25] "Aws snowball," 2020, last accessed 20 June 2020. [Online]. Available: https://aws.amazon.com/snowball/

[26] "Aws snowball user guide," 2020, last accessed 20 June 2020. [Online]. Available: https://docs.aws.amazon.com/snowball/latest/ug/AWSSnowball-ug.pdf

[27] M. J. Sumedha Chauhan and A. K. Kar, "The acceptance of electronic voting machines in india: a utaut approach," in *Electronic Government an International Journal*, 2018. [Online]. Available: https://www.researchgate.net/publication/326642813_The_acceptance_of_electronic_voting_machines_in_India_A_UTAUT_approach

[28] D. A. Kumar and T. U. S. Begum, "Electronic voting machine âĂŞ a review," in *Proceedings of the International Conference on Pattern Recognition, Informatics and Medical Engineering*. IEEE, 2012. [Online]. Available: https://ieeexplore.ieee.org/document/6208285

[29] E. C. O. INDIA, “Evm brochure for electors,” 2019. [Online]. Available: https://eci.gov.in/files/file/11411-evm-broucher-for-electors/

[30] T. Jabbarifar, “The importance of classroom assessment and evaluation in educational system,” 2000. [Online]. Available: https://pdfs.semanticscholar.org/db8c/4d3e5e56aa80c220e17eeac25183acaaa43d.pdf

[31] “Moodle,” last accessed 20 June 2020. [Online]. Available: https://moodle.org/

[32] “Moodle download stats,” last accessed 20 June 2020. [Online]. Available: https://download.moodle.org/local/downloadmoodleorg/stats.php

[33] “Moodle plugins portal,” last accessed 20 June 2020. [Online]. Available: https://moodle.org/plugins/

[34] R. M. H. Borromeo, “Online exam for distance educators using moodle,” 2013. [Online]. Available: https://ieeexplore.ieee.org/document/6820155

[35] “Goals of an online assessment system,” last accessed 20 June 2020. [Online]. Available: https://docs.moodle.org/dev/Goals_of_an_online_assessment_system

[36] M. B. B. Sithara H. P. W. Gamage, Jennifer R. Ayres and E. J. Smith, “Optimising moodle quizzes for online assessments,” 2019. [Online]. Available: https://stemeducationjournal.springeropen.com/track/pdf/10.1186/s40594-019-0181-4

[37] “Safe exam browser,” last accessed 20 June 2020. [Online]. Available: https://www.safeexambrowser.org/about_overview_en.html

[38] “Safe exam browser repo,” last accessed 20 June 2020. [Online]. Available: https://github.com/SafeExamBrowser

[39] The Parliament of the Democratic Socialist Republic of Sri Lanka., “Public examinations act (no. 25 of 1968),” 1968, last accessed 20 June 2020. [Online]. Available: https://www.lawnet.gov.lk/1946/12/31/public-examinations-6/

[40] The Parliament of, the Democratic Socialist Republic of Sri Lanka, “Evidence (special provisions) act (no. 14 of 1995),” 1995, last accessed 20 June 2020. [Online]. Available: https://www.lawnet.gov.lk/1946/12/31/evidence-special-provisions-2/

[41] The Parliament of the Democratic Socialist Republic of Sri Lanka, "Electronic transactions (no. 19 of 2006)," 2007, last accessed 20 June 2020. [Online]. Available: http://www.commonlii.org/lk/legis/num_act/et19o2006281/

[42] S. Marsoof, "Electronic and computer evidence in proceedings before courts and labour tribunals.pdf," *Bar Association Law Journal*, 2011, last accessed 20 June 2020. [Online]. Available: https://www.academia.edu/38507680/Electronic_and_Computer_Evidence_in_Proceedings_before_Courts_and_Labour_Tribunals.pdf

[43] The Parliament of the Democratic Socialist Republic of Sri Lanka, "Personal data protection act- draft," 2019.

[44] D. Sule, "Importance of forensic readiness." ISACA JOURNAL, 2014. [Online]. Available: https://www.isaca.org/resources/isaca-journal/past-issues/2014/importance-of-forensic-readiness

[45] R. Rowlingson, "A ten step process for forensic readiness," vol. 2. International Journal of Digital Evidence, 2004.

[46] E. Huebner and F. Henskens, "The role of operating systems in computer forensics," 2008. [Online]. Available: https://dl.acm.org/doi/pdf/10.1145/1368506.1368508?download=true

[47] B. Potgieter, C. Lew, and J. Botha, "Evidence that use of the itil framework is effective," 01 2005. [Online]. Available: http://citrenz.ac.nz/conferences/2004/potg_itil.pdf

[48] F. Salahdine and N. Kaabouch, "Social engineering attacks: A survey," *Future Internet*, vol. 11, 04 2019. [Online]. Available: https://www.researchgate.net/publication/332151597_Social_Engineering_Attacks_A_Survey/fulltext/5ca4c0dda6fdcc12ee8fceca/Social-Engineering-Attacks-A-Survey.pdf

[49] A. Gutmann, K. Renaud, J. Maguire, P. Mayer, M. Volkamer, K. Matsuura, and J. MÃijller-Quade, "Zeta-zero-trust authentication: Relying on innate human ability, not technology," in *2016 IEEE European Symposium on Security and Privacy (EuroS P)*, 2016, pp. 357–371. [Online]. Available: https://ieeexplore.ieee.org/document/7467365

[50] N. The, United, "Universal declaration of human rights," 1948, last accessed 20 June 2020. [Online]. Available: hhttps://www.un.org/en/universal-declaration-human-rights/

[51] R. Davison, M. Martinsons, and N. Kock, “Principles of canonical action research,” *Inf. Syst. J.*, vol. 14, pp. 65–, 01 2004.

