DEVELOPING A THREAT MATRIX FOR SMART MOBILE DEVICES IN A UNIVERSITY NETWORK TOWARDS A SECURE LOCAL AREA NETWORK ECOSYSTEM

Irene Wanjiru Wanja

A Thesis Report Submitted to the Institute of Postgraduate Studies of Kabarak University in Partial Fulfillment for the Requirement for the Award of the Degree of Master of Science in Information Technology Security and Audit

KABARAK UNIVERSITY

NOVEMBER 2018

DECLARATION

Declaration

The thesis report is my work and to the best of my knowledge it has not been submitted to any other university previously for degree award.

Signed: ……………………………………… Date …………………………….

Irene Wanjiru Wanja

GMI/NE/0760/05/16

RECOMMENDATION

To the Institute of Postgraduate Studies:

The thesis entitled “Developing a threat matrix for smart mobile devices in a university network towards a secure local area network ecosystem” and written by Irene Wanjiru Wanja is presented to the Institute of Postgraduate Studies of Kabarak University. We have reviewed the research thesis and recommend it be accepted in partial fulfillment of the requirement for award of the degree of Master of Science in IT Security and Audit.

Signed: …………………………………….. Date …………….............................

Prof. Kefa Rabah
School of Computer Science and Bioinformatics,
Kabarak University

Signed: ……………………………………... Date …………….........................

Prof. Simon Maina Karume
Department of Computing and Informatics,
Laikipia University

COPYRIGHT

DEDICATION

I dedicate this research to my daughter Mary Magdaline Wanja and my mother Charity Mutahi.

ACKNOWLEDGEMENTS

I give glory and Honor to the Almighty God for His provision of wisdom, strength and wellbeing and for the gift of life, family, friends and provision without which I would not have made it this far in my academic pursuits. I owe a lot to Kabarak University for giving me resources to pursue my education. My sincere gratitude goes to my supervisors Prof. Kefa Rabah and Prof. Simon Maina Karume. Your guidance and counsel made this research possible. I would also like to acknowledge the efforts of every person who encouraged, supported in various ways during the period I was writing this thesis. May God bless you all.

ABSTRACT

The need by staff and students to use smart mobile devices in university network is indisputable. This is because they help them to work and study more effectively as well as achieve better work-life balance. However smart mobile devices pose a security challenge as they continue to expand the corporate network unchecked thus increasing the attack surface. This creates a major security burden to security professionals who are supposed to ensure that smart mobile devices' adherence to the security policy. The purpose of this study was to propose a solution on how to determine the likelihood of threat attack in a university network. The objectives of the study were to assess threats introduced to the university network through smart mobile devices, to develop a threat matrix that computes likelihood of threat attack, to identify security requirements needed for a secure university LAN ecosystem and to test and validate the matrix. Case study research design was adopted where Egerton University was selected as a case study with 384 respondents from all the campuses as target population. Response rate of 80% was recorded and considered sufficient for the study. The matrix was designed based on five of the ISO 27001's domains which closely relate to operation of smart mobile devices in a corporate network. Regression analysis was used to determine the Functional weights to compute likelihood of attack. The matrix was implemented as a web-based application using Hypertext Preprocessor (PHP) as server-side scripting language, MySQL was employed as a database engine and Bootstrap 4 was used for styling user interface. The developed threat matrix acted as threat and risk assessment tool to provide recommendations that maximize the protection of confidentiality, integrity and availability of university data while still providing functionality and usability of smart mobile devices.

Key words: smart mobile devices**,** security threats, security requirements, threat matrix

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF EQUATIONS

ABBREVIATIONS

COBIT - Control Objectives for Information and Related Technology

ICT – Information Communication Technology

IOT – Internet of Things

IS – Information system

ISMS - Information security management system

ISO - International Standards Organization

IT – Information Technology

LAN – Local Area Network

NIST - National Institute of Standards and Technology

SMD – Smart Mobile Devices

TM- Threat Matrix

WLAN – Wireless Local Area Network

OPERATIONAL DEFINITIONS OF TERMS

The key terms used in this study were given the following operational definitions;

Security: Refers to provision of core values of information security assurance which include confidentiality, availability, integrity, authentication, authorization and non-repudiation (Heer, Garcia-Morchon, Hummen, Keoh, Kumar & Wehrle, 2011)

Security policy: This is a document that explains the physical and logical plan with an aim of protecting the information system core values while providing operational mechanism for secure cryptographic key distribution and non-repudiation (Shafagh & Hithnawi, 2014).

Smart mobile device: This is an electronic gadget that is able to connect to other devices or networks through various types of wireless protocols such as Wi-Fi, NFC, 3G, 4G, Bluetooth etc, the device can share and interact with its user and other smart mobile devices. Examples include smart phones, tablets, smart-watches, smart bands and smart key chains (Techopedia Dictionary, 2018).

Threat: This is the likelihood of a particular threat-source to exercise vulnerability or a weakness that can be accidentally triggered or intentionally exploited (Goguen & Fringa, 2002).

Threat matrix: This is a threat assessment tool that identifies threat attributes to help analyst characterize threats based on their overall capabilities (Mateski *et al.*, 2012). This is important in making decisions on how to improve security countermeasures and to improve security during operations.

CHAPTER ONE
INTRODUCTION

1.1 Background of the Study

A university local area network (LAN) consist of a group of computers and associated devices from various faculties and departments within the university that share a common communications line or wireless link to a server. These computers and other smart mobile devices use LAN connection to share resources such as a printer or network storage. Smart mobile devices (SMD) on the other hand refers to any physical object associated with computing resources and is capable of transmitting data to other similar objects either through physical transmission medium and logical protocols or with human through the device user interface (Mohammed, 2010). A university local area network comprise of interconnected key departments and other offices within a university campus or campuses. This may include administrative departments, residence halls, libraries, Lecture halls, student centers and athletic facilities. The nodes are usually interconnected either through wired or wireless means. Wi-Fi hotspots are one of the wireless means whereby users connect their smart mobile devices such as smart mobile phones, notebook, tablet or laptop computers to the university network. This enables staff; students and other stakeholders to conduct research communicate and carry on with their duties.

BYOD (Bring Your Own Device) is a technology, concept or strategy for employees and in this case students prefer working with their personal smart mobile devices such as smart phones, tablet PCs and laptop computers to access corporate internal resources such as database and applications. With the introduction of BYOD, corporate internal infrastructures have moved from a closed to an open environment. This means that it is now possible to gain access to corporate servers for work and other services from every point of connection through Internet using personal smart mobile devices. This was only possible inside corporate network in the past.

The use of personal devices have been enhanced as a result of the following; popularization of smart mobile devices including tablet PC and smart phone, implementation of the wireless Internet environment, increased importance on real-time communication and work continuity (Koh & Im, 2014). Staff and students are more comfortable using their own devices due to convenience of accessing the university information from anywhere at any time. Staffs become more productive since they are able to continue working even beyond the normal working hours. The university on the other hand is able to save on cost of procuring computing devices since most of the users prefer using their own devices (Calder, 2013). The use of smart mobile devices in a corporate network has introduced the need manage and control devices and data not only in an IT department inside a company but also by individual users. Hence security policies should be focused on both user-centered security policies and devices-centered security policies. With the advent of BYOD it has become necessary to supervise not only a specific point of access but also all points of access to corporate network.

According to Ernest and Young (2013) introduction of BYOD technology in an organization is more likely to expand the risk landscape and is capable of increasing certain risks. The majority of universities allow use of personally owned smart mobile devices due to insufficient IT resources available to support their ever growing number of staff and students (Hossain *et al.*, 2015). To enhance the benefits brought about by use of smart mobile devices in a corporate environment security issues must be addressed. According to Miller, Voas and Hurlburt (2012) smart mobile devices contain a wealth of personal information which may be mixed with corporate information stored on the same device. This creates the need to control access to these devices to protect the privacy of information. When both organization and personal information coexist in one device, it becomes a challenge to find a balance between security control for organization’s data and privacy of personal data (Madakam & Date, 2016).

Security becomes a harder challenge to the organizations and in this case the universities due to the large variety of smart mobile devices that need to be managed within corporate network. This is in comparison with threats and security concerns associated with laptops introduced by the organizations Miller et al. (2012). According to Madakam and Date (2016), security threats brought about by use of smart mobile devices can be classified as direct threats example device loss or theft and indirect threats example communication interception due to unsecured wireless network, location tracking of malware attack.

According to Cisco (2017) Higher education requires high-speed local area network to achieve leading edge functionality. To accomplish this, a robust end-to-end network that meets the current and future needs of students, staff and other stakeholders is required. This can be realized through use of switches in a wired environment and the enhanced flexibility, mobility, portability, and scalability enabled by a combined wired and wireless infrastructure. Unfortunately all this technology comes with a fair share of security challenges that need to be addressed.

1.2 Statement of the Problem

Smart mobile devices come with convenience and efficiency of work and study, but they pose a security challenge in the corporate network if unchecked. One of the major reasons for increased security threats is the concern of managing heterogeneous disparate smart mobile devices. Additionally, corporate confidential data stored in smart mobile device can easily be exposed in the event that the device is lost or stolen. When personal devices infected with malicious codes are connected to the university's internal infrastructures, for example through intranet, it may lead to a threat to university's IT assets. There is also a risk for hackers to abnormally access internal corporate infrastructures using normally registered personal devices through spoofing. This can easily be done if there is a threat assessment tool that can inform the level of exposure to attack and hence provide some policy review advisory notes or guideline and is the purpose of this study. Such a tool could help to provide guidelines on technical security mechanisms or otherwise to aid in enforcing the security policy. The study proposes a Threat matrix serves as threat and risk assessment tool to provide recommendations that maximize the protection of confidentiality, integrity and availability of university data while still providing functionality and usability of smart mobile devices. The matrix computes the likelihood of attack from various threats that affect smart mobile devices.

This is useful in determining whether or not the existing policies, procedures and protection items in place are adequate.

1.3 Purpose of the Study

This study aimed at developing a threat matrix to compute likelihood of threat attack on the university network for a secure LAN ecosystem.

1.3.1 Objectives of the Study

(i) To assess the threats introduced through the use of smart mobile devices in the university network

(ii) To develop a threat matrix to compute likelihood of threat attack on a university network

(iii)To determine security requirements for a secure university LAN ecosystem based on the computed likelihood of attack

(iv) To test and validate the matrix

1.4 Research Questions

The researcher aimed to find answers to the questions listed below;

(i) Are there security threats introduced through use of smart mobile devices in a university network?

(ii) How can a threat matrix that computes likelihood of threat attack be developed?

(iii) What are some of security requirements needed to enhance security of a university LAN ecosystem based on the likelihood of attack?

(iv) Can the developed matrix compute likelihood of attack?

1.5 Significance of the Study

This research study is relevant to all stakeholders as listed below;

(i) The research enlighten the university network administrators and the management at large of the various types of security threats that are likely to attack the network and hence enable them adopt and implement the most appropriate security solutions as countermeasures.

(ii) The findings of this research offer an insight guide to network users on how to securely connect their devices to the corporate network without compromising the security of data in the institution. This does not only raise level of awareness to the users on the importance of security but also help to minimize the levels of exposure of corporate information and information systems.

(iii) A successful threat matrix is a significant addition to reducing insecurity in corporate networks knowledge area that is relevant to academicians for future research.

1.6 Expected Outcomes of the Research Study

The aim of this research study was to come up with the following deliverables;

(i) A matrix that serves as a risk assessment tool to determine likelihood of threat attack introduced as a result of connecting smart mobile devices to university network.

(ii) Downloadable list of recommendations resourceful to both university management and users of smart mobile devices on how to securely use their devices.

(iii)A list of security requirements for a secure university LAN ecosystem will guide the management in implementing most suitable security solutions.

1.7 Justification of the Study

With proliferation of smart mobile devices in cooperate networks as a result of adoption of BYOD, security concern increases. Hence there is need for a secure ecosystem to guard the institution information and other personal data against malicious attack. The Verizon (2015) Data Breach Investigations Report states that currently there are tens of millions of devices in use. Personal devices infected with malware can be used to gain access to university data. Data breaches can be caused by hackers infiltrating university network or gaining access through stolen or lost devices. Cybercriminals can gain unauthorized access to information systems in the university database and alter the data thereby affecting the integrity of the data.

Smart mobile devices normally contain a large amount of sensitive data which can be both personal and corporate data. These devices are also often used to perform other sensitive transactions such as online payments. According to Zhao and Ge (2013), Open-source platforms for smart mobile devices such as Android and other third-party applications have also become very popular. This provides more opportunities and attracts malware creators. In their research they recognize the inability for most of the manufacturers to put more effort on device security. In the event that the device is compromised it can lead to compromise of both personal and corporate information stored on the smart mobile device. The attacker can also change the settings of the device leading to more harmful consequences.

Currently organizations face the risk of cyber threat from every corner. As the university continues to expand, more students are admitted and more staff is employed, the number of different smart mobile devices used by these students and staff and other stakeholders is also likely to increase. These endpoints raise the opportunity for attack and as such there is need to raise awareness among users as most of these risk factors are aimed at people who operate or use the organization network. According to ISACA Journal Volume 4 users need to be aware that they are responsible for protecting the device, preventing physical tampering, setting security-specific features, and avoiding supply chains that provide compromised or unsecure devices. Users can easily and unknowingly download malware to their smart mobile devices or fall victim to man-in-the-middle attacks where cyber criminals pose as legitimate body to intercept and gather sensitive information for their own malicious use. Smart mobile devices proliferation with ever advancing technological features brings into focus device security. According to Delac, Silic and Krolo (2011) devices is rapidly becoming attractive target for malicious attacks. Malicious content installed in these smart mobile devices can easily be spread due to advances in network technologies which provide smart-phones with capabilities of connecting to the internet over 3G, 4G or Wi-Fi networks.

1.8 Scope of the Study

This research aimed at developing a threat matrix for university LAN ecosystem after a careful exploration of security threats affecting smart mobile devices and environment. The study aimed at developing a risk assessment tool that would guide the university management in selecting and implementing the most suitable security solution. This thesis targeted to develop a comprehensive and informative threat matrix that acts as a guide in evaluating security measures that have already been put in place and determine what more needed to be done to secure the university network. Egerton University was used as a case study being the largest public university within Nakuru County with campuses distributed within Nakuru and Nairobi counties. This would appropriately represent other universities within Kenya and beyond.

1.9 Limitations of the Study

Information concerning security in an institute is treated as sensitive information and therefore many respondents were not willing to respond to research enquiries for fear of this information being used against them. The researcher however assured the respondents that the information obtained from them was to be treated as highly confidential and would only be used for the purpose of this academic research. The questionnaire was structured in a manner that was easy to understand for easier response. Time and the availability of resources allocated for this research might also be regarded as limiting factors for this research.

1.10 Assumptions of the Study

After assurance of confidentiality of the information provided by the respondents, the researcher assumed that the respondents would respond on time and to the best of their knowledge. It also assumed that independent variables which included information security policy, asset management, access control, operations security and communications security would be sufficient domains from ISO 27001 to explore security threats introduced to university network through connected smart mobile devices. Moderating variables consisting of government regulations would be sufficient variables to develop a threat matrix.

CHAPTER TWO

LITERATURE REVIEW

2.0 Introduction

This chapter is a review of literature on similar research that has been done before to improve the security of university LAN ecosystem. It particularly evaluated security threats brought about by connected smart mobile devices to university network. Security requirements that are necessary to secure corporate networks were then reviewed. Later a review of the already existing security solutions for smart mobile devices was done. This helped in identifying the gap that this study seeks to fill. A conceptual framework that guided the development of a threat matrix to compute likelihood of attack was presented as the chapter concluded.

2.1 Smart Mobile Devices Security Threats

Threat is the likelihood of a particular threat-source to exercise vulnerability or a weakness that can be accidentally triggered or intentionally exploited (Goguen & Fringa, 2002). The rise of mobile technology has enhanced access to information. Students especially in universities are increasingly moving away from paper books towards tablets and laptops. Learning has been made easier with students learning at their own pace and access educational materials anywhere anytime. Majority of the students want to use their smart mobile devices more frequently and especially in research.

According to Bernabe et al. (2014), mobile computing also known as nomadic computing is the use of portable computing devices such as laptops, smartphones, tablets, music players, handheld video games etc. in conjunction with communications technologies to allow users to access the internet and data regardless of their location (Bernabe *et al.,* 2014). Computing devices connect to the Internet in a variety of ways such as wirelessly using a Wi-Fi card and a wireless internet connection or hotspot, through a broadband connection such as third generation (3G) or fourth generation (4G) wireless connections provided by a cellular network, or by tethering using a cellphone as a modem (Pinola, 2012).

The benefits of using smart mobile devices also come with various cyber security threats and vulnerabilities. These vulnerabilities can be related to the hardware of the device, the internet connections (Bluetooth or wireless), installed applications, stored data and information transfer. Threats can be rated as low, medium or high depending on the likelihood to occur and the impact to the user (Bosworth, Kabay & Whyne, 2009).

Portability of these smart mobile devices makes them easy to lose or be stolen. Malicious buyers would be more attracted to the information contained in the smart mobile device and would be willing to pay more than the device cash value (Barcelo, 2011). This threat brings about the vulnerability of losing personal data. A study done by the Ponemon Institute found that 55 percent of consumers were aware that they could be putting their employers' confidential business information at risk when using their smartphone for both business and personal use. The survey also found that 52 percent of those who are aware of the risk said that it had happened (NZ Business, 2011). Malware threats include viruses, Trojans, worms, spyware and other malicious software which severely degrades and destroy computer's operating system. Most malware target laptops but threats against mobile phones have also increased recently. Infected smart mobile devices pose a danger of infecting other computers when connected to a corporate network. The "blind spot" is a large threat for businesses that allow their employees to use corporate devices and travel for weeks exposed to malware without updating anti-virus software and then returning and connecting to the business' network (Friedman & Hoffman, 2008).

Phishing is another type of attack that tricks users into giving out personal information or downloading a file that could be a virus. This is done through sending of e-mails or displaying web-sites that appears legitimate but it is from cybercriminals looking for easy target. These attacks continue to become sophisticated by day and become hard to recognize even for an experienced computer user. In May 2011, Trend Micro discovered vulnerability in Hotmail that could compromise a user's account just by previewing an e-mail. The malicious messages, specially crafted for individual targets, triggered a script that could steal e-mail messages and contact information and forward new messages to another account (Newman, 2011).

Bluetooth is a technology that allows computing devices to transfer data between devices wirelessly. Smart mobile devices with activated Bluetooth and set to discoverable mode are vulnerable to bluesnarfing attacks. This is an attack that uses Bluetooth connection to steal data such as text messages often without the knowledge of the user. It requires software such as “spy Buddy” which is easy to install and can monitor the device content without being detected (Lee & Kim, 2015).

Although applications submitted to Apple and Android markets are evaluated prior to being added to the marketplace, recent events leave reason to believe the security of applications is not the number one priority (Westervelt, 2011). In June of 2010, Apple banned a Vietnamese developer from the iTunes store after his electronic books application reportedly charged 400 users for books they did not purchase. Experts believe the developer launched the attack to boost his ratings in the iTunes store; as he was able to move from position 50 to 21 in a matter of weeks. In response, Apple implemented a new policy that requires users to enter credit card data more often (Computer Weekly, 2010). One month later a reported 4.6 million Android users downloaded a wallpaper application that was collecting data such as the users’ phone number and transmitting information to China (Warwick, 2010). Security firm Lookout studied the application and reported that although the application was suspicious there was no proof that the activity and data transmission was malicious. It was reported that applications that seemed good could be stealing personal information which posed a big risk especially at a time when apps were exploding on smartphones (Warwick, 2010).

A study by Veracode Inc. found a hard-coded cryptographic key in 40 percent of Android applications. Veracode discovered these keys assign the same password to multiple users allowing for anyone, namely an attacker, to easily discover and publish keys in public forums (Westervelt, 2011). This implied that if someone lost their phone and an attacker got access to that application, the attacker could basically get access to all the data that everyone in the organization can access (Westervelt, 2011). According to Abomhara and Køien (2014) smart mobile devices security threats such as intruder model with an example of Dolev-Yao (DY) intercepts messages in transit from smart mobile devices to the hubs. Denial-of-service attack makes the machines or the network unavailable to intended users. Physical attacks occur due to mobility of smart mobile devices, user privacy attacks are as a result of availability of information generated by these smart mobile devices and can be accessed remotely with anonymity.

According to Sopori et al. (2017) the increase of security risks with the growth of smart mobile device market as hackers are presented with greater surface area of attack from the huge amounts of data generated by these smart mobile devices. According to this research, security problems are as a result of simple processors and operating systems which do not support sophisticated security mechanism hence making smart mobile devices vulnerable to attacks. The paper identifies applications attacks under four distinct classes which include physical attacks, network attacks, software attacks and encryption attacks. According to Babar et al. (2011) security attacks on embedded devices continue to increase day by day and summarizes these attacks with a figure as shown below;

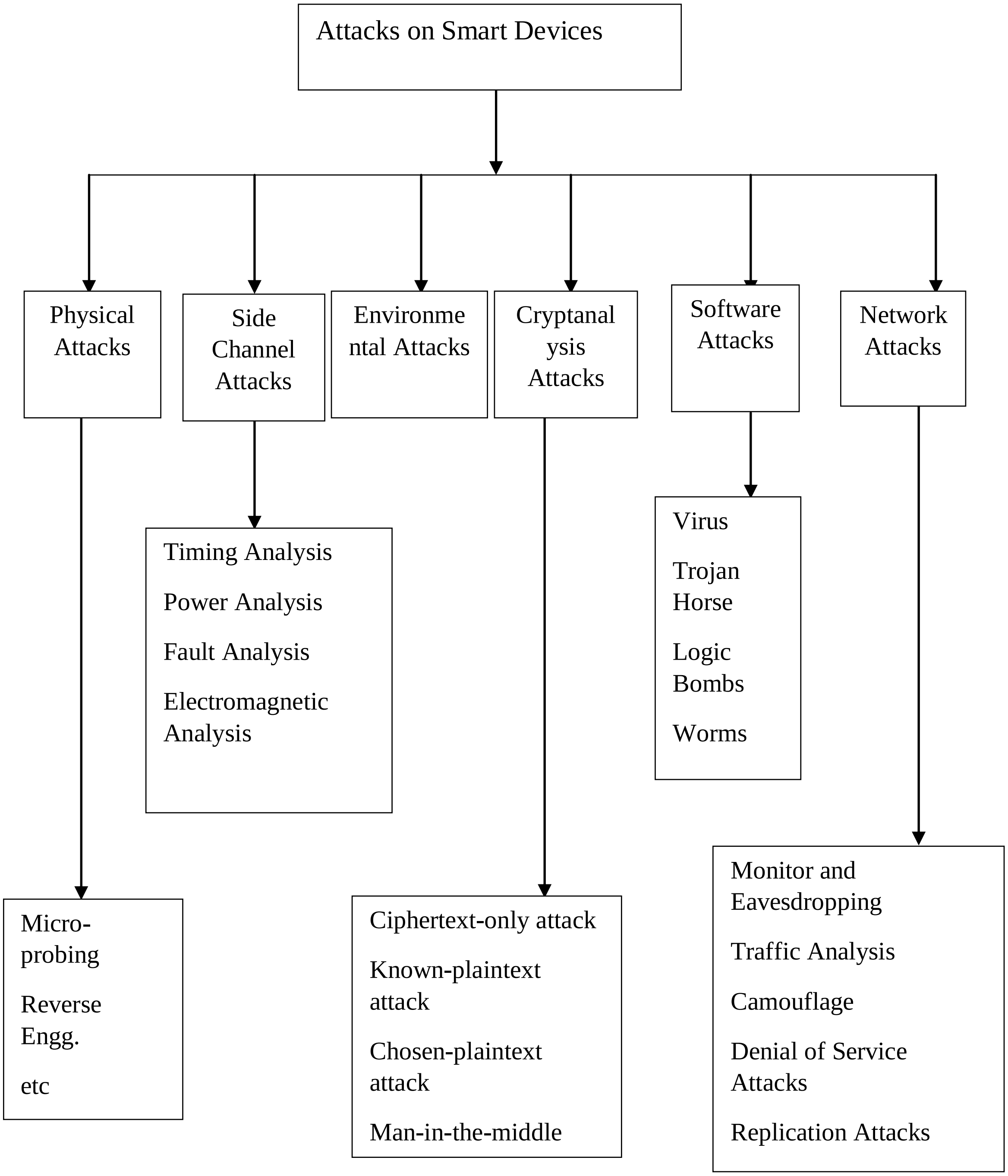


Figure 1: Attacks on Smart mobile Devices

Source; Adopted from Babar et al. (2011)

According to Deloitte (2016), everything from short messaging service (SMS) to the Internet itself is used in ways that go beyond its original intent, often with negative implications for security. Similarly, identity management—the authentication and authorization of devices for machine-to-machine communication—is often accomplished by relying on user names, passwords, and basic machine certificates. These continue to be points of compromise, and it is possible that new solutions for machine-level authentication need to be created to more effectively secure the vast array of smart mobile devices that are being predicted.

According to a report published by Ernst and Young Global Limited (2015), Internet of things has become the medium of interconnection for people and because human communication is mediated by machines and is more and more indirect, there is a deeply rooted security problem with the possibility of impersonation, identity theft, hacking and, in general, cyber threats. The report indicates that Internet of things will increasingly rely on cloud computing, and smart mobile devices with sensors built in, along with thousands of applications to support them. The problem is that the truly integrated environments needed to support this connected technology do not exist, and cloud computing is in need of serious improvement, especially in terms of security. One vulnerable device can lead to other vulnerable devices, and it is almost impossible to patch all the vulnerabilities for all the devices. The market of vulnerability will be vast and so would be the number of victims. It is easier for an attacker to plant a “Trojan” in a phone, if the phone is connected to the computer which has already been compromised. With even more devices connected, it will be even easier for a cyber-criminal to get into your attack vector.

According to a report published by US Department of Homeland Security (2016) smart mobile devices had brought undeniable benefits; however, security was not keeping up with the pace of innovation. Increase in network connections integration into nation’s critical infrastructure increased vulnerability to cyber threats. National dependence on network-connected technologies had grown faster than the means to secure it. The report further said that the same technology had introduced risks that include malicious actors manipulating the flow of information to and from network-connected devices or tampering with devices themselves, which lead to the theft of sensitive data and loss of consumer privacy, interruption of business operations, slowdown of internet functionality through large-scale distributed denial-of-service attacks, and potential disruptions to critical infrastructure.

2.2 Security Requirement for Smart Mobile Devices

Employers need to consider this risk when drafting security policies to ensure the rules on the use or prohibition of personal devices for company purposes are spelled out. Hardware and software of the device should be known to the employer and employees they are also required to follow minimal secure practices on their devices before accessing company websites or e-mail (NZ Business, 2011). The Information Systems Control Journal notes “The biggest decision a corporation needs to make with respect to smart mobile device deployment is the cost of support based on graduated levels of security. If the total cost of the device and the risk it generates does not surpass the business benefit, corporate management should just say no (Milligan & Hutcheson, 2008).

It is hard to prevent theft or loss of devices, but the loss of data can be minimized by encrypting the information on the device, requiring a password, biometrics, or an access key to use and configuring the device to erase data after a number of failed logon attempts. The cost of these mitigations is minimal since most operating systems offer password protection and biometric systems are also relatively inexpensive (Milligan & Hutcheson, 2008). Another option is to install software that allows remote wipe of the data such as Lojack for laptops and Sophos for smartphones (Barcelo, 2011). Users may not want to take the extra steps in logging on to their devices but the pay-off is rewarding if the device is lost or stolen. Although some phishing attacks may be hard to recognize, the best prevention strategies are to read e-mail carefully to ensure it is from a reputable source, look for grammatical errors and avoid opening attachments unless their receipt is expected (Newman, 2011).

Wireless hotspots which smart mobile device users connect to; may have little or no security. This leaves the device vulnerable to interception or spoofing (Friedman & Hoffman, 2008) which can lead to loss or manipulation of personal or corporate data stored on that smart mobile device. Unsecured Wi-Fi connections such as those at the local coffee shop are an open invitation for snoopers and can even allow an attacker to take over a users' browsing session. A hotspot attack called sidejacking uses automated tools to take over unsecured websites. One such tool developed by Mozilla as a Firefox browser plug-in is called "Firesheep." which automates session hijacking attacks over unsecured Wi-Fi networks. This is done by analyzing traffic between a Wi-Fi router and a person's laptop or smartphone using a packet sniffer. This is according to Westervelt (2011) Top 5 phone security threats in 2012.

Users can reduce risks of hotspots and wireless networks by deactivating the automated search on their device and connecting to secure wireless connections whenever possible. Developers such as Google offer encryption support for browsers using open connections. According to this research, IBM has also created a Secure Open Wireless Standard that uses a digital certificate to secure the hotspot and ensure the Service Set Identifier (SSID) is legitimate (Westervelt, 2011). With the amount of uses for Bluetooth technology today, it is important for users realize the security threats to Bluetooth, to pair with known devices only, and turn Bluetooth off when not in use.

Mitigation of application vulnerabilities is easier said than done as the resources and infrastructures for creating applications are still very immature. Some suggestions for improvement in software are code signing which allows users to verify the applications' source; sandboxing, which separates an application from other processes; and permission notifications to warn users of an application attempting to access their data (Westervelt, 2011). It will be up to the application police such as Google for Android and Apple for iTunes to raise the standard for security requirements in applications and to users to review the application before downloading.

According to O'Dell (2010), defense-in-depth strategy which helps in building security from the initial stage up to monitoring and management of smart mobile devices which allow the organization to buy more time to plan defense of their resources, by keeping the potential attacker engaged layer after layer. Security layers according to this white paper include; device or equipment, gateway and networks, facilitation and *consumerization* or application.

2.2.1 Role of ICT Security Policy

According to Shafagh and Hithnawi (2014), a security policy is a document that explains the physical and logical plan with an aim of protecting the information system core values which include confidentiality, integrity, availability and authenticity while providing operational mechanism for secure cryptographic key distribution and non-repudiation. Security on the other hand refers to provision of core values of information security assurance which include confidentiality, availability, integrity, authentication, authorisation and non-repudiation Aware et al. (2005). These security services can be provided by cryptographic mechanisms such as hash functions, block cipher and signature algorithms. Souppaya and Scarfone, (2013), term security as organized framework that consists of concepts, techniques or procedures required to protect systems or assets against unintentional threats. In their research it is noted that threats can be classified as either internal which originate from within the network or external that originate from outside the network.

To develop and implement a comprehensive security policy it is important to first understand the risks, threats and vulnerabilities currently existing in the environment. TechTarget.com (2012), emphasize on the importance of learning about the problem as much as possible in order to develop a solid response plan. According to this research, a policy should provide guidelines on how to respond to an attack in the fastest and most efficient manner. As a result selected countermeasures and safeguards should be deployed intelligently to create protection to the mission-critical assets.

Bring Your Own Device (BYOD) is a technology, concept and policy that allows employees to perform their duties by accessing corporate IT resources using their personal devices Koh et al. (2014). While this improves personal operational convenience, the level of security threats is equally increased. This research recommends device-centered security policies such as device authentication in a corporate infrastructure. According to Computer Security Institute approximately 60% to 80% of network misuse originates from inside the network hence internal threats are worse than external threats. It is therefore important to analyze how university students and staff use their smart mobile devices to connect to the internet through company network and the security threats involved in these connections.

While consumers continue to enjoy the benefits that come with the smart mobile devices technology, the repercussions caused by security breach can be devastating. According to Arabo and Pranggono (2013), security policy faces a lot of challenges which may be due to different entities that are involved and different protection requirements that are needed. Smart mobile devices come with variety of models which use different technologies with various protocol types to operate; this poses a challenge of designing a comprehensive security policy that will cater for all these operational mechanisms.

ISO 27000 series is one of the most referenced security models which was originally published as British Standard 7799. This code of practice was later in 2000 adopted as information security framework. It provides a very broad information security framework that can be applied to all types and sizes of organizations. The latest revision of this standard was published in 2013, and its full title is now ISO/IEC 27001:2013. It can be thought of as the information security equivalent of ISO 9000 quality standards for manufacturing, and even includes a similar certification process. ISO/IEC 27001 International Standard was prepared to provide a model for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an Information Security Management System (ISMS). An ISMS is a systematic approach developed to manage sensitive company information to ensure that security is maintained.

An ISMS is a system of processes, documents, technology and people that help to manage, monitor, audit and improve your organization's information security. It helps you manage all your security practices in one place, consistently and cost-effectively. This International Standard adopts the "Plan-Do-Check-Act" (PDCA) model, which is applied to structure all ISMS processes (Calder &Watkins, 2008). Plan establishes ISMS policy, objectives, processes and procedures relevant to managing risk and improving information security to deliver results in accordance with an organization's overall policies and objectives. Do implements and operates the ISMS policy, controls, processes and procedures. Check assesses and, where applicable, measures process performance against ISMS policy, objectives and practical experience and report the results to management for review. Act takes corrective and preventive actions, based on the results of the internal ISMS audit and management review or other relevant information, to achieve continual improvement of the ISMS.

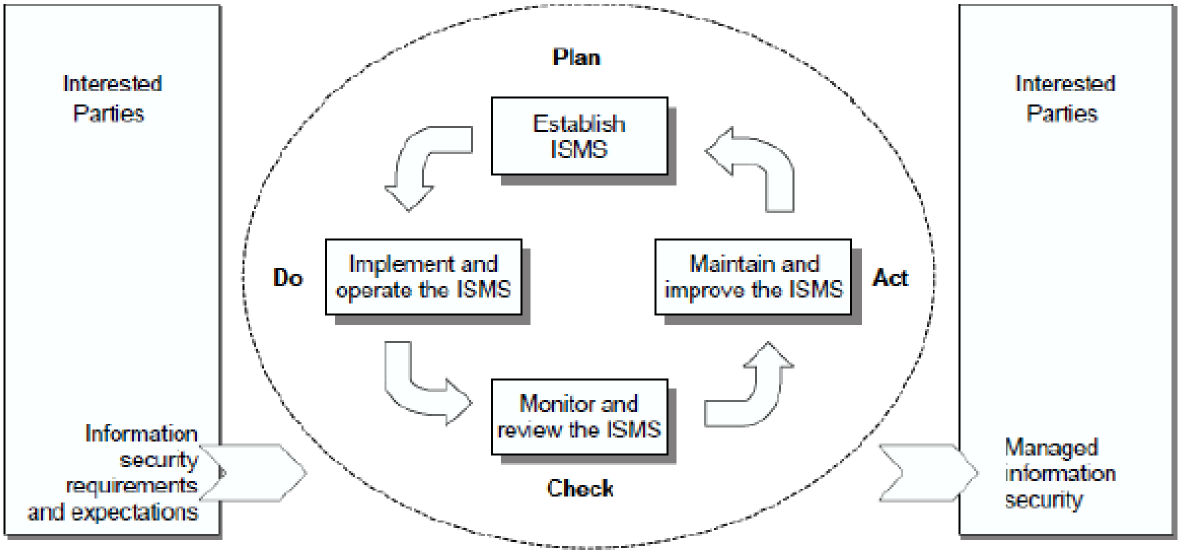

Interested Parties
Information security requirements and expectations
Plan
Establish ISMS
Do
Implement and operate the ISMS
Maintain and improve the ISMS
Act
Monitor and review the ISMS
Check
Interested Parties
Managed information security

Figure 2: PDCA Model

Source; (ISO/IEC 27001, 2005)

ISO 27002 on the other hand is a commonly used international standard for information security throughout the world and provides insight to security controls to protect information and information technology. It is a standard that contains guidelines and best practices recommendations for 10 security domains. The U.S. National Institute of Standards and Technology (NIST) has been building a broad gathering of data security benchmarks and best practices documentation. The NIST Special Publication 800 arrangement was first distributed in 1990 and has developed to give exhortation on pretty much every part of data security. In spite of the fact that not particularly a data security system, NIST SP 800-53 is a model that different structures have developed from. U.S. government organizations use NIST SP 800-53 to conform to the Federal Information Processing Standard's (FIPS) 200 necessities. Despite the fact that it is particular to government organizations, the NIST structure could be connected in some other industry and ought not to be neglected by organizations hoping to fabricate a data security program.

Control Objectives for Information and Related Technology (COBIT) is a structure created in the mid-90s by ISACA, an independent organization of IT administration experts. This system began principally centered around lessening technical risks in organizations, however has advanced as of late with COBIT 5 to likewise incorporate alignment of IT with business-vital objectives. It is the most usually utilized system to accomplish consistence with Sarbanes-Oxley rules. COBIT 5 for Information Security provides guidance to help IT and security professionals understand, utilize, implement and direct important information security-related activities, and make more informed decisions while maintaining awareness about emerging technologies and the accompanying threats. COBIT 5 enables information and related technology to be governed and managed in a holistic manner for the whole enterprise, taking in the full end to end business and functional areas of responsibility, considering the IT-related interest of internal and external stakeholder.

2.3 Security Solutions for Smart Mobile Devices

According to Vermesan and Friess (2013), there exists two main ways of addressing security concerns in a BYOD environment, this include access control where people are at the center and device control where devices are at the center. The research identifies three different security approaches that can be used to control smart mobile devices.

Mobile Device Management (MDM) provides support to full device control through software solutions that companies can use to control, lock down, enforce policies and encrypt mobile devices. Mobile Application Management (MAM) according to this research acts like MDM but it is only applied to specific applications on a device. MAM can enable IT security personnel to control and secure specific corporate applications and leave the rest of the things contained on a smart mobile device to the user. Mobile Information Management (MIM) on the other hand allow files and documents synchronization across different devices to manage security.

Mobile Device Management systems consists of two main components; MDM agent which is an application installed on mobile devices and sends its status as well as data to MDM server which manages received data and triggers commands on the registered mobile device to either control, lock down, encrypt or enforce policies accordingly (Riahi *et al.,* 2013). According to this research, Mobile Application Management (MAM) system is another security model used to remotely install, update, remove, audit and monitor enterprise related applications contained on mobile devices. Mobile Information Management (MIM) preserves enterprise information in a central location and securely it between different endpoints and platforms. This only allows limited number of trusted applications to manage and control the encrypted corporate data Huang et al. (2015).

Network Access Control (NAC) is a security framework which limits the number of connected devices while determining permissions and denying unrecognized devices access to a company’s internal network (Youker, 2014). According to this research, NAC is useful in ensuring that likelihood of data leakage, infection of malware and other related attacks are avoided or minimized. Desktop virtualization is a type of security framework which enables desktop computers, virtual machines of servers to host sessions for remotely located smart mobile devices (Youker, 2014). These models centralize resources, data as well as security management. This reduces or eliminates the need to transmit data onto smart mobile devices and hence reduces the likelihood of data leakage.

Containerization is used as a security framework to partition smart mobile device storage into different independent sections which separates personal data from work data (Rhodes, 2013). Each section has its own security policies and allows remote access for company control without affecting personal data. Remote wiping is a reactive solution which is triggered when a device is lost or stolen or when the owner leaves the company (Youker, 2014). This is done by removing all company applications and data contained in the smart mobile device. Some MDM and MAM solutions already contain remote wiping procedures.

Other security applications include anti-virus, anti-malware and spyware applications which are important in strengthening BYOD security frameworks. Companies should enforce use of these measures and owners of smart mobile devices should have this software installed and actively scanning. This reduces the probability of infections to other resources and other devices connected to the company network (Romer, 2014). Frameworks are often customized to solve specific information security problems, just like building blueprints are customized to meet their required specifications and use. Developing a threat matrix for smart mobile devices will ensure that the core values of information security which includes confidentiality, integrity and availability of university information systems is maintained. It will also serve as an audit tool indicating whether the implemented countermeasures are able to protect the university against security attacks.

According to Abdelrahman et al. (2013) in their research on security for smart networks developed an architecture called NEMESYS which is a data collection, visualization and analysis infrastructure in-order to gather data concerning smart mobile devices attack. The collected data is made available to anomaly detection mechanism for it to detect any deviations from normal user behavior and the core network in real time.

Rapid increase in technology and increased usage of smart phones makes them vulnerable to malware and other security breaches (Zaidi *et al.*, 2016) in their survey on security for smart phones devices categorize threats as new attacks and old attacks. Each type of attack is then displayed in a form of a table showing its cause and suggested solution for the attack. Jha and Sunil (2014), in their research on trends, challenges and solutions of smart mobile devices recognize the development and demand to seamless connectivity of smart mobile devices to provide functionality to users. New risks and threats are introduced as these devices provide more features and functionality. A detailed discussion of malware is presented and an integrated security solution for smart mobile devices is the proposed. According to this research, security solution can be achieved by first investigating secure system architecture of the smart mobile device then re-evaluate and enhance security system architecture of that smart mobile device. They proposed multi-layers integrated security solutions for smart mobile devices.

According to Beach et al. (2009) in a research on managing online risk identifies matrixes as a common tool in both qualitative and quantitative risk analysis. The column structure in a matrix identifies the kind of information to be collected and analyzed. An example of a social media risk assessment matrix is then given as shown in the table below;

Table 2.1: Facebook Risk Assessment Table

Risk/ Threat	Control	Mitigation	Likelihood	Impact	Risk Rating
Technical					
Virus: Social media sites tend to be the target for virus attacks	Facebook is blocked on the bank's network prohibiting its access within the bank	Facebook is blocked on the bank's network prohibiting its access within the bank	Medium	Medium	Medium
Cross-site Scripting: Cross-site scripting (XSS) is a type of computer security vulnerability typically found in web applications that enable malicious attackers to inject client side script into web pages viewed by other users	Facebook is blocked on the bank's network prohibiting its access within the bank	Facebook is blocked on the bank's network prohibiting its access within the bank	High	Medium	Medium
Employee productivity: The use of Facebook on user's computers tends to distract employees from business priorities. If the bank's employees spend too much time on Facebook, it might affect his/her performance at work	Facebook is blocked on the bank's network prohibiting its access within the bank	Facebook is blocked on the bank's network prohibiting its access within the bank	Low	Medium	Medium

Cisco Secure Data Center for the Enterprise Solution Portfolio designed a threat management systems capabilities matrix which gave the IT Security teams a way to map threat management capabilities to Cisco's Before, During, and After Security Model, which can be applied across the entire organization. This matrix was used by IT security team to build a solid foundation for the NIST Cyber security Framework. It ensured that the effectiveness of the entire threat management program was enhanced.