[52] The Parliament of the Democratic Socialist Republic of Sri Lanka, “Computer crime act, no. 24 of 2007,” 2007, last accessed 20 June 2020. [Online]. Available: https://www.cert.gov.lk/Downloads/Acts/Computer_Crimes_Act_No_24_of_2007(E).pdf

[53] The Parliament of the Democratic Socialist Republic of Sri Lanka., “Intellectual property act (no. 36 of 2003),” 2003, last accessed 20 June 2020. [Online]. Available: http://www.commonlii.org/lk/legis/num_act/ipa36o2003314/

Appendix A

Survey of Iteration-I

Following are the list of questions included in the survey.

01. Name
02. Contact number
03. Email address
04. Designation
05. School/Department
06. Examination Center ID
07. District
08. Operating System used in student machines
09. Internet Service Provider
10. Have you conducted GIT Online Exam– Pilot 1?
11. What is the duration the GIT Online Exam – Pilot 1
12. What were the issues you had during GIT Online Exam – Pilot 1?
13. What is your feedback on GIT Online Exam – Pilot 1?
14. Are you satisfied on GIT Online Pilot 1 Exam?

Appendix B

Survey of Iteration-II

Following are the list of questions included in the survey.

01. Name
02. Contact number
03. Email address
04. Designation
05. School/Department
06. Examination Center ID
07. District
08. Operating System used in student machines
09. Internet Service Provider
10. Have you conducted GIT Online Exam– Pilot 2?
11. What is the duration of the GIT Online Exam – Pilot 2?
12. What were the issues you had during GIT Online Exam – Pilot 2?
13. What is your feedback on GIT Online Exam – Pilot 2?
14. Are you satisfied on GIT Online Pilot 2 Exam?

Appendix C

Survey of Iteration-III

01. Name
02. Contact number
03. Email address
04. Designation
05. School/Department
06. Examination Center ID
07. District
08. Operating System used in student machines
09. Did you attend provincial awareness program?
10. Was the awareness program useful?
11. What is your feedback on awareness Program?
12. Do you think you should have enough training?
13. What kind of additional training/awareness you need (Installation ,
14. Please explain if you choose 'other' in the previous question.
15. When did you collect installation media? (date & time)
16. How did you install the media?
    * I myself installed it
    * Technical Team installed it
    * I installed the media in other centers as well
    * Someone helped me over the phone
    * Other
17. Please explain if you choose 'other' in the previous question.

18. Was the coordinating centre people helpful during the distribution
19. Please explain if you choose 'No' or 'Moderate' in the previous qu

= Issues occurred during the GIT Pilot3 Exam =

20. Could not start exam on time
    * DVD was damaged
    * Issues with USB stick
    * I did not know how to change network IP range
    * Switch, cables were damaged
    * Power outage
    * Server down (when we were using onlineexams.gov.lk)
    * Other
    * No, we have started on time
21. Please explain if you choose 'other' in the previous question.
22. How did you conduct the exam?
    * Online
    * Using the local server
23. Were there any issues related to local server?
    * No
    * Yes
24. Please explain the issue if you had issues with local server.
25. Were there any issues related to online system?
26. Please explain the issue if you had issues with online server.
27. What are the questions related issues?
    * Download link wasn't working
    * Some answers were not able to upload
    * Wrong Sinhala Translation of the question
    * Wrong Tamil Translation of the question
    * Spelling mistakes
    * Other
28. Please explain what did you mean by 'other issues' in previous ques
29. Were you satisfied with the support given by vendors and service pr
30. Please explain if your answer is 'No' or 'Moderate'.
31. Who was the Internet Service Provider

32. Were you satisfied with the support given by Ministry of Education?
33. Please explain if your previous answer is 'No' or 'Moderate'.
34. Comments and Suggestions

Appendix D

Survey of Implementation

01. Your Name
02. Contact Number
03. Email address
04. District
05. What was your exam centre number GIT exam (Conducted in Oct 2019)?
06. What was the method use for GIT exam (Conducted in Oct 2019)?
07. How many sessions were conducted for the exam by local server?
08. How many sessions did you conduct the exam in the online server?
09. Have you conducted any extra session (9th Day)?
10. Which method are you preferring to use for the next exam?
11. What is the reason to select the above option?
12. What were the issues you had during last exam?
13. Please explain if you choose 'other' in the previous question.
14. Please describe above issues in detail.
15. Were you able to install and setup local server?
16. Is your centre ready to run the next exam?
17. Does your centre have a proper internet connection to run the next
18. Suggestions and comments

Appendix E

Administrative Incidents Reported During the Examination

1. Use of different index number(sitting on wrong place and using o
2. Appearing on a different examination centre.
3. Wrong candidate signature.
4. Late attendance.
5. Appearing without an admission card.
6. Getting different medium other than the requested medium.
7. Inability to present a valid identity card.
8. Wrong ID number.
9. Signing on a different admission card.