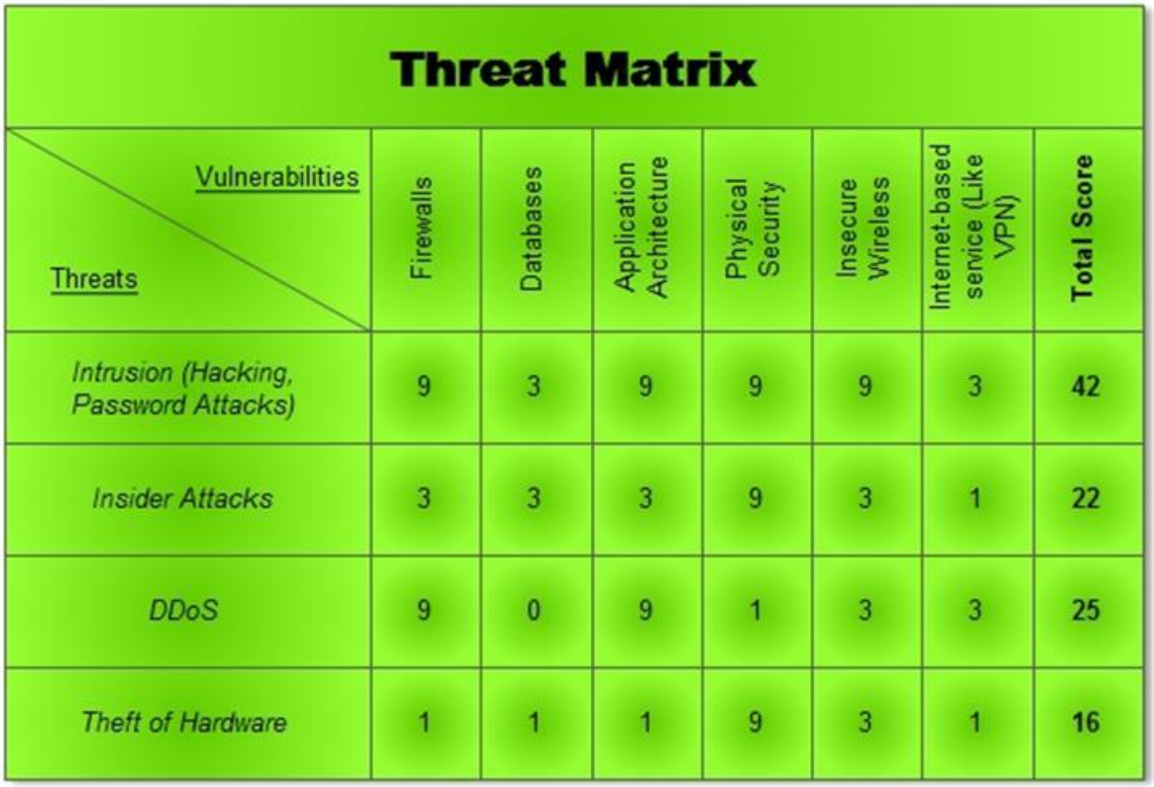
Table 2.2: Threat Management System Capabilities Matrix

<table>
<tr><th colspan="5">Threat Management System Capabilities Matrix</th></tr>
<tr><th colspan="5">Mapping Capabilities to the Attack Continuum</th></tr>
<tr><th></th><th>Description</th><th>Before</th><th>During</th><th>After</th></tr>
<tr><td>Threat Containment and Remediation</td><td>File, packet and flow based inspection and analysis for threats</td><td>End point protection agents, network based flow protection</td><td>Cloud based end point file analysis, network based file analysis, network based flow analysis, signature based analysis, dynamic analysis</td><td>Connections and flows analysis and remediation</td></tr>
<tr><td>Access Control and Segmentation</td><td>Access control policies, segmentation, secure separation</td><td>End point group assignments, security zones, user to asset access policies</td><td>Fabric enforcement, firewall policy enforcement, connection validation and protocol compliance</td><td>Policy enforcement and logging</td></tr>
<tr><td>Identity management</td><td>User identity and access posturing, network based</td><td>User mapping to groups, resources and acceptable</td><td>User context analysis and policy enforcement</td><td>User access and threat origination analysis and</td></tr>
</table>

	user context	access locations		remediation
Application viability and control	File control and trajectory, application quarantine	Policies to limit and control internal & external client & web applications including apps version	Enforcement of application control policies	Visibility into all applications being accessed and running on network
Logging and traceability management	Threat forensics and compliance	Proper configuration of threat management system reporting	Active out of band logging	Immediate access by proper threat management platform. Consolidation of logs into central repository for further forensics and compliance

A research by InfoSec-institute (2014) defines threat matrix as one that uses threat attributes to help the analyst to characterize the type of threat based on its overall nature. This allows analyst to describe the full spectrum of the threat. According to this research, a matrix is a framework or model for organizing a set of related metrics. Threat attributes can be grouped into two majors groups; commitment attribute and resource attribute. The threat matrix is graduated into levels of magnitude, with each level corresponding to a different kind of threat. The higher the value the more sophisticated a threat is and it may attain the goal easier.

Table 2.3: Threat Matrix Sample



Threat Matrix

Vulnerabilities Threats	Firewalls	Databases	Application Architecture	Physical Security	Insecure Wireless	Internet-based service (Like VPN)	**Total Score**
Intrusion (Hacking, Password Attacks)	9	3	9	9	9	3	**42**
Insider Attacks	3	3	3	9	3	1	**22**
DDoS	9	0	9	1	3	3	**25**
Theft of Hardware	1	1	1	9	3	1	**16**

2.4 Research Gap

From the security solution for smart mobile devices presented in section 2.3 above and summarized in Table 2.4 below, none of them integrates a threat assessment as part of their proposed solution. Before designing and deploying smart mobile device security solutions, it would be prudent to assess the security status in order to implement the most suitable solution. However there seems to be no tool designed to assess risks and threats brought about by use of smart mobile devices before proposing a solution.

Table 2.4: Summary of Smart Mobile Devices Security Solutions

Tool	**Solution provided**
Mobile Device Management (MDM)	Provides support to full device control through software solutions that companies can use to control, lock down, enforce policies and encrypt mobile devices.
Mobile Application Management (MAM)	Acts like MDM but it is only applied to specific applications on a device
Mobile Information Management (MIM)	Allow files and documents synchronization across different devices to manage security.
Network Access Control (NAC)	Limits the number of connected devices while determining permissions and denying unrecognized devices access to a company's internal network
Desktop virtualization	Enables desktop computers, virtual machines of servers to host sessions for remotely located smart mobile devices
Containerization	Used as a security framework to partition smart mobile device storage into different independent sections which separates personal data from work data
Remote wiping	A reactive solution which is triggered when a device is lost or stolen or when the owner leaves the company

Using ISO 27001best practices as benchmark framework, the researcher aimed at designing a matrix with a more comprehensive approach that comprised five of the domains of ISO 27001. This includes; information security policy, asset management, access control, operations security and communications security. The developed security matrix will act as a risk assessment tool to determine likelihood of attack from various threats introduced to university network through use of smart mobile devices. After submitting the assessment questions included in the matrix, feasible threats and vulnerabilities will be identified. The computed likelihood of attack information will help the university determine the security controls that need to be improved or to be added to the network.

2.5 Conceptual Framework

Conceptual model that was used to guide the research is presented in two phases. In the first phase the framework was used to derive the formula for computing likelihood of attack. The five independent variables selected from ISO 27001 domains included; information security policy, asset management, access control, operations security and communications security. These being some of the most common clauses in which smart mobile devices are operated with regard to corporate networks. The moderating variable included government regulations. Threat matrix formed the dependent variable and was used to compute likelihood of threat attack. The figure below shows conceptual framework that was used to derive the formula to determine likelihood of threat attack.

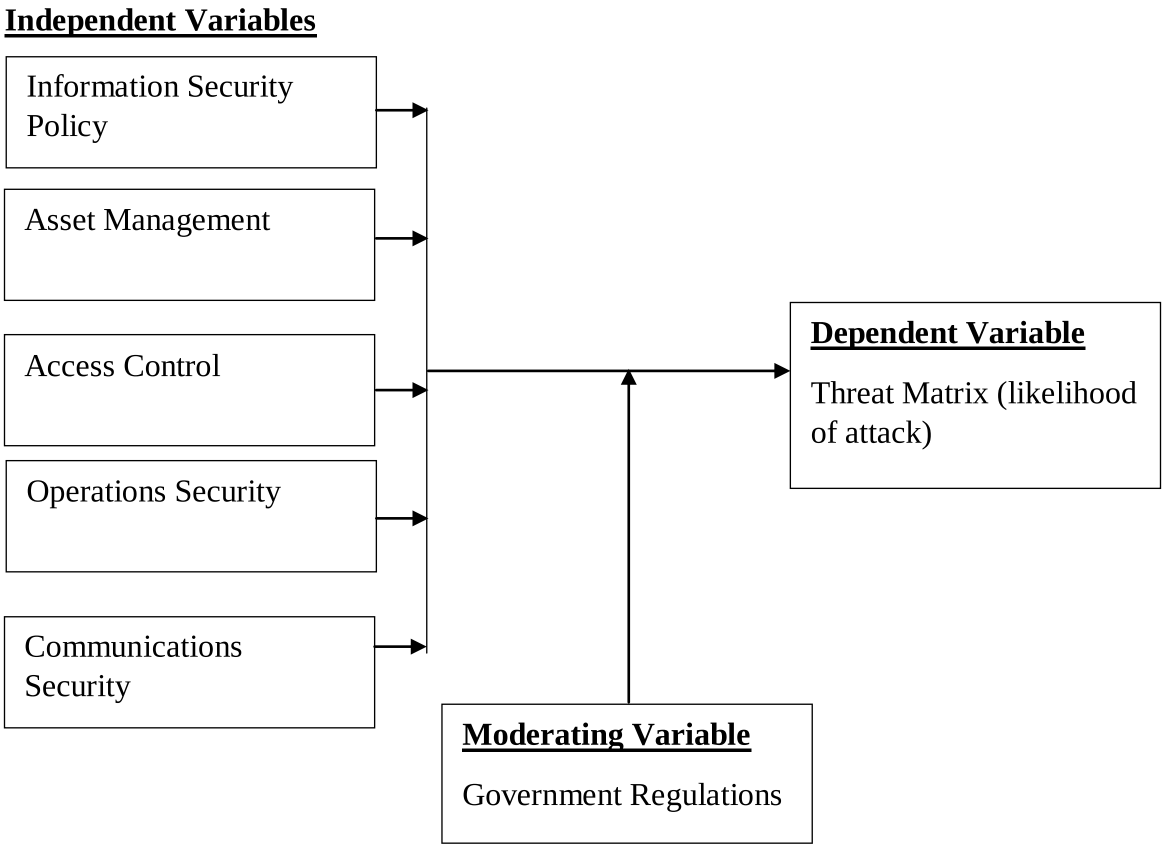


Figure 3: Conceptual framework Phase 1

Source: Author (2018)

Likelihood of attack was computed from functional weights obtained after analyzing data of the independent variables as shown in the formula below;

Likelihood of attack *=f (Information security policy, Asset Management, Access Control, Operations security, communications security)*

Where;

Information security policy: aims at providing directions and support to management of security in university information systems.

Asset management: aims at ensuring information security assets are identified, security designated and people know how to handle the assets. This will also ensure that the information contained in smart mobile devices receive appropriate level of protection. Users should also understand the risk of theft, fraud or misuse of the devices.

Access control: aims at limiting access to university information and information systems while considering business needs by means of formal processes to grant or revoke access rights.

Operations security: controls in this sections aims at ensuring that operations of smart mobile devices including operating systems are secure and protected from malware and other viruses.

Communications security: aims at protecting university network infrastructures and services. This will also include information that is transmitted through the university network to and from smart mobile devices.

The second phase of the framework demonstrates the implemented prototype which had various module including; user registration module that allowed new users to register in order to access other system functionalities. User login module allowed only authorized users to access the system functionalities after submitting the correct credentials. Assessment module allowed users to answer the assessment questions; the results were then submitted to the database and were used to compute the likelihood of attack. Reports module allowed users to view their scores and recommendations of the submitted assessment.

The figure below show how the prototype was implemented.

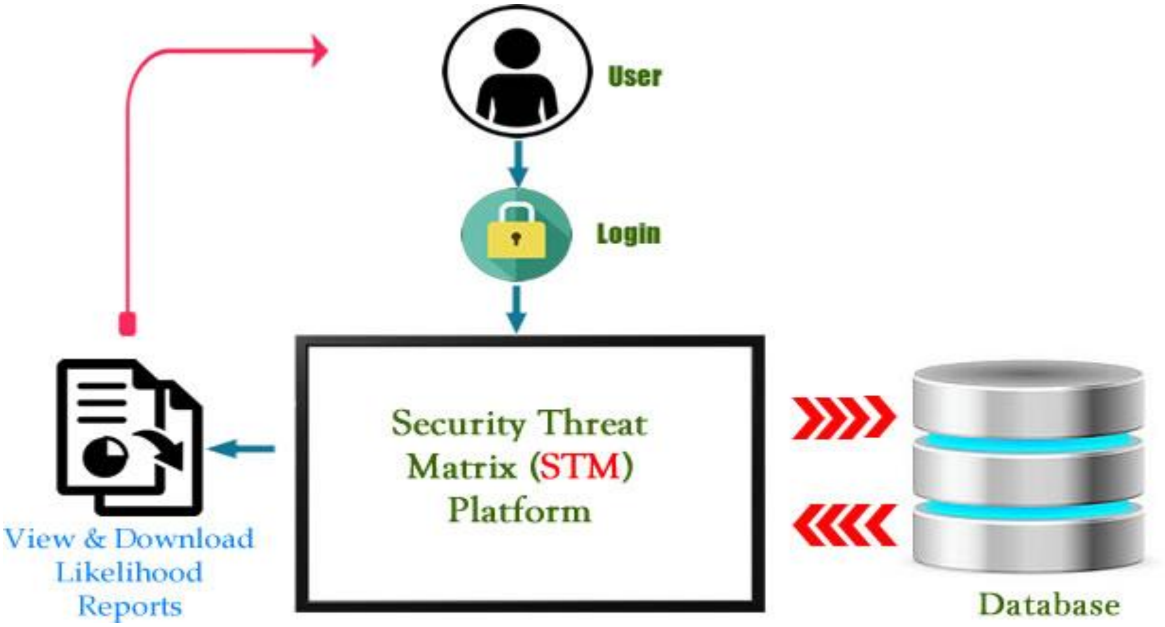

User
Login
Security Threat Matrix (STM) Platform
View & Download Likelihood Reports
Database

Figure 4: Conceptual Framework Phase 2

Source: Author (2018)

CHAPTER THREE
RESEARCH DESIGN AND METHODOLOGY

3.1 Introduction

This chapter provides an insight on how the research was conducted and organized to gather important data and information concerning security of smart mobile devices in a university LAN ecosystem. Relevant and diverse views of many scholars who have conducted intensive studies in security of smart mobile devices were also sought. The chapter was set to analyze the process of data collection, the source of data, the type of data collected and laid the guidelines for interpreting and drawing conclusions from the data.

3.2 Research Design

The main purpose of a research design is to confirm that the evidence obtained enables the researcher to effectively address the research problem clearly (Suo *et al.*, 2012). This research employed a case study design as it sought an in-depth study of security threats affecting university networks through use of smart mobile devices.

3.3 Location of the Study

Egerton University was used as a case study to narrow down the research. This is because it is a public university with high number of students and staff and with campuses spread across Nakuru and Nairobi counties hence a suitable representation of other institutes of higher learning in Kenya and beyond.

3.4 Population of the Study

Population is a group of people, objects or items with similar characteristics from which samples of research are drawn for measurement (Shukla, 2011).The target population for this study was Egerton University being a public university with highest number of students and staff and a well-established IT infrastructure within Nakuru County.

3.5 Sampling Procedure and Sample Size

3.5.1 Sampling Procedure

A sample is a subset of the population (Dematteo *et al.,* 2005). Sample size refers to the number of respondents participating in a research model as defined by KPMG (2015). Selecting sampling methods and determining sample size are important in applied statistics research in order to draw precise conclusions. Therefore, the sample size is an important factor of any scientific research (Kim *et al.,* 2015).Since the population under study was large and the degree of variability or the distribution of the people who owned smart mobile devices was not known, the researcher used Cochran's formula to calculate the sample size. Stratified random sampling technique was then used to determine how the questionnaires were to be distributed since the population was heterogeneous. The population was divided into three strata according to the various campuses within the university. A sample size in each stratum was then determined. Random sampling method was used to select the respondents from each stratum. This ensured that every single individual in the sampling frame had a chance of being selected into the sample.

3.5.2 Sample Size

The researcher used +/- 5% as level of precision or the sampling error which gave the range in which the true value of the population was estimated to be. Confidence level of 95% was picked meaning 95 out of 100 samples would have the true population value within the range of specified precision. Since the population under research was heterogeneous, a larger sample size was required to obtain an appropriate level of precision. A proportion of 50% which indicated a greater level of variability was used.

Using Cochran's formula the sample size was calculated as shown below;

$$n_o = \left(z^2 pq\right) \div e^2$$

Equation 1: Sample Size Formula

Source: Cochran (1977)

Where;

n_o is the sample size

z is the selected critical value of confidence level

p is the estimated proportion of an attribute present in the population

q is 1-p

e is the desired level of precision

Using 95% confidence level, 50% proportion of variability with 5% level of precision the researcher obtained the sample size as calculated below;

z=1.96, p=0.5, q=1-0.5, e=0.05

Hence

$$n = \left((1.96)^2 * 0.5 * 0.5\right) \div (0.05)^2$$

n= 384.16

n= 384

Therefore the number of respondents required for the study was 384.

Using stratified random sampling, the population size was categorized according to the various campuses that Egerton University is comprised of. The table below shows how sample size of each campus was determined.

Table 3.1: Sample Size per Campus

Campus	**Population size**	**Sample size**
Njoro campus	12,348	$(12348 \div 14257) * 384 = 333$
Nakuru campus	1,262	$(1262 \div 14257) * 384 = 34$
Nairobi campus	647	$(647 \div 14257) * 384 = 17$
Total	**14,257**	**384**

To evenly distribute the questionnaires, random sampling was used. This ensured that every single individual in the sampling frame had an equal chance of being selected into the sample. The questionnaires were then distributed using drop and pick method.

3.6 Instrumentation

Relevant literature was reviewed and a tool of data collection particularly the questionnaire was developed. Quantitative research method was used to analyze the collected data according to content validity as per the set objectives of the research.

3.7 Data Collection

The researcher obtained permission to carry out the research from the school of Postgraduate studies. This was later followed by research permit obtained from National Council for Science, Technology and Innovation. Later a consent letter was acquired from Egerton University authorizing the researcher to collect research data from the university. Primary data was obtained through use of structured questionnaires while secondary data was obtained from Egerton University reports and other publications.

3.8 Data Analysis

The collected data was analyzed using quantitative analysis. SPSS was used for data entry and descriptive analysis. The collected data assisted in establishing the relationship between independent variables and dependent variable. The regression analysis of the collected data assisted in obtaining the functional weights of the five independent variables which was then used to compute the likelihood of attack. After developing the matrix, it was deployed online and was accessible through a web link. Respondents were requested to register and run assessment; the matrix then computed likelihood of attack and hence displayed the security status of the university network.

3.9 Matrix Development

Likelihood of attack was expected to take a linear form as a function of weight and security variable scores. The security variable scores were determined by the linear scale attached to each question of the assessment. The weights were obtained from regression analysis of the collected data. The expected linear equation for the implementation of the matrix as a mathematical formula would therefore be in the form demonstrated in equation 2 below;

Likelihood of Attack = $L_1SV_1 + L_2SV_2 + L_3SV_3 + \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots + L_nSV_n$

Equation 2: Threat Matrix Development Equation

Source: Researcher (2018)

Where;

L_1, L_2, L_3 …………………… L_n respectively are different weights that were determined from a cross-section security variables discussed in the study.

While;

SV_1, SV_2, SV_3 ………………………. SV_n respectively are average scores for security variables associated with security threat exposure in this study which included Information Security Policy, Asset Management, Access Control, Operations Security and Communications Security.

After developing the matrix, the collected data was used to run assessment which then was used to compute likelihood of attack. The matrix was also deployed online and was accessible through a web link. Respondents were requested to register and run assessment. The computed likelihood of attack therefore displayed the security status of the university network. From this matrix, downloadable recommendations were obtained. Computed likelihood of attack determined the security requirement needed to be implemented as countermeasure to reduce the risk of attack.

3.10 Matrix Implementation

The matrix was implemented using rapid prototype as a proof of concept. The prototype assisted in testing the effectiveness of the matrix. It provided an insight to the functionality of the matrix and helped to capture any changes needed at an early stage of development. The matrix was in a form of a working web-based application to proof the feasibility of an all-inclusive and final application for managing security threats in corporate networks brought about by use of connected smart mobile devices. The Figure below shows a rapid prototyping model according to Sabale and Dani (2012).

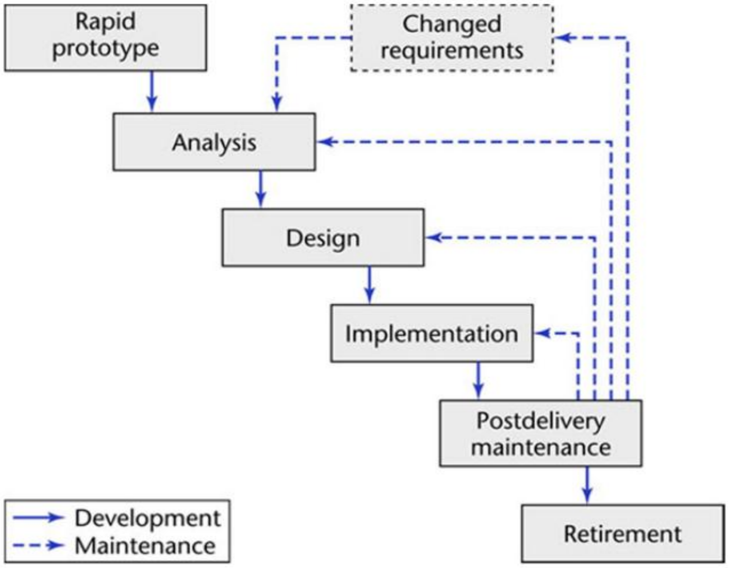


Figure 5: Rapid Prototype Model

Source: (Sabale & Dani, 2012)

3.11 Ethical Considerations

The information obtained from this research was treated with high levels of confidentiality and integrity and as such the researcher sought to assure the respondents that the information they provided would under no circumstance be used against them or for any other purpose other than academic. Respondents were allowed to voluntarily participate in answering the questionnaire and willingly provided the information that the researcher sought to find. To protect the privacy and confidentiality of the respondent’s information, strict ethical standards of anonymity was adhered to.

CHAPTER FOUR
DATA ANALYSIS, PRESENTATION AND DISCUSSION

4.0. Introduction

This chapter presents analyses and interpretation of the collected data. Descriptive and inferential statistics were used in data analysis. Data from both staff and students were duly analyzed and interpreted.

4.1. Response Rate

It was established that 384 sampled respondents were issued with questionnaires and later collected. Out of these, 310 of the questionnaires were returned. This gave a return rate of 80% which was considered to provide satisfactory data for the research.

4.2. General and Demographic Information

4.2.1. Population Category

Table 4.1: Population Category

Statement	Frequency	Percent
Staff	210	68
Student	100	32
Total	310	100.0

The finding in table 4.1 above show that 68% of the study population was students while 32% were staff working in various departments at the university. They were chosen because they had the desired characteristics that would provide sufficient data for the research.

4.2.2. Frequency of Use of Smart Mobile Device in the Internet through Corporate Network

Table 4.2: Frequency of use of smart mobile devices in the Internet through corporate network

Characteristic	Frequency	Percent
Hourly	136	43.9
Daily	122	39.4
Weekly	52	16.8
Total	310	100.0

To validate significance of this research, it was prudent to examine if users of smart mobile devices connect to the internet through university network. It was noted that 43.9% use their smart mobile devices hourly, followed by those that use it on daily basis. Besides, 16.8% reported to weekly use their smart mobile devices while connected to university network. The results therefore show that majority of smart mobile devices users connect to university network and hence exposing corporate network to threats brought about by use of these devices.

4.2.3. Loss of Smart Mobile Device

Table 4.3: Loss of smart mobile device

Characteristic	Frequency	Percent
Never	110	35.5
Once	154	49.7
More than once	46	14.8
Total	310	100.0

One of the major threats to corporate information stored in smart mobile devices is data loss or theft. Response to this question would therefore determine how vulnerable the university data was against this threat. It was established that majority (49.7%) of the respondents had lost their smart mobile devices at least once while 35.5% reported that they had never lost their smart mobile devices as indicated in table 4.3 above.

4.2.4. Smart Mobile Device Security and Privacy Awareness Training

Table 4.4: Smart mobile device security and privacy awareness training

Opinion	Frequency	Percent
Yes	44	14.2
No	266	85.8
Total	310	100.0

Table 4.4 above indicates respondents who had attended smart mobile device security and privacy awareness training were 14.2% of the total sample while 85.8% had not attended. This would determine how attentive users are to security matters with regard to use of their smart mobile devices.

4.3. Threat Evaluation

To evaluate threats introduced through use of smart mobile devices in the university network, Descriptive analysis was conducted to determine respondents view relating to variables under investigation. Furthermore, Chi-square goodness of fit was used to compare the observed sample distribution with the expected probability distribution and to test whether the responses were statistically significant at 5% level of significance. Spearman correlation analysis was done to determine nature of the relationship between the independent and dependent variables.

4.3.1.: Sufficiency of the Information Security Policy to Safeguard Against Threats introduced by Smart Mobile Devices

Table 4.5: Sufficiency of the Policy to Safeguard against Threats introduced by Smart Devices

Statement	SD	D	N	A	SA	χ^2	P
The university security policy requires all smart mobile devices to have latest security patches and upgrades	34.8%	44.5%	15.5%	1.9%	3.2%	224.65	0.000
The university security policy requires all smart mobile devices to have an approved operating system	30%	40.9%	18.1%	10.3%	0.6%	147.61	0.000
The university security policy permits use of personally-owned devices	31.0%	46.5%	15.5%	5.9%	1.2%	214.19	0.000
I have read and clearly understood the university security policy	32.9%	38.7%	17.4%	9.0%	1.9%	150.32	0.000
The university has an ICT security policy which is implemented and enforced	29.0%	45.8%	15.5%	5.9%	3.9%	205.68	0.000

Key: SD = Strongly Disagree, D=Disagree, N = Neutral, SA = Strongly Agree, A = Agree and %=Percentage

The data showed that 79.3% of the respondents significantly (χ^2=224.65; $p<0.05$) disagreed that the university security policy requires all smart mobile devices to have latest security patches and upgrades which was supported by 70.9% who differed significantly that the university security policy requires all smart mobile devices to have an approved operating system (χ^2=147.61; $p<0.05$). However, only 7.1% agreed that the university security policy permits use of personally-owned devices. Similarly, 71.6% disagreed that the university has an ICT security policy which is implemented and enforced. It was noted that nearly all the respondents significantly (χ^2=150.32; $p<0.05$) disagreed that they have read and clearly understood the university security policy.

4.3.2. Threats Assessed in Information Security Policy Section

The questions asked in this section were used to assess different types of threats as indicated in table 4.6 below;

Table 4.6: Threats assessed to test Sufficiency of Information Security Policy

No.	Question	Threat Assessed
1.	The university security policy requires all smart mobile devices to have latest security patches and upgrades	Malware
2.	The university security policy requires all smart mobile devices to have an approved operating system	Malware
3.	The university security policy permits use of personally-owned devices	Theft or Loss
4.	I have read and clearly understood the university security policy	Lack of User Awareness
5.	The university has an ICT security policy which is implemented and enforced	Lack of User Awareness

4.3.3. Management of Smart mobile Devices within the Network

Table 4.7: Management of Smart Devices within the Network

Statement	SD	D	N	A	SA	χ^2	p
Whenever I am selling my smart mobile device, I always reset my device to factory setting and clear any saved data	31.3%	46.5%	13.9%	3.9%	4.5%	211.52	0.000
My smart mobile device can be locked if lost or stolen	32.9%	45.5%	16.5%	2.3%	2.9%	222.52	0.000
The university maintains a secured inventory of all smart mobile devices.	34.5%	45.8%	12.2%	5.6%	1.9%	237.13	0.000
The university security policy outlines reporting procedures for lost, stolen, or damaged smart mobile devices	28.6%	44%	14.5%	8.7%	4.2%	212.19	0.000
The university insures smart mobile devices against loss, theft, or damage	33.2%	40.6%	15.2%	8.4%	2.6%	164.74	0.000
The university security policy prohibits leaving smart mobile device unattended when attached to a corporate computer	34.2%	39.4%	16.5%	8.1%	1.9%	163.90	0.000
The security policy clearly specifies penalties for unauthorized use of smart mobile devices	28.6%	44%	14.5%	8.7%	4.2%	212.19	0.000
My smart mobile device characteristics are registered in the university database	33.2%	40.6%	15.2%	8.4%	2.6%	164.74	0.000

Key: SD = Strongly Disagree, D=Disagree, N = Neutral, SA = Strongly Agree, A = Agree and %=Percentage

The results revealed that 12.9% and 11% agreed that the university security policy outlines reporting procedures for compromised smart mobile devices and that their smart mobile device characteristics are registered in the university database respectively whereas 72.6% and 73.8% differed significantly (χ^2=212.19, & 164.74; $p<0.05$) respectively. The finding further showed that 80.3% of the respondents significantly (χ^2=237.13; $p<0.05$) disagreed that the university maintains a secured inventory of all smart mobile devices which was confirmed by 78.4% who significantly (χ^2=222.52; $p<0.05$) disagreed that their smart mobile device can be locked if lost or stolen. This view was further supported by 77.8% who significantly (χ^2=211.52; $p<0.05$) disagreed that they reset their smart mobile devices to factory settings neither do they clear their stored data before selling their device. It was clear that 73.8% disagreed that the university insures smart mobile devices against loss, theft, or damage. In view of the security policy, 73.6% of responses disagreed that the university security policy prohibits leaving smart mobile device unattended when attached to a corporate computer. This observation was upheld by 72.6% who affirm that the security policy does not clearly specifies penalties for unauthorized use of smart mobile devices

4.3.4. Threats Assessed in Management of Smart Mobile Devices Section

The questions asked in this section were used to assess different types of threats as indicated in table 4.8 below;

Table 4.8: Threats assessed in Management of Smart Mobile Devices

No.	Question	Threat Assessed
1.	The university security policy outlines reporting procedures for compromised smart mobile devices	Lack of User Awareness
2.	My smart device can be locked or its password can be changed if lost or stolen	Unauthorized Access
3.	The university maintains a secured inventory of all smart mobile devices.	Theft or Loss
4.	The university security policy outlines reporting procedures for lost, stolen, or damaged smart mobile devices	Theft or Loss

5.	The university insures smart mobile devices against loss, theft, or damage	Theft or Loss
6.	The university security policy prohibits leaving smart mobile device unattended when attached to a corporate computer	Data Leakage
7.	The security policy clearly specifies penalties for unauthorized use of smart mobile devices	Phishing Attack
8.	My smart mobile device characteristics are registered in the university database	Theft or Loss

4.3.5. Access Control of Smart Mobile Devices within and Outside the Network

Table 4.9: Access Control of Smart Mobile Devices within and outside the Network

Statement	SD	D	N	A	SA	χ^2	P
My smart mobile device has multiple authentication mechanisms eg Password, Fingerprint, on-screen pattern etc	29.4%	39.0%	16.8%	6.8%	8.1%	120.52	0.000
My smart mobile device uses password protection when not in use	32.6%	45.5%	13.2%	3.9%	4.8%	208.26	0.000
Allocation and reallocation of passwords is controlled through a formal management process	32.6%	46.1%	16.1%	2.3%	2.9%	226.77	0.000
I always disable or protect remote access to my smart mobile device whenever connected to the network	32.9%	45.5%	16.5%	2.3%	2.9%	222.52	0.000
My smart mobile device is set to lock screen whenever not in use for a certain period of time	34.5%	45.8%	15.2%	2.6%	1.9%	237.13	0.000

My smart mobile device has a unique name and password which is not known by anyone else	35.2%	38.1%	16.8%	8.7%	1.3%	161.84	0.000
My smart mobile device can hide data, after pre-defined number of failed logon attempts	32.6%	45.5%	14.5%	4.2%	3.2%	212.19	0.000
All smart mobile devices within the university network are monitored for unauthorized activities	34.2%	39.4%	16.5%	8.1%	1.9%	163.90	0.000
My smart mobile device undergoes authentication process before connecting to the university network	34.2%	39.4%	16.5%	8.1%	1.9%	163.90	0.000

Key: SD = Strongly Disagree, D=Disagree, N = Neutral, SA = Strongly Agree, A = Agree and %=Percentage

Regarding internet connectivity, it was observed that 73.6% significantly (χ^2=163.90; p<0.05) disagreed that their smart mobile devices undergo authentication process before connecting to the university network. This assessment was confirmed by 68.4% who disagrees that their smart mobile device has multiple authentication mechanisms e.g. Password, Fingerprint, on-screen pattern. As to whether smart mobile devices are monitored for unauthorized use when connected to university network, 73.6% disagreed leaving only 10% in support. Similarly, 78.4% assert that they do not protect their smart mobile device from remote access whenever they are connected to the university network. Passwords are critical in access controls. It was noted that 78.7% significantly (χ^2=226.77; p<0.05) disagreed that allocation and reallocation of passwords is controlled through a formal management process. This view was then supported by 73.3% and 78.1% who disagree that their smart mobile device has a unique name and password which is not known by anyone else and that their smart mobile devices uses password protection when not in use. This was further confirmed by 78.1% who disagreed that their smart mobile device can hide data, after pre-defined number of failed logon attempts. It was reported that 80.3% significantly (χ^2=237.13; $p<0.05$) disagreed to have set their smart mobile device to lock screen whenever the device remain not in use for a certain period of time.

4.3.6. Threats Assessed to Test Access Control of Smart Mobile Devices Section

The questions asked in this section were used to assess different types of threats as indicated in table 4.10 below;

Table 4.10: Threats Assessed to test Access Control to Smart Mobile Devices

No.	Question	Threat Assessed
1.	Access control policy is developed and reviewed based on the university security requirements	Unauthorized Access
2.	My smart mobile device has multiple authentication mechanisms e.g Password, Fingerprint, on-screen pattern etc	Unauthorized Access
3.	My smart mobile device is checked for identified security requirements before being granted access to the organization's information or assets	Malware
4.	Allocation and reallocation of passwords is controlled through a formal management process	Unauthorized Access
5.	I always disable or protect remote access to my smart mobile device whenever connected to the network	Data Leakage
6.	There are security practices in place to guide users in selecting and maintaining secure passwords	Lack of User Awareness
7.	My smart mobile device has a unique name and password which is not known by anyone else	Unauthorized Access

8.	My smart mobile device has enabled manufacturers debugging features	Unauthorized Access
9.	All smart mobile devices within the university network are monitored for unauthorized activities	Viruses
10.	My smart mobile device undergoes authentication process before connecting to the university network	Data Leakage

4.3.7 Operations Security Safeguard

Table 4.11: Operations Security Safeguard

Statement	SD	D	N	A	SA	χ^2	p
When downloading applications, I always use the official downloading sites	31.6%	37.7%	6.5%	14.2%	10.0%	118.87	0.000
My smart mobile device is updated and configured to install new updates whenever available	32.3%	42.3%	12.9%	6.5%	6.1%	166.16	0.000
Smart mobile devices are monitored when connected to the university computer or network	31.6%	46.5%	15.2%	4.2%	2.6%	218.74	0.000
My smart mobile device has some unapproved software and applications	28.6%	44%	15.2%	6.7%	5.6%	216.64	0.000
Manufacturer debugging features on my smart mobile device are disabled	31.6%	46.5%	13.2%	3.9%	4.8%	212.42	0.000
My smart mobile device contain an updated antivirus software that scans files as they are opened	32.9%	45.5%	16.5%	2.3%	2.9%	222.52	0.000

My smart mobile device has password expiration feature that allows password to expire after pre-defined time length	33.2%	46.8%	15.5%	2.6%	1.9%	239.00	0.000
I regularly synchronize my smart mobile device with university computer or network, for backup purposes	32.9%	45.5%	16.5%	2.3%	2.9%	222.52	0.000
The security policy outlines approved Modes of Operation: wired and wireless	34.5%	45.8%	15.2%	2.6%	1.9%	237.13	0.000
The university security policy specifies the types of information that can and cannot be stored, processed, and transferred on smart mobile devices	35.2%	38.1%	16.8%	8.7%	1.3%	161.84	0.000
My smart mobile device is automatically examined for compliance with the university security policy once I connect to its network	32.6%	45.5%	14.5%	4.2%	3.2%	212.19	0.000
My smart mobile device contain both personal and university data	34.2%	39.4%	16.5%	8.1%	1.9%	163.90	0.000

Key: SD = Strongly Disagree, D=Disagree, N = Neutral, SA = Strongly Agree, A = Agree and %=Percentage

According to table 4.11, 24.2% of respondents significantly (χ^2=118.87; $p<0.05$) agreed that when downloading applications, they always use the official downloading sites. Similarly, 5.2 % agrees that their smart mobile device contain updated antivirus software that scans files as they are opened. However, 16.5% were not sure whether their smart mobile device contained both personal and corporate data. It has been documented that updating of operating applications in vital in improving security devices in a network. It was noted that 74.6% significantly (χ^2=166.16; $p<0.05$) disagreed that their smart mobile device is updated and configured to install new updates whenever available.

Additionally, it was noted that respondents disagrees that the university security policy specifies the types of information that can and cannot be stored, processed, and transferred on smart mobile devices (73.3%)and that the security policy outlines approved Modes of Operation: wired and wireless(80.3%). Since the respondents outlined that their smart mobile device is not automatically examined for compliance with the university security policy once they connect to its network (78.1%), it is possible that their smart mobile device has some unapproved software and applications (12.3%) as reported. Moreover, 78.4% also reported that the do not regularly synchronize their smart mobile device with organizational computer or network, for backup purposes.

4.3.8 Threats Assessed in Operations Security Safeguard Section

The questions asked in this section were used to assess different types of threats as indicated in table 4.12 below;

Table 4.12: Threats assessed to test Operations Security Safeguard

No.	Question	Threat Assessed
1.	When downloading applications, I always use the official downloading sites	Phishing Attack
2.	My smart mobile device is updated and configured to install new updates whenever available	Viruses
3.	My smart mobile device has some unapproved software and applications	Malware
4.	My smart mobile device contain an updated antivirus software that scans files as they are opened	Viruses
5.	My smart mobile devices is assigned a unique Internet Protocol (IP) address each time I connect to the university network	Man-in-the-Middle Attack

6.	I regularly synchronize my smart mobile device with organizational computer or network, for backup purposes	Man-in-the-Middle Attack
7.	The security policy outlines approved Modes of Operation: wired and wireless	Unsecured Network
8.	The university security policy specifies the types of information that can and cannot be stored, processed, and transferred on smart mobile devices	Lack of User Awareness
9.	My smart mobile device is automatically examined for compliance with the university security policy once I connect to its network	Phishing Attack
10.	My smart mobile device contain both personal and corporate data	Data Leakage

4.3.9. Secure Communication Safeguard

Table 4.13: Secure Communications Safeguard

Statement	SD	D	N	A	SA	χ^2	P
I always connect my smart device to free public Wi-Fi whenever available	32.6%	46.8%	16.1%	2.3%	2.3%	235.55	0.000
Unneeded applications and services within the university network are disabled	33.9%	47.1%	15.5%	2.3%	1.3%	249.84	0.000
Unneeded network connections within the university network are disabled	30.0%	48.1%	14.5%	4.2%	3.2%	224.58	0.000
The university implements VPN software for smart devices, for remote network connections	33.9%	45.2%	16.8%	2.3%	1.9%	228.94	0.000
The university implements a firewall on smart devices	33.9%	46.5%	15.5%	2.9%	1.3%	241.00	0.000

The university implements encryption to protect information on smart devices	35.8%	39.7%	15.5%	7.4%	1.6%	178.84	0.000
Updated signatures are installed on my smart device each time they synchronize to a university computer or at regular intervals via a secure network connection	28.7%	47.4%	14.5%	5.8%	3.5%	206.13	0.000
The university security policy require all smart devices to use a password to synchronize to an organizational computer or network	33.9%	38.1%	18.1%	8.4%	1.6%	154.29	0.000
The university security policy provides protective measures against social engineering and other security attacks	30.0%	45.8%	14.5%	6.1%	3.5%	195.16	0.000
The university security policy prohibits use of public or untrusted network access points	35.8%	39.7%	15.5%	7.4%	1.6%	178.84	0.000
Smart device is not used to store, process, or transfer sensitive, proprietary, or classified data, unless encryption is used	28.7%	47.4%	14.5%	5.8%	3.5%	206.13	0.000

Key: SD = Strongly Disagree, D=Disagree, N = Neutral, SA = Strongly Agree, A = Agree and %=Percentage

It can be observed that 79.4% of respondents significantly (χ^2=235.55;p<0.05) disagreed that they always connect their smart mobile device to free public Wi-Fi whenever available and used to store, process, or transfer sensitive, proprietary, or classified data, unless encryption is used (76.1%). However, 3.6% differs that unneeded applications and services within the university network are disabled as confirmed by a similar 7.4% who reports that unneeded network connections within the university network are disabled.

As regards university security policy, it was established that respondents disagreed that the university security policy prohibits use of public or untrusted network access points and that the university security policy provides protective measures against social engineering and other security attacks with 75.5% (χ^2=178.84;$p<0.05$) and 75.8% (χ^2=195.16;$p<0.05$) respectively. Moreover, 76.1% of respondents disagreed that updated signatures are installed on their smart mobile devices each time they synchronize to a university computer or at regular intervals via a secure network connection. This was supported by 72% (χ^2=154.29; $p<0.05$) who disagreed that the university security policy require all smart mobile devices to use a password to synchronize to an organizational computer or network.

It was evident that 79.1% of respondents disagreed that the university implements VPN software for smart mobile devices, for remote network connections while 80.4% confirms the position by disagreeing that the university implements a firewall on smart mobile devices. Notably, 75.5 % disagree further with the view that the university implements encryption to protect information on smart mobile devices.

4.3.10 Threats Assessed in Secure Communication Safeguard Section

The questions asked in this section were used to assess different types of threats as indicated in table 4.14 below;

Table 4.14: Threats assessed to test Communication Security Safeguard

No.	Question	Threat Assessed
1.	I always connect my smart mobile device to free public Wi-Fi whenever available	Unsecured Network

2.	Unneeded applications and services within the university network are disabled	Malware
3.	Unneeded network connections within the university network are disabled	Unsecured Network
4.	The university implements VPN software for smart mobile devices, for remote network connections	Man-in-the-Middle Attack
5.	The university implements a firewall on smart mobile devices	Unsecured Network
6.	The university implements encryption to protect information on smart mobile devices	Data Leakage
7.	Updated signatures are installed on my smart mobile device each time they synchronize to a university computer or at regular intervals via a secure network connection	Viruses
8.	The university security policy require all smart mobile devices to use a password to synchronize to an organizational computer or network	Man-in-the-Middle Attack
9.	The university security policy does not allow smart mobile devices to be simultaneously connected to other devices while connected to university computer or network	Viruses
10.	The university security policy provides protective measures against social engineering and other security attacks	Phishing Attack
11.	The university security policy prohibits use of public or un-trusted network access points	Unsecured Network
12.	Smart mobile device is not used to store, process, or transfer sensitive, proprietary, or classified data, unless encryption is used	Man-in-the-Middle Attack

4.4. Design of Threat Matrix to Show the Security Status of the University Network

4.4.1. Correlation Analysis between Information Security Policy and Likelihood of Attack

A correlation analysis was conducted using average scores as obtained from staff and students (herein referred to as users) assessment. This was to determine the nature of relationship between Information Security Policy and Likelihood of Attack.

The result of the correlation is shown in Table 4.15 and discussion made thereafter.

Table 4.15: Correlation between Information Security Policy and Likelihood of Attack

		Likelihood of Attack	Information Security Policy
Likelihood of Attack	Spearman's rho Correlation Coefficient	1.000	-0.288**
	Sig. (2-tailed)	.	.000
	N	310	310

**. Correlation is significant at the 0.01 level (2-tailed).

It was observed that there exist a negative and statistically significant relationship between Information Security Policy and Likelihood of Attack (r= -0.288**; p<0.01). This implies that as Information Security Policy is enhanced in the university network, likelihood of attack decreases. Conversely laxity in tightening of Information Security Policy increases chances of likelihood of attack.

4.4.2. Correlation Analysis between Asset Management and Likelihood of Attack

A correlation analysis was conducted using average scores as obtained from staff and students (herein referred to as users) assessment. This was to determine the nature of relationship between Asset Management and Likelihood of Attack. The result of the correlation is shown in Table 4.16 and discussion made thereafter.

Table 4.16: Correlation between Asset Management and Likelihood of Attack

		Likelihood of Attack	**Asset Management**
Likelihood of Attack	Spearman's rho Correlation Coefficient	1.000	-0.505**
	Sig. (2-tailed)	.	.000
	N	310	310

**. Correlation is significant at the 0.01 level (2-tailed).

It was noted that there exist a negative and statistically significant relationship between Asset Management and Likelihood of Attack (r= -0.505**; *p*<0.01). This implies a weakened Asset Management increases chances of likelihood of attack while a strengthened Asset Management policy reduces Likelihood of Attack.

4.4.3. Correlation Analysis between Access Control and Likelihood of Attack

A correlation analysis was conducted using average scores as obtained from staff and students (herein referred to as users) assessment. This was to determine the nature of relationship between Access Control and Likelihood of Attack.

The result of the correlation is shown in Table 4.17 and discussion made subsequently.

Table 4.17: Correlation between Access Control and Likelihood of Attack

		Likelihood of Attack	**Access Control**
Likelihood of Attack	Spearman's rho Correlation Coefficient	1.000	-0.472**
	Sig. (2-tailed)	.	.000
	N	310	310

**. Correlation is significant at the 0.01 level (2-tailed).

Finding established that there exist a negative and statistically significant relationship between Access Control and Likelihood of Attack (r= -0.472**; p<0.01). This implies that when Access Controls is tightened in the network, chances of an attack decrease.

4.4.4. Correlation Analysis between Operations Security and Likelihood of Attack

A correlation analysis was conducted using average scores as obtained from staff and students (herein referred to as users) assessment. This was to determine the nature of relationship between Operations Security and Likelihood of Attack.

The results are shown in Table 4.18 and discussion made successively.

Table 4.18: Correlation Analysis between Operations Security and Likelihood of Attack

		Likelihood of Attack	**Operations Security**
Likelihood of Attack	Spearman's rho Correlation Coefficient	1.000	-0.473**
	Sig. (2-tailed)	.	.000
	N	310	310

**. Correlation is significant at the 0.01 level (2-tailed).

It was noted that there exist a strong, negative and statistically significant relationship between Operations Security and Likelihood of Attack (r= -0.473**; p<0.01). This infers that a weakened Operations Security increases chances of likelihood of attack while a reinforced Operations Security policy reduces Likelihood of Attack in a network.

4.4.5. Correlation Analysis between Communications Security and Likelihood of Attack

A correlation analysis was conducted using average scores as obtained from staff and students (herein referred to as users) assessment. This was to determine the nature of relationship between Communications Security and Likelihood of Attack.

The result of the correlation is shown in Table 4.19 and discussion made successively.

Table 4.19: Correlation Analysis between Communications Security and Likelihood of Attack

		Likelihood of Attack	Communications Security
Likelihood of Attack	Spearman's rho Correlation Coefficient	1.000	-0.834**
	Sig. (2-tailed)	.	.000
	N	310	310

**. Correlation is significant at the 0.01 level (2-tailed).

It was notable from findings that there exist a weak, negative and statistically significant relationship between Communications security and Likelihood of Attack (r= -0.834**; *p*<0.01). This assumes that a weakened Communications security increases risks of likelihood of attack while a strengthened Communications security policy lessens Likelihood of Attack in a network.

4.5. Regression Analysis

Regression was done using average scores from all the independent variables in order to predict the dependent variable. During this analysis, data from students and staff were used in the model since this is what determined possibility of threats attack to university network through use smart mobile devices. The following table shows the output from the analysis.

Table 4.20: Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.707[a]	.500	.492	.335

a. Predictors: (Constant), Communications Security, Asset Management, Access Control, Operations Security, Information Security Policy

It was established that 50% of the variation in the Likelihood of Attack can be explained by the independent variables of Communications Security, Asset Management, Information Security Policy, Operations Security, and Access Control with a standard error of estimate being 0.335.

4.5.1. Regression Weights

The estimated coefficients for the model are presented in Table 4.21. The Unstandardized beta Coefficients will be used in prediction of dependent variable.

Table 4.21: Coefficients [a]

Model	Unstandardized Coefficients		Sig.
	B	Std. Error	
(Constant)	5.233	.082	.000
Information security policy	-.084	.028	.003
Asset management	.199	.073	.007
Access control	-.003	.082	.968
Operations security	-.101	.071	.156
Communications security	-.530	.040	.000

a. Dependent Variable: Likelihood of Attack

a) Threat Matrix Equation

Likelihood of attack was computed using equation 3 as shown below.

$$Y=C+\beta1X1+ \beta1X2+ \beta1X3+ \beta1X4+ \beta1X5+\mathcal{E}$$

Equation 3: Threat Matrix Equation

Source: Researcher (2018)

Where C represents Constant that is the point where the regression line cuts the y-axis

Ɛ is standard error of estimate

β1 is the weight of independent variables as obtained after running the regression analysis

X1, X2, X3, X4 and X5 are scores earned on every independent variable

Using the constant, the unstandardized beta coefficients and standard error obtained from the regression analysis, likelihood of attack was hence computed as shown below.

Likelihood of Attack =5.233 + (-0.084*Information Security Policy) + **(**0.199*Asset Management) + (-0.003*Access Control) + (-0.101*Operations Security) + (-0.530*Communications Security) + 0.335.

4.6 Matrix implementation and discussion

This section explains how threat matrix was implemented in an attempt to answer question three of the research. Details of how the matrix was developed and implemented are presented in the subsequent sections.

4.7 Design Overview of TM System

This section describes an overview of Threat Matrix (TM) which includes, but not limited to, the objectives, system functionalities, processes and the system architecture as described in sections 4.7.1 to 4.7.5 below.

4.7.1 Design Objective

This study aimed at designing a threat matrix as a web-based model to determine the levels of security threats resulting from increased use of smart mobile devices in the university network. The model was expected to provide important security information to both users of the smart mobile devices (herein referred to as users) and to the ICT team of experts (herein referred to as professionals) who are the custodians of security in the university network. Through this model, users were to be informed on how to securely use their smart mobile devices whereas the ICT professionals would be able to know the security loopholes that need to be patched. Besides, the model would assist the university by providing the relevant information necessary in order to comply with international security standards such as ISO 27001 ISMS requirements.

4.7.2 Functional Overview

The matrix being a web-based application required employment of the latest web technologies in design. Hypertext preprocessor (PHP), therefore, was used as a server-side scripting language to design the model whereas MySQL was employed as a database engine. In addition, Bootstrap 4 was used for user interface styling.

To guarantee that only authenticated users were allowed access to the system, the first interface of the model provided a platform which prompted users to register with both username and password. The correct combination of both username and password was to allow users to login to access system functionalities such as clear previous assessment, run new threat assessment, view their average score and view or download recommendations.

4.7.3 TM System Processes

To test the effectiveness of the model, rapid prototyping was used. Model development was guided by the following processes;

a) **Gathering of the Requirement Process:** through experiences from other university networks and the growing concern of security of smart mobile devices as highlighted in the literature review, the researcher was able to gather the requirement of an effective Threat Matrix (TM).

b) **Rapid design Process:** Flow diagrams were used to display a quick conceptual framework of system database and modules. An overall design of different modules for both users and ICT professionals are shown in figure 6 below.

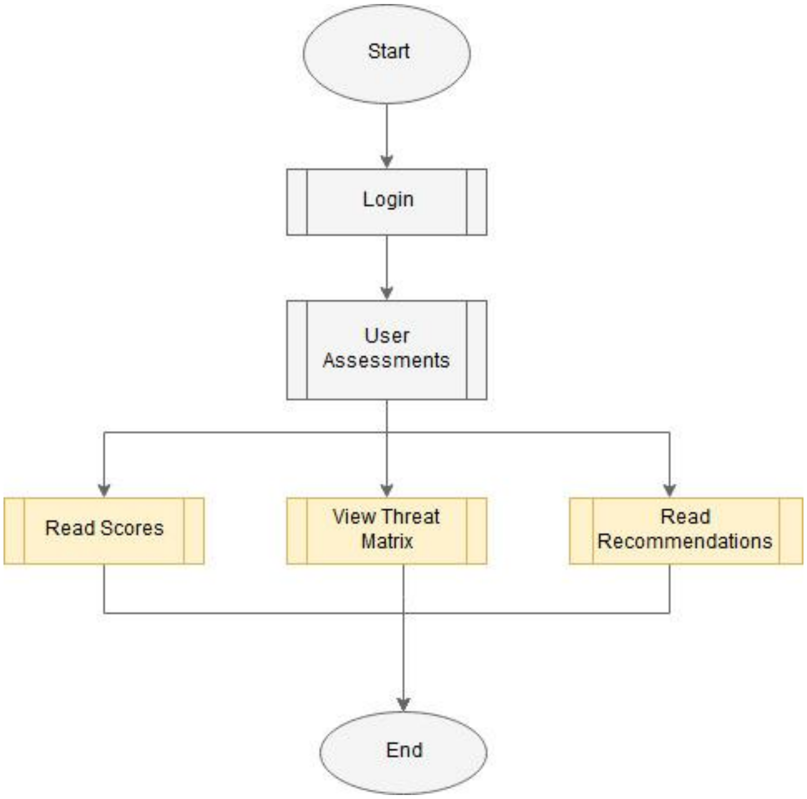


Figure 6: Web-based TM System Flowchart

Source: Researcher (2018)

c) **Prototype Design Process:** To provide interactive and styling functions, Bootstrap 4 was used as a CSS framework. PHP server side scripting language was used to develop the prototype and MySQL as the database engine.

d) **Evaluation Process:** Goal-based evaluation technique was used to test the prototype against gathered system objectives. This provided an insight to the functionality of the model and helped to capture any changes needed at an early stage of development.

e) **Coding and testing Processes:** Coding was done after all the requirements were gathered. To ensure that the system met the expected results, a link was sent to several end-users to test the system by registering and performing other system functionalities such as running threat assessment and clearing previous assessment. The feedback received helped in further refining the system.

f) **Deployment Process:** A complete prototype files and database were deployed online.

4.7.4 TM System Architecture

TM system comprised of different independent modules which perform different functions. The major modules are as listed below;

a) **User Registration Module:** This is a module that allows different categories of users (staff, student of ICT professionals) to register by providing compulsory information such as username, e-mail address, name of the organization and a unique password. The users were also expected to select the type of user from the user-category which determines the next interface that user will be able to view.

b) **User authentication module:** this module was used to control access to the system by allowing only the registered users to login into the system. The login was successful only when the user provides correct combination of both username and password.

c) **Password management Module:** This module allowed encryption of passwords. It was used to determine the complexity of the password and verify if the password entered was correct or not. STM system uses SHA 256 hashing algorithm to encrypt password information at the database level.

d) **User Session handling module:** This module handled user sessions by detecting when a user successfully logged into the system, the activities that the user performs while logged in. Besides, this module was responsible for destroying the session when the user logged out of the system. This module was also used to enhance security by automatically logging out the user when a session remained idle for a specified amount of time. This helped to prevent unauthorized access of the system.

e) **Home Page Module:** This module was designed primarily to display content depending on the type of category. It is therefore referred in this context as dashboard. The User dashboard allows the user to assess their likelihood of attack from various threats; to run threat assessment, to clear previous assessments, to views average scores obtained resulting from the assessment and to view suggested recommendations as a result of the assessment. The ICT professional dashboard displays to professionals the cumulative likelihood of attack obtained from various assessments run by staff or students. It also allows the professionals to run their own professional assessment which is basically inputting the policy status of the university to mitigate threats. It also allows them to clear the previous assessments. This module also contains organization recommendations which should be applied to improve the security standards of the university network.

f) **Run Assessment module:** In this module, users are allowed to answer questions retrieved from the database in form of likert scale of 1 to 5 whereby the users are expected to check the radio button that represents their most suitable answer. Once completed the user is allowed to submit the results.

g) **Reports Module:** This module contains recommendations which are generated from the results obtained after running threat assessment. It also contains scores for each question as examined in threat assessment. This is what determines the recommendations that the system suggests for the user based on their assessment scores.

h) **Help Module:** This module acts as a user guide to assist users in learning how to navigate through the system and perform system functions.

i) **Databases:** The TM platform maintains five working databases, that is; (i) users database which stores all registered users for the purpose of referencing when users attempt to login to the system. (ii) User assessment database that stores records of users' assessments scores and the associated threats; (iii) User questions database that stores the user assessment questions, weights and associated recommendations; (iv) Professional assessment database that stores professionals' assessment scores and associated threats; (v) Professional questions database that stores professional assessment questions, the categories, associated threats and associated professional recommendations.

4.7.5 System Components Interface

The TM is a web-based application and is therefore accessible through a web-browser. Different navigation links were provided to different user category to ensure ease of use. The figure 7 below presents the TM navigation panels.

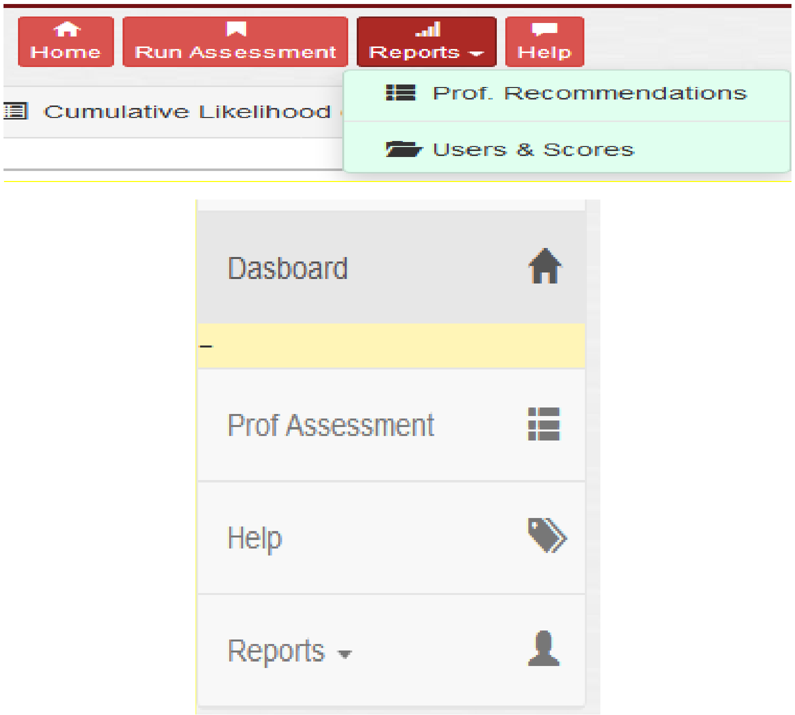


Figure 7: TM Prototype Navigation Panel

Source: Researcher (2018)

4.8 System Design and Testing

A logical design of the TM web-based model is presented in this section. It is comprised of several sections to expound on the system design and testing;

4.8.1 User Registration

This is the first section of the TM model where every user is expected to register in-order access the system. Personal details such as user name, email address, name of organization, user category and password are required in this interface. The user is also expected to agree with the terms of service provided in order to be allowed to register. Once successfully registered, the user details are saved in the database whereby the user name and password are used by the authentication module to match the details of the user for the subsequent logins. Figure 8 below provides flowchart of the registration process while figure 9 provides the graphical user interface of the registration module.

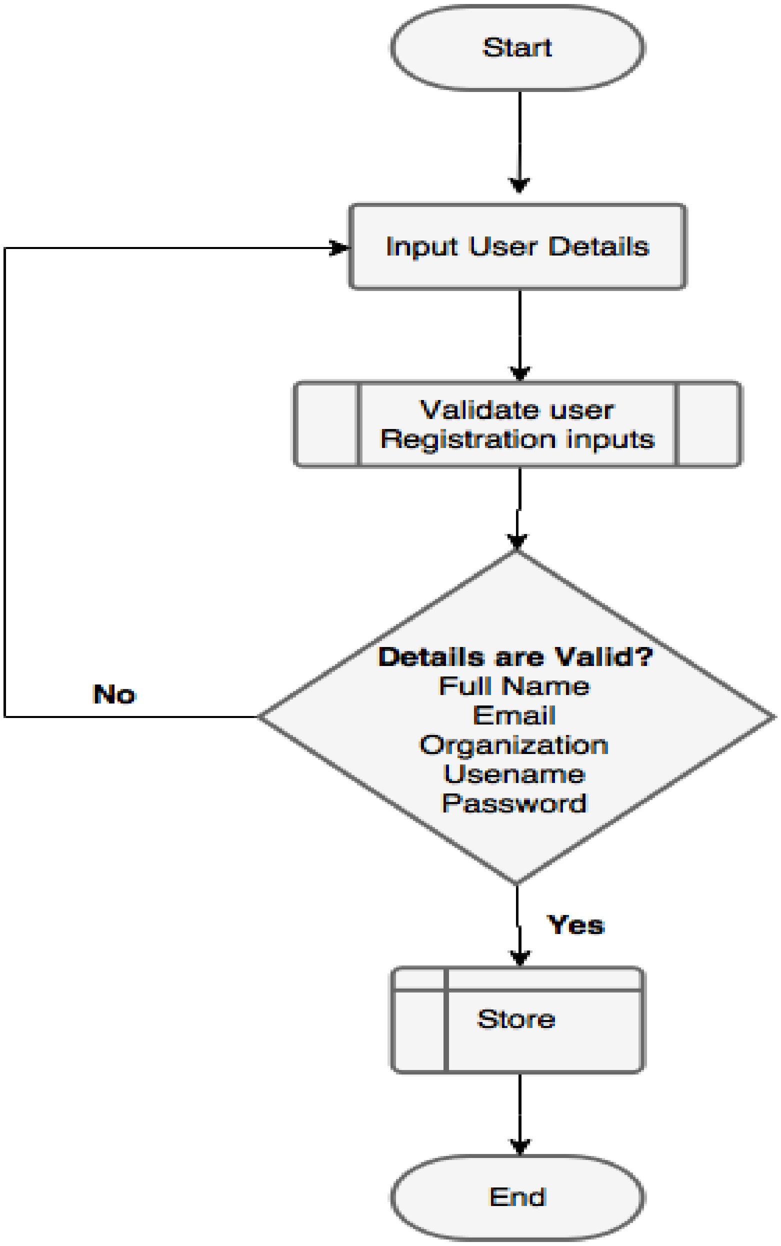


Figure 8: Registration Process Flowchart

Source: Researcher (2018)

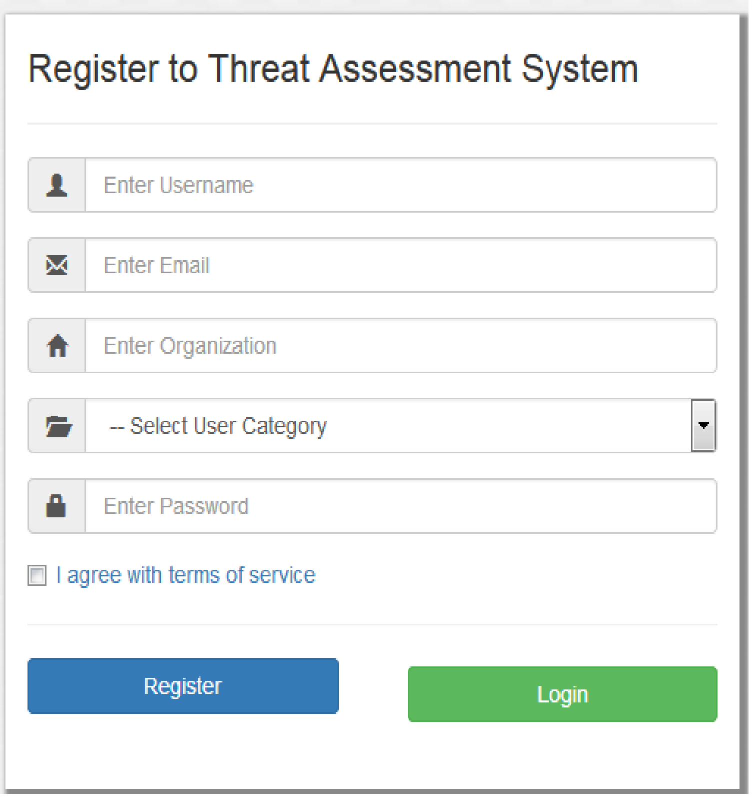


Figure 9: Registration Process GUI

Source: Researcher (2018)

4.8.2 Login Module

In this module, user sessions and logins are managed. When a user attempts to login, this module refers to the users' table in the database to determine if the user is registered or not and whether the user has provided the correct password. If the user details are not found in the database, the system displays an error message which states that the user was not found, this gives the user and opportunity to register. If the user provides an incorrect password, the system prompts the user to enter the correct password. Figure 10 below shows a flowchart representing the logic of the login system whereas figure 11 presents a graphical user interface of the login system.

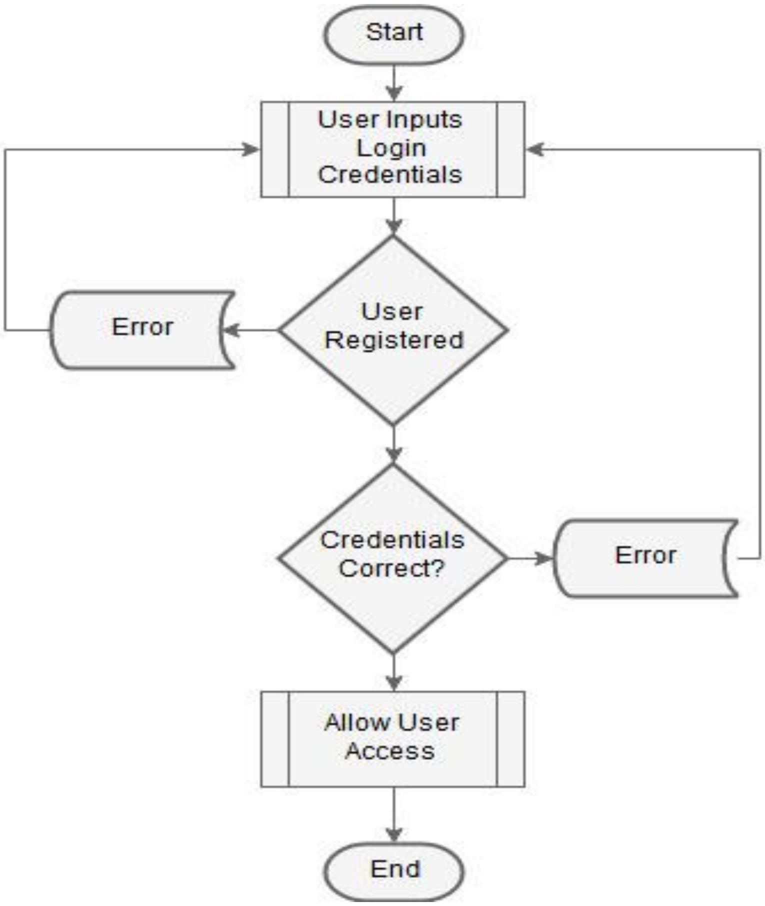


Figure 10: Login Process Flowchart

Source: Researcher (2018)

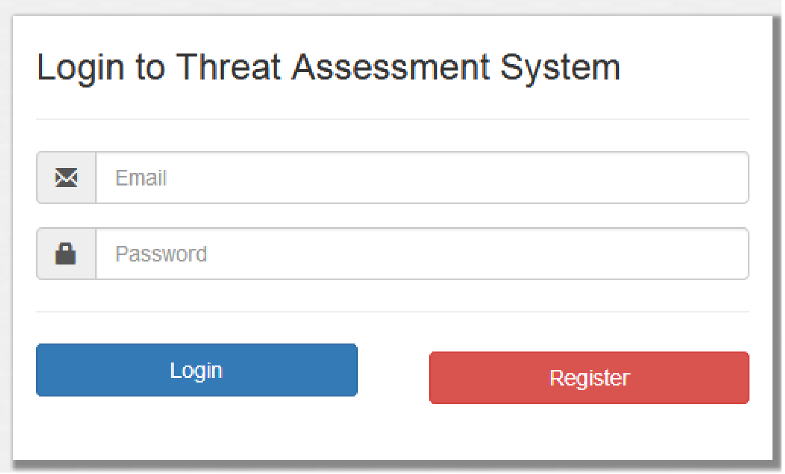

Login to Threat Assessment System

Figure 11: Login GUI

Source: Researcher (2018)

4.8.3 Threat Aassessments Module

This is a self-assessment module for staff and students in which the system displays questions which are retrieved from the database and has five choices to allow the user to select their preferred choice. Once the user has completed the assessment they are allowed to submits the results in the database from which the likelihood of attack is computed using the model equation presented in (equation 1, chapter 3) of this document. Figure 12 below shows a flowchart presentation of the assessment logic whereas figure 13 is the presentation of the graphical user interface of the risk assessment module.

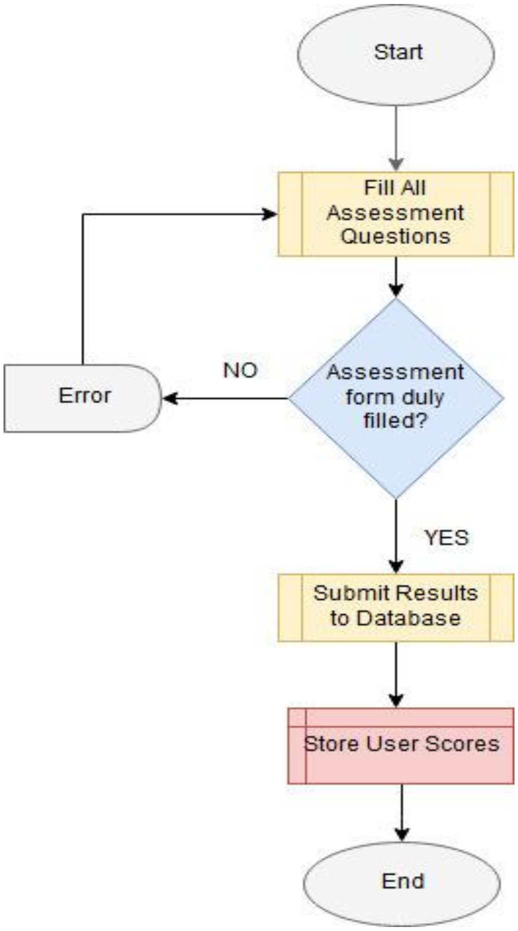
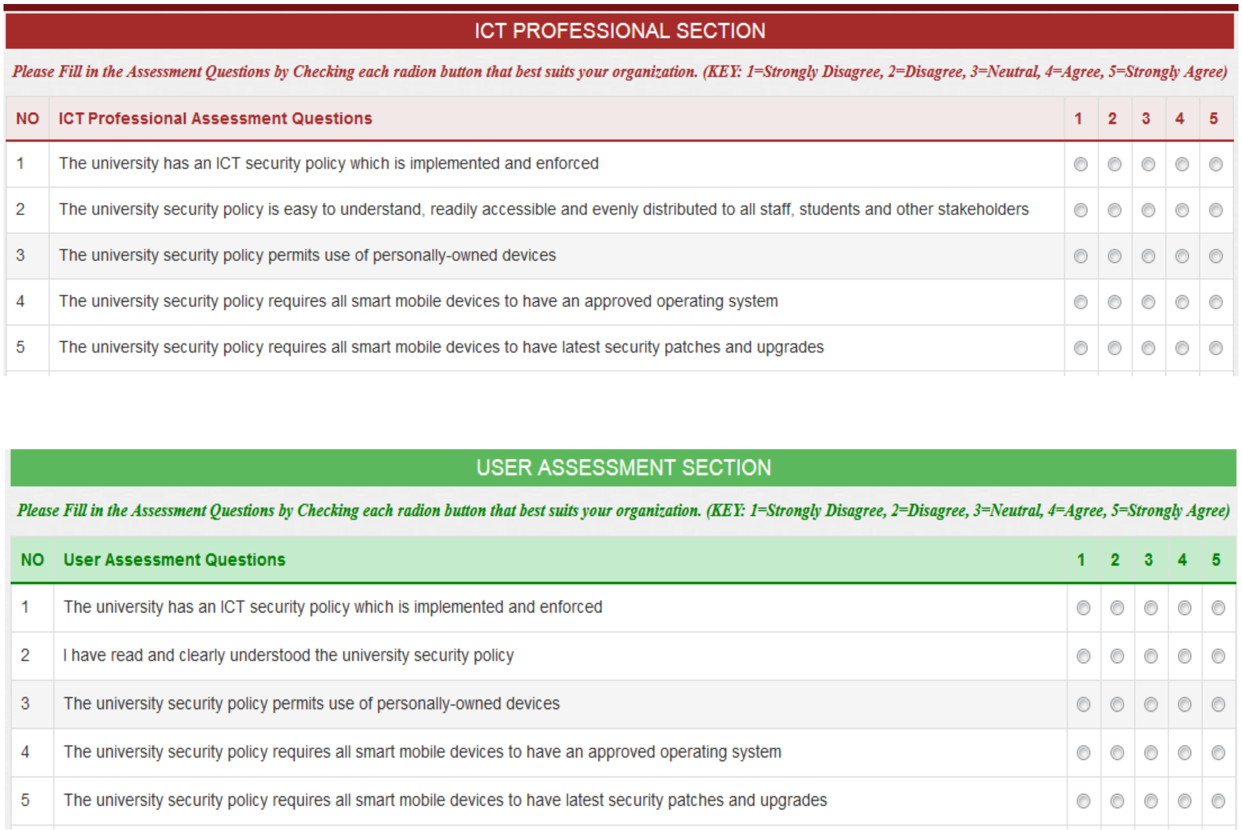

Start
Fill All Assessment Questions
Assessment form duly filled?
NO
Error
YES
Submit Results to Database
Store User Scores
End

Figure 12: Threat Assessment Flowchart

Source: Researcher (2018)



ICT PROFESSIONAL SECTION

Please Fill in the Assessment Questions by Checking each radion button that best suits your organization. (KEY: 1=Strongly Disagree, 2=Disagree, 3=Neutral, 4=Agree, 5=Strongly Agree)

NO	ICT Professional Assessment Questions	1	2	3	4	5
1	The university has an ICT security policy which is implemented and enforced	○	○	○	○	○
2	The university security policy is easy to understand, readily accessible and evenly distributed to all staff, students and other stakeholders	○	○	○	○	○
3	The university security policy permits use of personally-owned devices	○	○	○	○	○
4	The university security policy requires all smart mobile devices to have an approved operating system	○	○	○	○	○
5	The university security policy requires all smart mobile devices to have latest security patches and upgrades	○	○	○	○	○

USER ASSESSMENT SECTION

Please Fill in the Assessment Questions by Checking each radion button that best suits your organization. (KEY: 1=Strongly Disagree, 2=Disagree, 3=Neutral, 4=Agree, 5=Strongly Agree)

NO	User Assessment Questions	1	2	3	4	5
1	The university has an ICT security policy which is implemented and enforced	○	○	○	○	○
2	I have read and clearly understood the university security policy	○	○	○	○	○
3	The university security policy permits use of personally-owned devices	○	○	○	○	○
4	The university security policy requires all smart mobile devices to have an approved operating system	○	○	○	○	○
5	The university security policy requires all smart mobile devices to have latest security patches and upgrades	○	○	○	○	○

Figure 13: Threat Assessment GUI

Source: Researcher (2018)

4.8.4 Likelihood of Attack Assessment Module

This module computes likelihood of threat attack depending on the scores obtained from the submitted assessments. Likelihood of attack was computed as a function weight derived from chapter 4 of this document as demonstrated below;

Likelihood of Attack =5.233 + (-0.084*Information Security Policy) + **(**0.199*Asset Management) + (-0.003*Access Control) + (-0.101*Operations Security) + (-0.530*Communications Security) + 0.335.

Equation 4: Likelihood of Attack Equation

Source: Researcher (2018)

Threat levels are then displayed in as an index in percentage form. The threat matrix displays percentage indices in five levels, namely; very likely, likely, possible, unlikely and very unlikely. A threat is very likely to attack the university network if the user scores 1 for all the 45 assessment questions. Similarly a threat is very unlikely to attack if the user scores 5 for all the assessment questions. Possible likelihood of attack is achieved is the user scores 3 in every assessment question. Figure 14 shows a flowchart presentation of likelihood of attack computation and figure 15 displays its GUI representation.

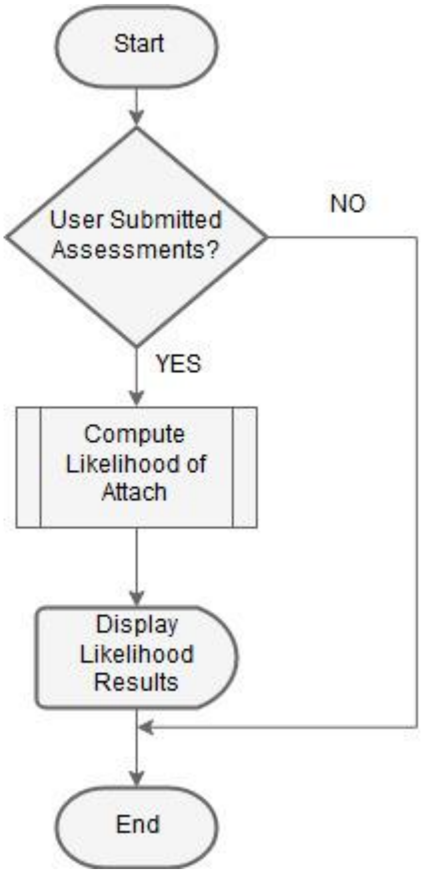

Start
User Submitted Assessments?
NO
YES
Compute Likelihood of Attach
Display Likelihood Results
End

Figure 14: Likelihood of Attack Computation

Source: Researcher (2018)

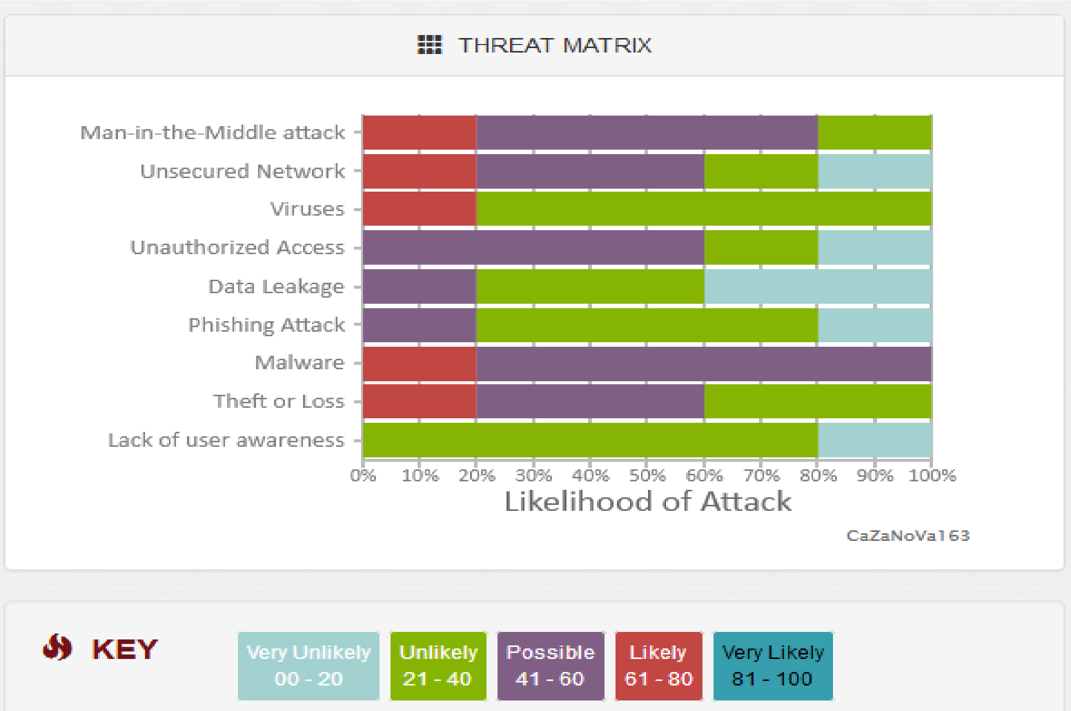


Figure 15: Threat Matrix GUI

Source: Researcher (2018)

4.8.5 User Scores Module

This module is used to display the scores based on the scores submitted by users after running threat assessment. The module also displays the date and time when the assessment was done to distinguish different assessments done on different time intervals. On the ICT professional dashboard, the system gives statistics of all the assessee who have submitted the assessment and their respective likelihood of attack in percentage format. **Best-case scenario** is achieved when the assessee scores 5 for every assessment question; this result to 100% likelihood of attack meaning it is very unlikely for the assessed threat to attack the university network. **Worst-case scenario** is achieved when the assessee scores 1 for every assessment question. This resulted to 2.6% likelihood of attack which means the assessed threats are very likely to attack the university network. Figure 16 below shows the assessment scale that was used to present the user scores.

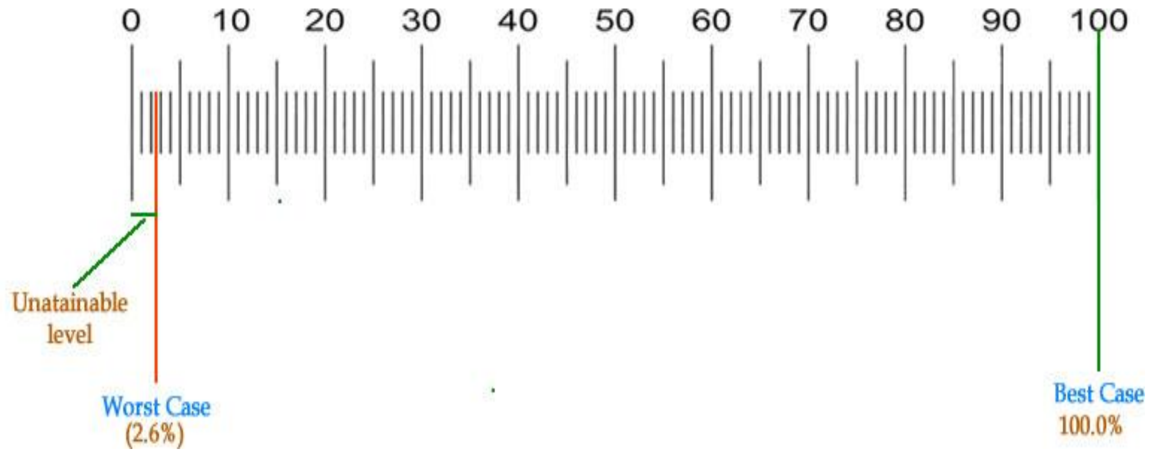


Figure 16: Scores Assessment Scale

Source: Researcher (2018)

User can then download the scores in portable document format (pdf). The figure 17 presents the assessment score retrieval logic in a flowchart. The figure 18 and 19 shows the graphical user interface from both user and professional module

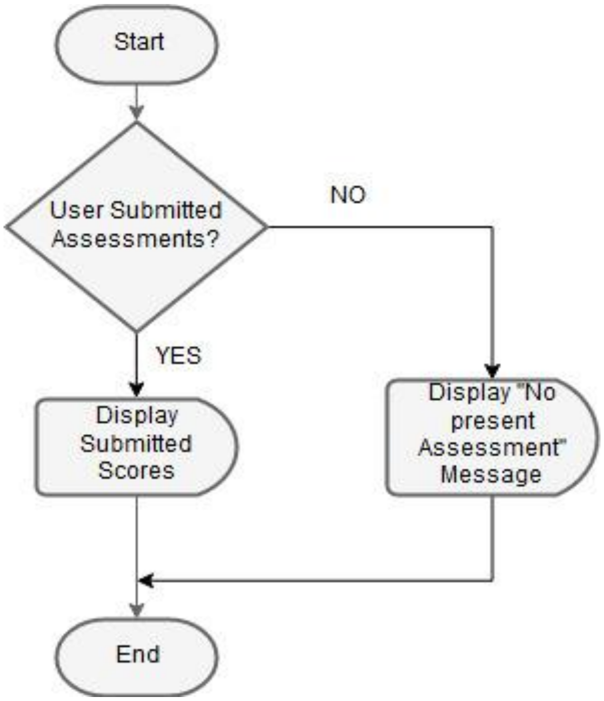
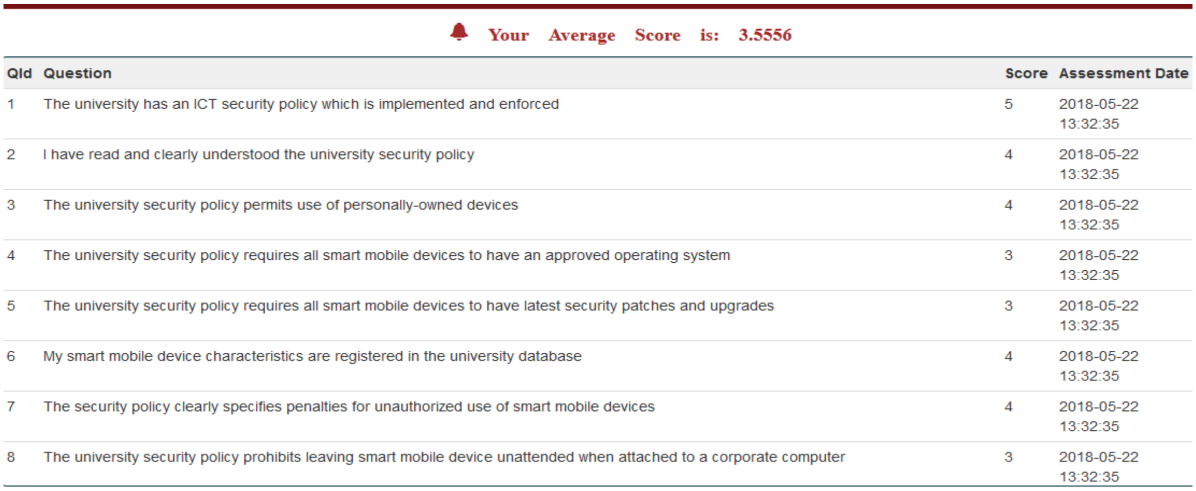

Start
User Submitted Assessments?
NO
YES
Display Submitted Scores
Display "No present Assessment" Message
End

Figure 17: Scores Flowchart

Source: Researcher (2018)

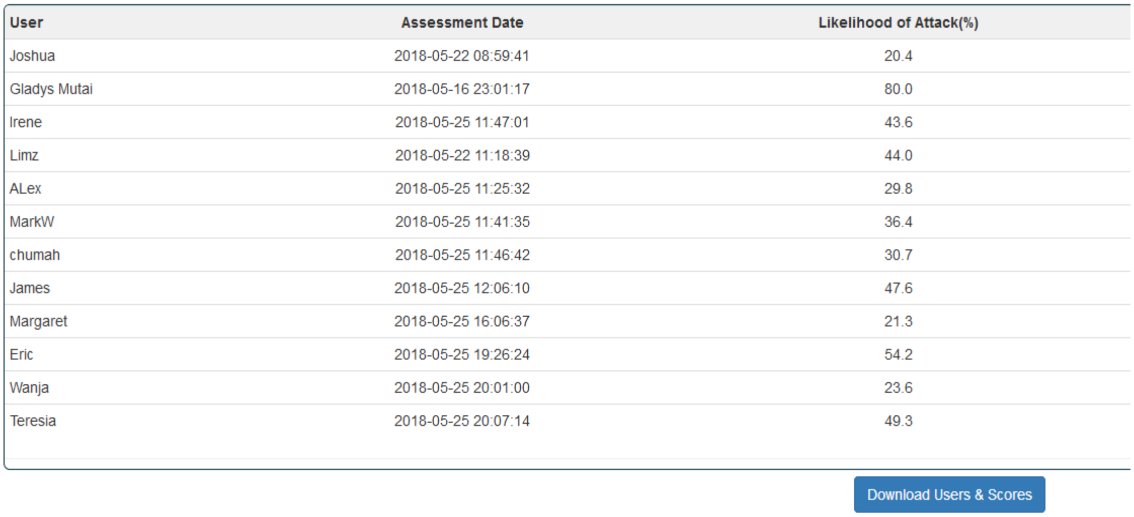


Your Average Score is: 3.5556

QId	Question	Score	Assessment Date
1	The university has an ICT security policy which is implemented and enforced	5	2018-05-22 13:32:35
2	I have read and clearly understood the university security policy	4	2018-05-22 13:32:35
3	The university security policy permits use of personally-owned devices	4	2018-05-22 13:32:35
4	The university security policy requires all smart mobile devices to have an approved operating system	3	2018-05-22 13:32:35
5	The university security policy requires all smart mobile devices to have latest security patches and upgrades	3	2018-05-22 13:32:35
6	My smart mobile device characteristics are registered in the university database	4	2018-05-22 13:32:35
7	The security policy clearly specifies penalties for unauthorized use of smart mobile devices	4	2018-05-22 13:32:35
8	The university security policy prohibits leaving smart mobile device unattended when attached to a corporate computer	3	2018-05-22 13:32:35

Figure 18: User Scores GUI

Source: Researcher (2018)



User	Assessment Date	Likelihood of Attack(%)
Joshua	2018-05-22 08:59:41	20.4
Gladys Mutai	2018-05-16 23:01:17	80.0
Irene	2018-05-25 11:47:01	43.6
Limz	2018-05-22 11:18:39	44.0
ALex	2018-05-25 11:25:32	29.8
MarkW	2018-05-25 11:41:35	36.4
chumah	2018-05-25 11:46:42	30.7
James	2018-05-25 12:06:10	47.6
Margaret	2018-05-25 16:06:37	21.3
Eric	2018-05-25 19:26:24	54.2
Wanja	2018-05-25 20:01:00	23.6
Teresia	2018-05-25 20:07:14	49.3

Figure 19: Professional Scores GUI

Source: Researcher (2018)

4.8.6 Recommendations Component

Based on the user or professional assessments, this module suggests a number of recommendations necessary to mitigate threats resulting from use of smart mobile devices. A recommendation was assigned to each assessment question as a security requirement as shown in table 4.22 below.

Table 4.22: Assessment Questions with Recommendations

Number	Assessment Question	Recommendation
1.	The university has an ICT security policy which is implemented and enforced	Information Security Policy should provide the guiding principles and responsibilities necessary to safeguard the security of the University’s information systems.
2.	I have read and clearly understood the university security policy	Users should be aware of Information Security Policy; the policy should be readable and understandable and should be enforced within the organization to all users.
3.	The university security policy permits use of personally-owned devices	Smart mobile devices face the risk of loss, theft or being exploited by malicious users. Having a Mobile Device Policy will help to protect the University network and information systems.
4.	The university security policy requires all smart mobile devices to have an approved operating system	Mobile Operating Systems manage cellular and wireless network connectivity as well as phone access
5.	The university security policy requires all smart mobile devices to have latest security patches and upgrades	Security patches are software issued by a company whenever a security flaw is uncovered. They are important in fixing discovered security vulnerabilities.
6.	My smart mobile device characteristics are registered in the university database	The university should have asset management system to help keep track of all the assets used by all stakeholders to enable asset recovery in case of loss or theft.

7.	The security policy clearly specifies penalties for unauthorized use of smart mobile devices	It is important for the university to monitor internet usage in order to detect activities that may negatively impact on the university reputation
8.	The university security policy prohibits leaving smart mobile device unattended when attached to a corporate computer	Smart mobile devices should be disconnected from corporate computers when not in use to prevent hackers from infiltrating to more valuable targets like user’s computers and corporate databases
9.	The university insures smart mobile devices against loss, theft, or damage	The university should insure all the assets to enable data recovery in the event of device loss or damage
10.	The university security policy outlines reporting procedures for lost, stolen, or damaged smart mobile devices	The university security policy should clearly outline incident reporting procedures in case of device loss or theft to enable speedy recovery of the lost device.
11.	The university maintains a secured inventory of all smart mobile devices.	An asset inventory should be maintained within the university database to uniquely identify the asset in case it is lost or stolen.
12.	My smart mobile device can be locked or its password can be changed if lost or stolen	Smart mobile devices should be locked with a passcode when not being used or when left idle for a long time to prevent loss of private information stored on the device.
13.	The university security policy outlines reporting procedures for compromised smart mobile devices	When a smart device is compromised, the university security policy should clearly outline the reporting procedures to prevent spread to other devices

14.	My smart mobile device undergoes authentication process before connecting to the university network	Authentication process is a way of confirming that a device has been pre-approved by the university ICT department to connect to the corporate network.
15.	All smart mobile devices within the university network are monitored for unauthorized activities	Network monitoring should be done to optimize data flow by assessing activities such as bandwidth utilization and applications being accessed.
16.	My smart mobile device has enabled manufacturers debugging features	Enabling manufacturer's debugging features enables the mobile device receive updates from the manufacturer regarding new security patches
17.	My smart mobile device has a unique name and password which is not known by anyone else	Smart mobile devices should have unique username and other credentials to enable only authorized users have access to the device
18.	There are security practices in place to guide users in selecting and maintaining secure passwords	Users should be trained on how to select strong and secure passwords that are not easy to guess and to regularly change the passwords
19.	I always disable or protect remote access to my smart mobile device whenever connected to the network	Smart mobile devices should be protected from remote access when connected to university network to prevent sensitive information from being leaked to unauthorized users.
20.	Allocation and reallocation of passwords is controlled through a formal management process	Allocation and reallocation of passwords should be a regular process which should be controlled by the university ICT department

21.	My smart mobile device is checked for identified security requirements before being granted access to the organization's information or assets	Before granting access to corporate information or assets, mobile devices should be checked to confirm if they have installed updated antivirus
22.	My smart mobile device has multiple authentication mechanisms eg Password, Fingerprint, on-screen pattern etc	Multiple authentication mechanism is a method of confirming a user's claimed identity in which a user is granted access only after successfully presenting 2 or more pieces of evidence (or factors) to an authentication mechanism
23.	Access control policy is developed and reviewed based on the university security requirements	Access control policy should be used to determine the allowed activities to authorized users. Access to corporate information is granted after a successful user authentication
24.	My smart mobile device contain both personal and corporate data	Both personal and corporate data contained in smart mobile devices should be protected from risk of exposure and data loss through use of appropriate security controls such as passwords
25.	My smart mobile device is automatically examined for compliance with the university security policy once I connect to its network	Smart mobile devices must be examined to ensure that the device is not compromised in any way and that all communications is secure
26.	The university security policy specifies the types of information that can and cannot be stored, processed, and transferred on smart	Users should be trained on the type of information that can be stored, processed and transferred through smart mobile devices to reduce the risk of

	mobile devices	information loss and data leakage
27.	The security policy outlines approved Modes of Operation: wired and wireless	The university security policy should specify the modes of operation whether wired or wireless and the risks associated with each mode
28.	I regularly synchronize my smart mobile device with organizational computer or network, for backup purposes	Users of smart mobile devices should regularly synchronize their devices to enable perform backup
29.	My smart mobile devices is assigned a unique Internet Protocol (IP) address each time I connect to the university network	Internet Protocol address should be used as an interface identification for a network of machines. This is also used to provide the location of that device
30.	My smart mobile device contain an updated antivirus software that scans files as they are opened	An updated antivirus software contains controls of the latest vulnerabilities that will protect the smart mobile device from the current threats
31.	My smart mobile device has some unapproved software and applications	Users should avoid installation of unapproved applications to their smart mobile devices to protect the device from malware attack
32.	My smart mobile device is updated and configured to install new updates whenever available	Smart mobile devices should be configured to automatically obtain new updates whenever available which contains latest files needed to combat new viruses
33.	When downloading applications, I always use the official downloading sites	Applications should always be downloaded from official site to protect the device from malware that exploit system vulnerabilities

34.	Smart mobile device is not used to store, process, or transfer sensitive, proprietary, or classified data, unless encryption is used	Encryption provides end to end data security for data being transmitted across network
35.	The university security policy prohibits use of public or untrusted network access points	Users should avoid connecting to public or untrusted network access points since they are highly insecure due to data being emitted through airwaves.
36.	The university security policy provides protective measures against social engineering and other security attacks	The university security policy should provide guidelines on how to securely use e-mails including clicking to suspicious links sent through e-mails
37.	The university security policy does not allow smart mobile devices to be simultaneously connected to other devices while connected to university computer or network	Smart mobile devices should not be connected simultaneously to other devices while connected to university computer or network to prevent spread of viruses in case one device is infected
38.	The university security policy require all smart mobile devices to use a password to synchronize to an organizational computer or network	To synchronize to the university network or computer it is necessary to use password to ensure that only authorized and legitimate users are granted access to the network
39.	Updated signatures are installed on my smart mobile device each time they synchronize to a university computer or at regular intervals via a secure network connection	Smart mobile devices should have updated signatures installed whenever they synchronize to the university computer or network to prevent attack of a new virus attack or a variant of the previous one
40.	The university implements encryption to protect information on smart mobile devices	Data stored in smart mobile devices should be encrypted which translates data into another form, or code, so that

		only people with access to a secret key
41.	The university implements a firewall on smart mobile devices	A firewall is software or firmware that enforces a set of rules about what data packets will be allowed to enter or leave a network. Firewalls are incorporated into a wide variety of networked devices to filter traffic and lower the risk that malicious packets traveling over the public internet can impact the security of a private network
42.	The university implements VPN software for smart mobile devices, for remote network connections	A virtual private network (VPN) is a technology that creates a safe and encrypted connection over a less secure network, such as the internet. VPN technology was developed as a way to allow remote users and branch offices to securely access corporate applications and other resources. To ensure safety, data travels through secure tunnels and VPN users must use authentication methods -- including passwords, tokens and other unique identification methods -- to gain access to the VPN.
43.	Unneeded network connections within the university network are disabled	Unneeded network connections should be disabled to prevent computer break-ins which occur as a result of people taking advantage of security holes or problems with these programs. The more services that are running on your computer, the more opportunities there

		are for others to use them, break into or take control of your computer through them
44.	Unneeded applications and services within the university network are disabled	Unneeded applications should be disabled to reduce the risk of attack. Attack surfaces should be reduced to the absolute minimum.
45.	I always connect my smart mobile device to free public Wi-Fi whenever available	Data sent through public Wi-Fi can easily be intercepted, smart mobile devices risk the security of their personal information, digital identity. Smart mobile devices should be protected by an effective security and anti-malware to reduce the risks

This module filters the recommendations for all the questions whose user assessment scores goes below the threshold and allows the user to download the recommendations in printable document format (pdf). The figures 20 and 21 shows logic flowchart and GUI presentations respectively.

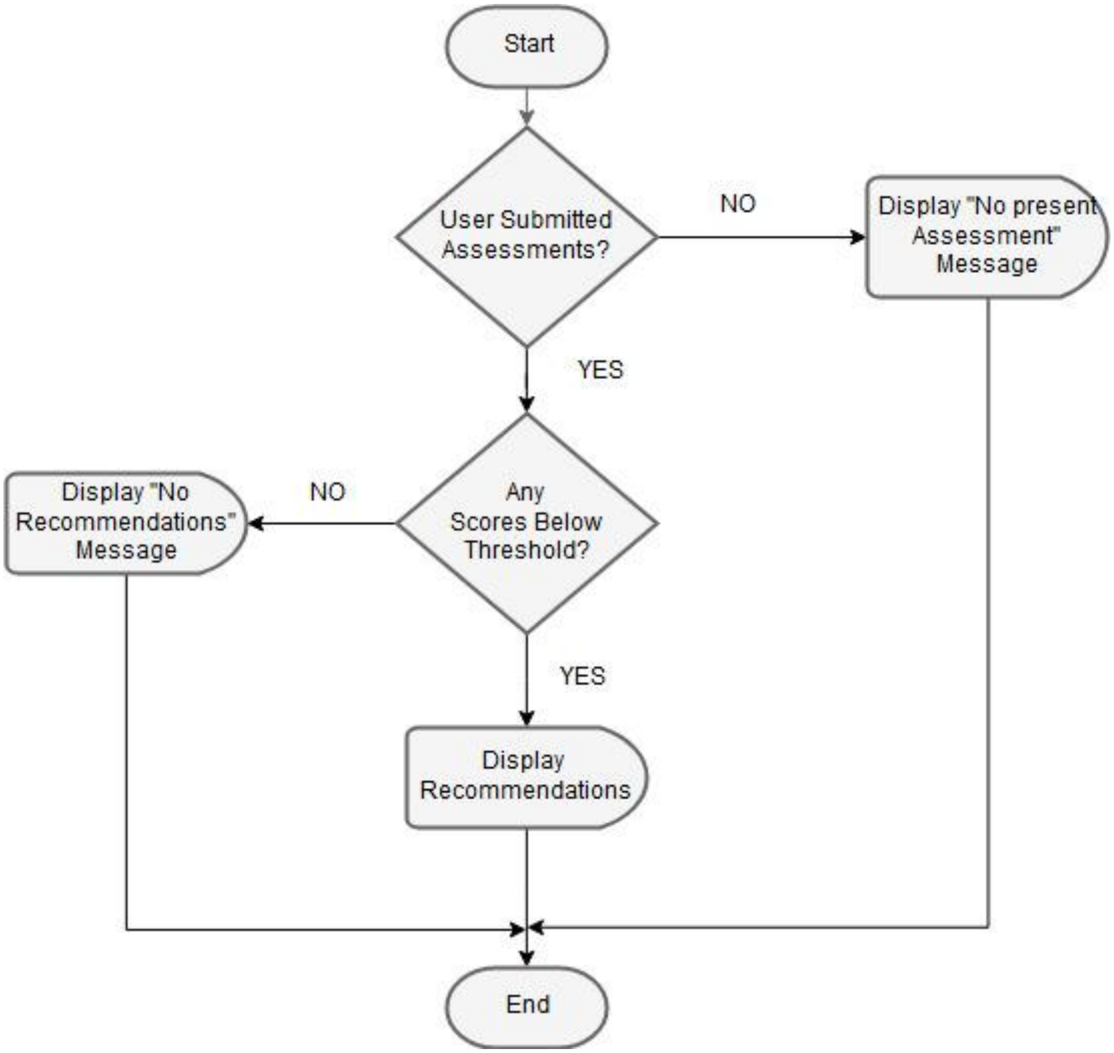
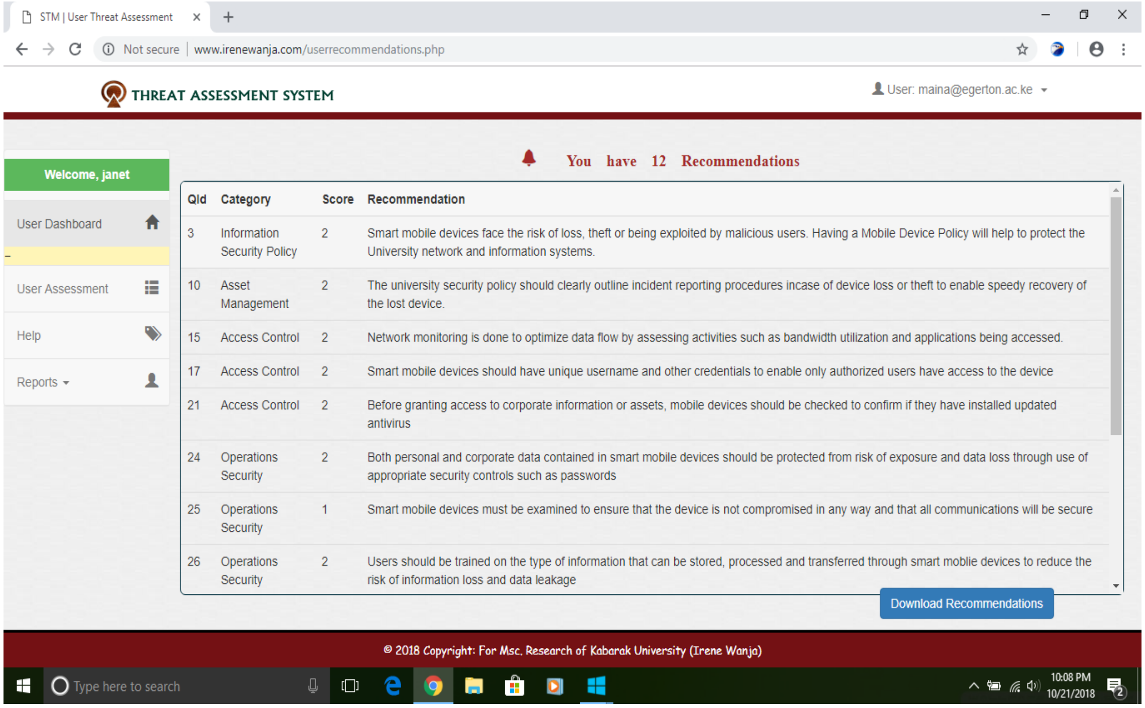

Start
User Submitted Assessments?
NO
Display "No present Assessment" Message
YES
Display "No Recommendations" Message
NO
Any Scores Below Threshold?
YES
Display Recommendations
End

Figure 20: Recommendations Flowchart

Source: Researcher (2018)



You have 12 Recommendations

QId	Category	Score	Recommendation
3	Information Security Policy	2	Smart mobile devices face the risk of loss, theft or being exploited by malicious users. Having a Mobile Device Policy will help to protect the University network and information systems.
10	Asset Management	2	The university security policy should clearly outline incident reporting procedures incase of device loss or theft to enable speedy recovery of the lost device.
15	Access Control	2	Network monitoring is done to optimize data flow by assessing activities such as bandwidth utilization and applications being accessed.
17	Access Control	2	Smart mobile devices should have unique username and other credentials to enable only authorized users have access to the device
21	Access Control	2	Before granting access to corporate information or assets, mobile devices should be checked to confirm if they have installed updated antivirus
24	Operations Security	2	Both personal and corporate data contained in smart mobile devices should be protected from risk of exposure and data loss through use of appropriate security controls such as passwords
25	Operations Security	1	Smart mobile devices must be examined to ensure that the device is not compromised in any way and that all communications will be secure
26	Operations Security	2	Users should be trained on the type of information that can be stored, processed and transferred through smart moblie devices to reduce the risk of information loss and data leakage

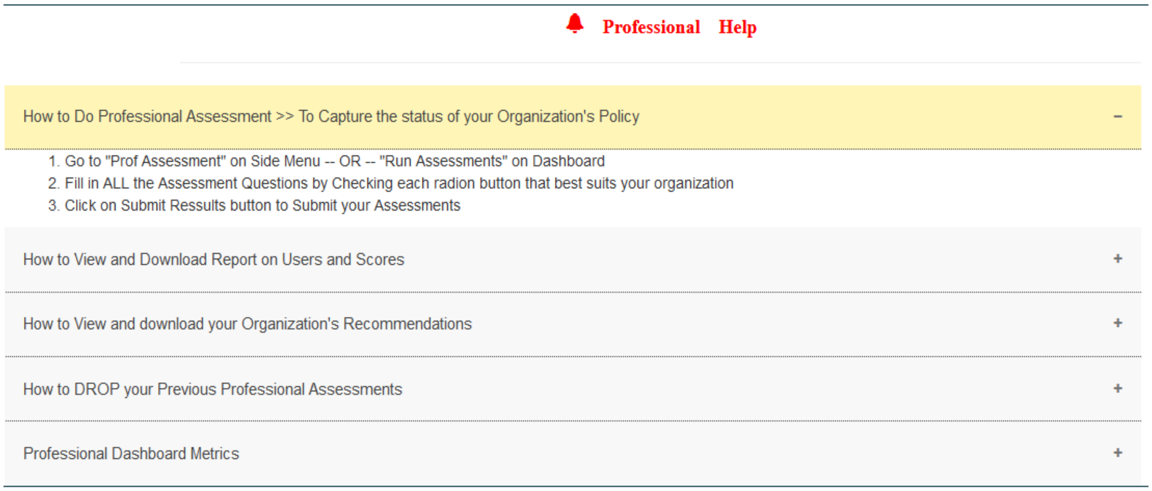
© 2018 Copyright: For Msc. Research of Kabarak University (Irene Wanja)

Figure 21: Recommendations GUI

Source: Researcher (2018)

4.8.7 Help Module

This module acts as a user guide to direct users on how to carry out various activities within the TM system. Guidelines are enumerated in a readable and easy to understand formats in the help module. Figure 22 and 23 below presents a Graphical layout of the help interface for both professionals and users respectively.



Professional Help

How to Do Professional Assessment >> To Capture the status of your Organization's Policy –

1. Go to "Prof Assessment" on Side Menu -- OR -- "Run Assessments" on Dashboard
2. Fill in ALL the Assessment Questions by Checking each radion button that best suits your organization
3. Click on Submit Ressults button to Submit your Assessments

How to View and Download Report on Users and Scores +

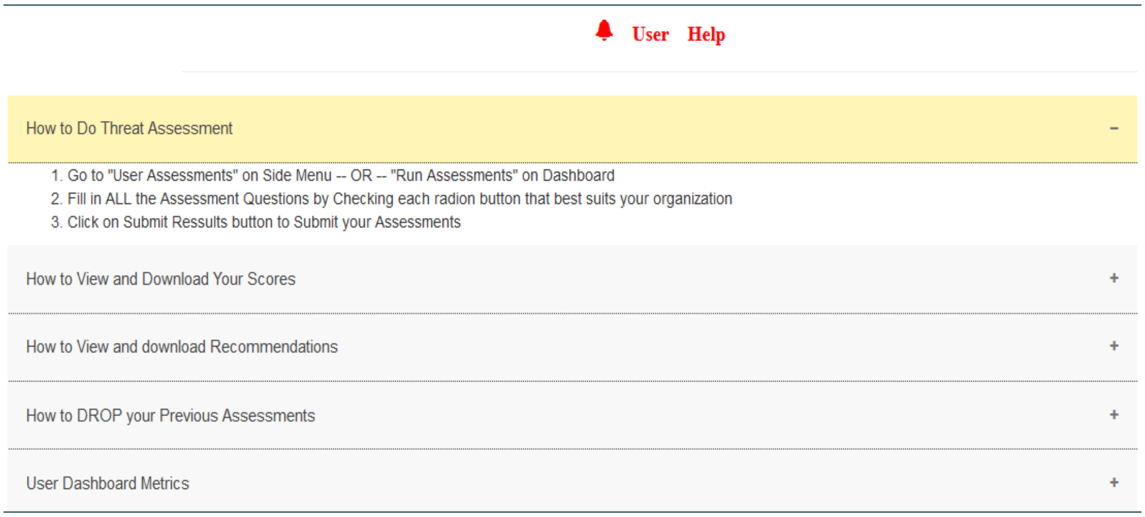
How to View and download your Organization's Recommendations +

How to DROP your Previous Professional Assessments +

Professional Dashboard Metrics +

Figure 22: Professional Help

Source: Researcher (2018)



User Help

How to Do Threat Assessment −

1. Go to "User Assessments" on Side Menu -- OR -- "Run Assessments" on Dashboard
2. Fill in ALL the Assessment Questions by Checking each radion button that best suits your organization
3. Click on Submit Ressults button to Submit your Assessments

How to View and Download Your Scores +

How to View and download Recommendations +

How to DROP your Previous Assessments +

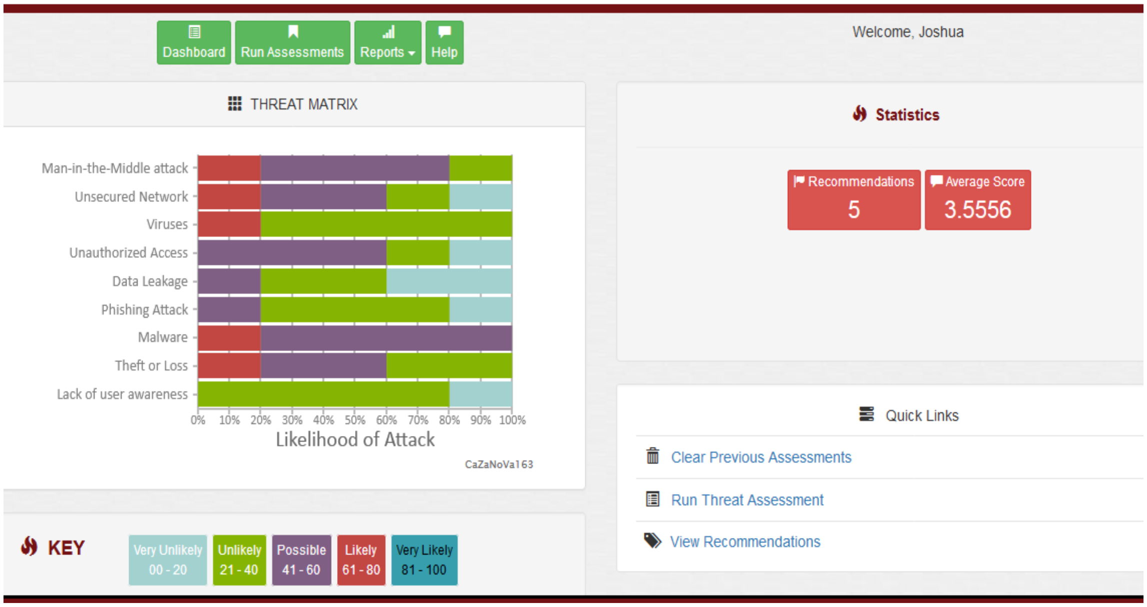
User Dashboard Metrics +

Figure 23: User Help GUI

Source: Researcher (2018)

4.8.8 User Home Page

This is the first page that appears when the user logs into the TM system. It contains navigation links that allow users to perform other system functionalities such as clear previous assessment, run new threat assessment, view reports which include recommendation and user's average scores. This module also contains the threat matrix in a graphical form which shows the likelihood of attack from various threats using different color codes. This is useful in determining the likelihood of attack by different threats as a result of increased use of smart mobile devices. Figure 24 below shows graphical representation of user home page.



Recommendations 5

Average Score 3.5556

Figure 24: User Home Page GUI

Source: Researcher (2018)

4.8.9 Professionals Home Page

This is the first page the ICT professionals view when they login to the system which in this context is referred to as the professional dashboard. The page displays a graphical representation of the overall status of the likelihood of attack obtained from the various threat assessments as submitted by various users (staff and students). It also contains navigation links which allow professionals to perform system activities, such as; to clear previous professional assessments, to run professional assessment, and to view organization's recommendations. Besides, the dashboard displays various statistics such as the number of users who have submitted their assessment, the average score based on all the submitted scores, and the overall likelihood of attack. Figure 25 presents a graphical user interface layout of the professional dashboard.

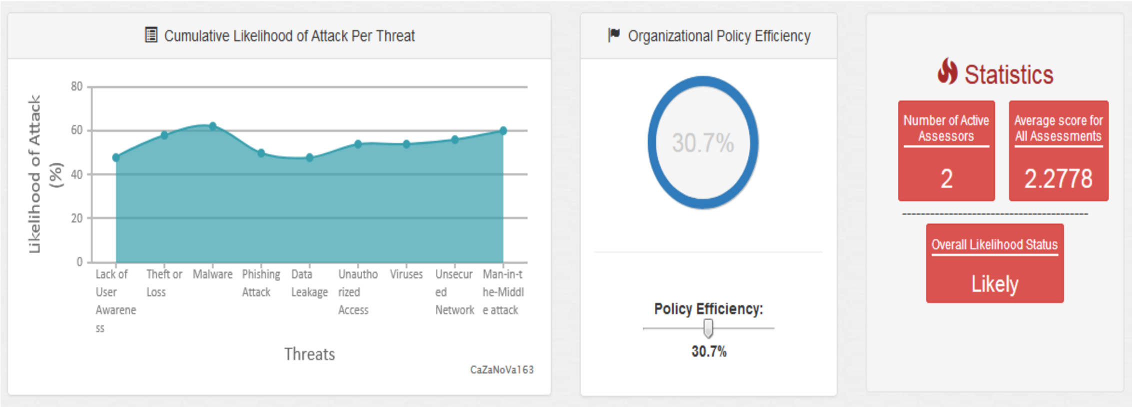


Figure 25: Professional Home Page GUI

Source: Researcher (2018)

4.8.10 Entity Relationship Diagram

TM entity relationship diagram is presented in figure 26 below. It contains 5 database tables used to store different types of information as indicated.

a) User registration and authentication information: user_id, user_name, email, password (using SHA256 cryptographic hash), organization and user_category.

b) User_Questions information: question_id, category, question, associated_threat and recommendations.

c) Professional_Questions information: question_id, category, question, associated_threat and recommendations

d) User_assessment information: user_id, question_id, assessment_date, score and threat.

e) Professional_assessment information: user_id, question_id, assessment_date, score and threat

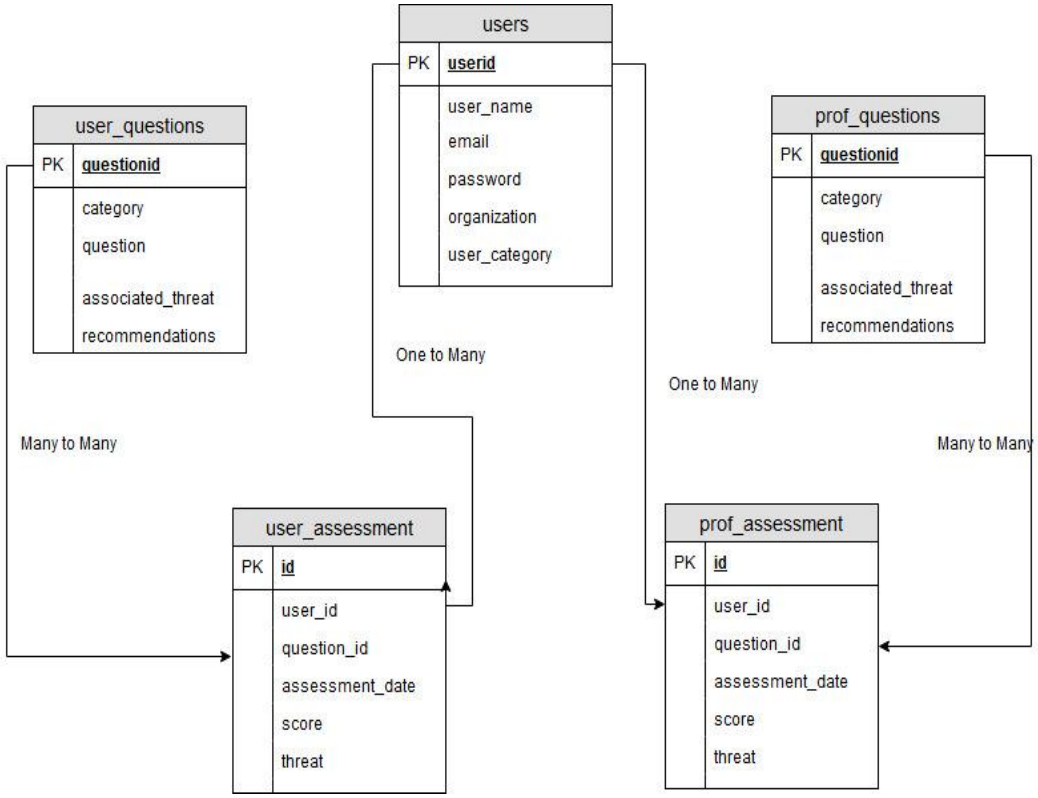


Figure 26: Entity Relationship Diagram

Source: Researcher (2018)

4.8.11 Proof of Concept

The TM system prototype was developed as a proof of concept using MySQL as the database engine and PHP as server side-scripting language. Bootstrap 4 which is a framework of CSS was used to style user interface for the purpose of user interaction with the system. phpStorm was used as program editor to write and test the code. Apache web server assisted in running the application locally. The application was later deployed online and is accessible through www.irenewanja.com

4.9 System Evaluation

Goal-based evaluation technique was used to test the prototype to determine if the designed model would achieve the preset objectives. The evaluation is presented in table 4.23 below;

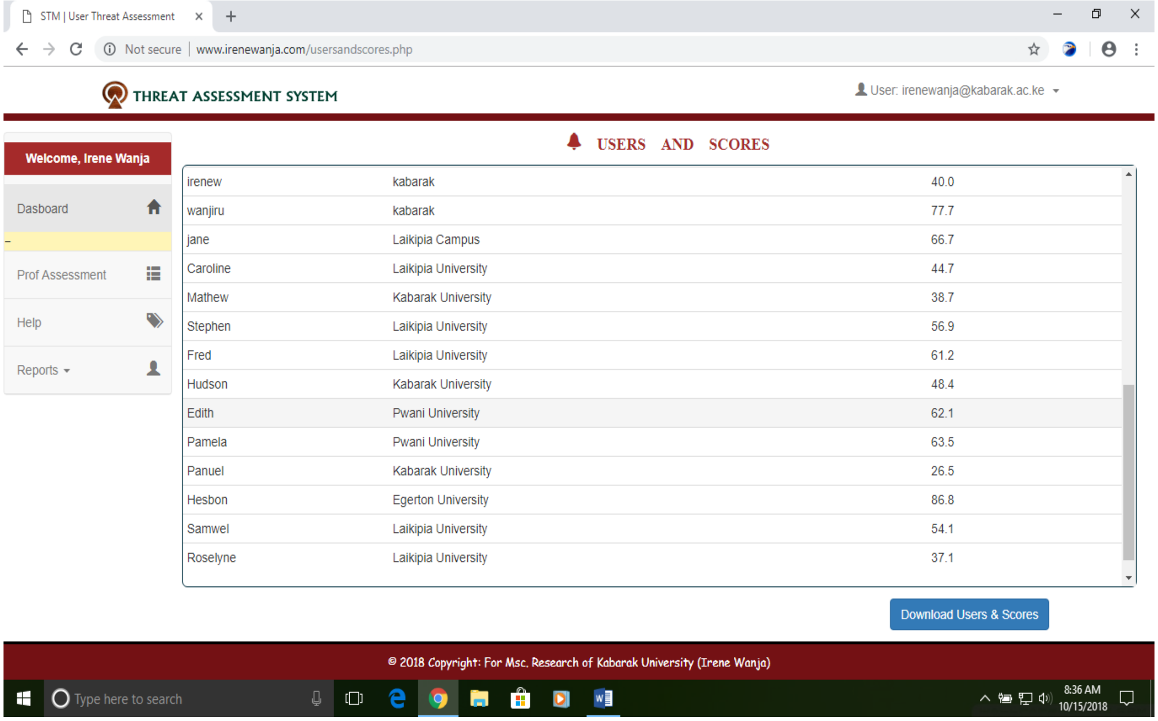
Table 4.23: Goal-Based Evaluation

	Objective	Evaluation Results
1.	**User registration:** the purpose of this was to capture user personal details which were to be stored in the database and to validate user input for the subsequent logins. This was also to ensure that the password supplied in plaintext is hashed into cipher text.	**a)** The prototype accepted user details validated the user input such as the standard e-mail format and the length of password for complexity. **b)** The prototype applied SHA256 to hash the password from plaintext to cipher text. **c)** The prototype successfully stored the supplied user details into the database.
2.	**User Authentication:** to allow authorized users to access the system, the prototype was expected to prompt users to provide their login details.	**a)** The prototype directed users to provide their login details to compare with what was stored in the database. **b)** The prototype further denied access to users whose details did not match what was stored in the database.
3.	**Threat Assessment and Submission:** The prototype was expected to display all the questions that had been designed to assess security status whereby users were supposed to select their most suitable answer using the provided Likert scale. On completion and submission, the prototype was expected to store the results in the database,	**a)** The prototype successfully retrieved threat assessment questions with a scale of 1 to 5 for users to make their choice **b)** The submitted assessments were securely stored in the database.
4.	**Likelihood of Attack Computation:** It was expected	**a)** The prototype was able to retrieve the scores from the database and to compute

	that the prototype would compute the likelihood of attack using the scores earned from the submitted assessment and display the results in a graphical format.	the results to determine the likelihood of attack. **b)** Using JQUERY, the prototype was able to provide a graph showing different levels of likelihood of attack from various threats using different color codes.
5	**Average Scores and Recommendations:** From the submitted assessment, the prototype was expected to compare the scores with preset threshold to determine the recommendations that would be suggested for the user. These recommendations were expected to be in printable and portable format.	**a)** The prototype successfully retrieved the scores that were below the set threshold and were used to display the suggested recommendations. **b)** The prototype was able to display the recommendations in a printable and portable format.

4.10 Verification and Evaluation of the Model

The designed TM model was hosted with domain registrar. The model allowed users to register as new users and stored their personal details into the database. This information was later used to verify user details each time they logged in to the system. The correct match of username and password allowed user to access the system. The SHA256 hash algorithm successfully hashed user passwords provided in plaintext into cipher text to enhance security. Each successful user login was marked with different timestamps which was used to distinguish the various threat assessments the user performed. The application was later deployed online and is accessible through www.irenewanja.com. Users from different universities were requested to register and run the assessment in order to validate the matrix. The system successfully computed the likelihood of attack through the scores obtained after running threat assessment. This was presented in percentage against each username. The figure 27 below represents verification and evaluation of the matrix.



irenew	kabarak	40.0
wanjiru	kabarak	77.7
jane	Laikipia Campus	66.7
Caroline	Laikipia University	44.7
Mathew	Kabarak University	38.7
Stephen	Laikipia University	56.9
Fred	Laikipia University	61.2
Hudson	Kabarak University	48.4
Edith	Pwani University	62.1
Pamela	Pwani University	63.5
Panuel	Kabarak University	26.5
Hesbon	Egerton University	86.8
Samwel	Laikipia University	54.1
Roselyne	Laikipia University	37.1

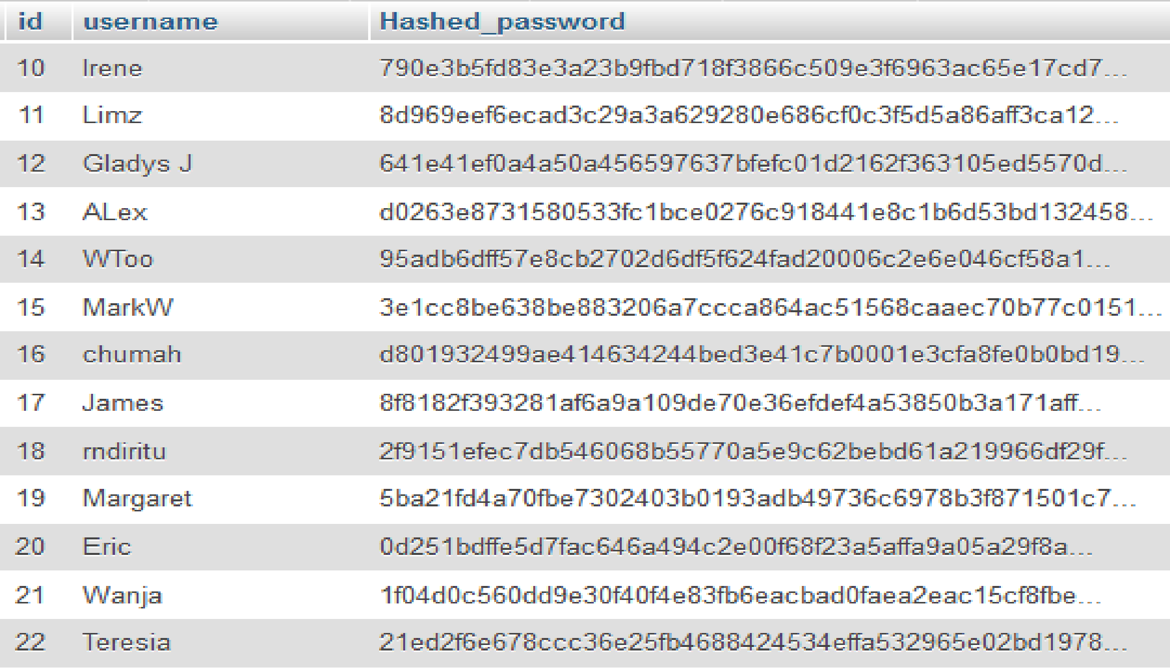
© 2018 Copyright: For Msc. Research of Kabarak University (Irene Wanja)

Figure 27: Model Verification Evaluation

Source: Researcher (2018)

4.11 TM System Security

TM System was designed with security in mind. The user must login before performing any system functions and where they are not registered they are prompted to register. Security is also assured through use of form validation constraints to enform valid emails and ensure passwords complexity is observed. At the database level, complex passwords submitted to the database are encrypted using SHA256 hashing to ensure they are not readable to persons who have access to the database. The figure 28 below shows a graphical presentation of a section of the user database depicting how passwords are encrypted using SHA256.



id	username	Hashed_password
10	Irene	790e3b5fd83e3a23b9fbd718f3866c509e3f6963ac65e17cd7...
11	Limz	8d969eef6ecad3c29a3a629280e686cf0c3f5d5a86aff3ca12...
12	Gladys J	641e41ef0a4a50a456597637bfefc01d2162f363105ed5570d...
13	ALex	d0263e8731580533fc1bce0276c918441e8c1b6d53bd132458...
14	WToo	95adb6dff57e8cb2702d6df5f624fad20006c2e6e046cf58a1...
15	MarkW	3e1cc8be638be883206a7ccca864ac51568caaec70b77c0151...
16	chumah	d801932499ae414634244bed3e41c7b0001e3cfa8fe0b0bd19...
17	James	8f8182f393281af6a9a109de70e36efdef4a53850b3a171aff...
18	rndiritu	2f9151efec7db546068b55770a5e9c62bebd61a219966df29f...
19	Margaret	5ba21fd4a70fbe7302403b0193adb49736c6978b3f871501c7...
20	Eric	0d251bdffe5d7fac646a494c2e00f68f23a5affa9a05a29f8a...
21	Wanja	1f04d0c560dd9e30f40f4e83fb6eacbad0faea2eac15cf8fbe...
22	Teresia	21ed2f6e678ccc36e25fb4688424534effa532965e02bd1978...

Figure 28: TM Model Security

Source: Researcher (2018)

4.12 TM System Scalability

The developed Threat Matrix can be used in any other organization although the scope of study was within Egerton University. This is because the threat assessment questions used are not limited to the area of study only but can be expanded to assess other types of threats to suit any other organization. The system being a web-based model can be accessed through web browser such as Chrome and Mozilla using any smart mobile device whether laptop, desktop or mobile phone with internet connections.

Likelihood of Attack =5.233 + (-0.084*Information Security Policy) + **(**0.199*Asset Management) + (-0.003*Access Control) + (-0.101*Operations Security) + (-0.530*Communications Security) + 0.335.

The following SQL code was used to compute likelihood of attack:

```
$sql = “SELECT ROUND(100*((5.233+SUM(b.weight*a.userscore)+0.335)/
(5.233+SUM(b.weight*5)+0.335),1) FROM userassessments  a  INNER JOIN
userquestions  b  ON a.questionid=b.questionid INNER JOIN users c ON
a.userid=c.id”;
```

The code gets the sum of all the assessment questions then divides the sum by the product of the number of questions and the highest possible score (5), the result is later converted to percentage then rounded off to one decimal point as per user who run the assessment.

CHAPTER FIVE
SUMMARY, CONCLUSIONS AND RECOMMENDATIONS

5.1 Introduction

This chapter summarized the findings of the research. It focused on the achievements of the research objectives, the recommendations from the web-based model and areas of future study.

5.2 Summary

The main objective of this research was to evaluate security threats brought about by use of smart mobile devices when connected to the university network. Although the university has implemented and enforced ICT security policy in which countermeasures are already put in place, new security challenges continue to emerge. Among these challenges are threats created as a result of use of smart mobile devices. The study sought to assess security threats introduce to the university information systems and data through use of smart mobile devices. A Threat Matrix which was a web-based model was developed to show levels of likelihood of attack for various threats that were found to be common. This assisted in determining the security gap that needed to be addressed to enhance security of the university network. The matrix also provided recommendations on security requirements that were needed to improve the security status of the university network.

5.3 Conclusions

This study aimed at analyzing security exposure of the university network to risks associated with connected smart mobile devices. Implementation of ICT security policy is supposed to address these challenges but new threats continue to emerge as more smart mobile devices are connected to the network. This study developed a threat matrix that displays various levels of likelihood of attack able to notify ICT security experts on the efficiency of the enforced security policy and areas that need improved countermeasures. This will also sensitize users of smart mobile devices on how to securely operate their devices without compromising their information as well as that of the university.

The section below discusses specifics objectives as achieved;

a) What is the New Security Threats Introduced through Use of Smart Mobile Devices Connected to University Network?

While the university permits use of personally-owned devices, the study found out that most of the users of smart mobile devices are not aware of the security risks posed by these devices to the university network. The university data and other information face the risk of being accessed by other unauthorized people through smart mobile devices that contain both personal and corporate data in the event that the device is lost or stolen. The study discovered that most of the devices are not installed with anti-viruses or are not updated with the latest security patches; this exposes the university to virus and malware attack when the device is connected to the university network. The study established that there is need to create awareness to users through training on how to securely operate their smart mobile devices and especially when connected to the university network and other public networks.

b) How Can a Threat Matrix be developed to Show the Likelihood of Attack in the University Network?

After establishing that the enforced security policy was not sufficient to safeguard the university network from threats emanated from use of smart mobile devices, the study developed a Threat Matrix (TM). This is a web-based model which showed cumulative likelihood of security threats attack as assessed from various users of the smart mobile devices. This was then compared with the already implemented countermeasures as assessed from ICT professionals to determine how effective the mitigations were and hence the efficiency of ICT security policy.

c) What is Security Requirements Needed to Enhance Security of the University LAN ecosystem?

The study established some security gap between threats that were likely to attack the university network and the already implemented countermeasures. As a way of protecting corporate data and information systems, the developed model provided some recommendations on what was required to be done to enhance security status of the university network as well as smart mobile devices. This was reported as security requirements that both the ICT professionals and users of smart mobile devices were supposed to adopt.

d) How Can the Developed Matrix Compute the Likelihood of Threat Attack?

After developing threat matrix, users were requested to register and login to access system functionalities. They were then able to run assessment questions and submit to the database. The system then computed the likelihood of attack and displayed the result on user dashboard where each threat had various levels of likelihood based on the submitted assessment. The matrix also displayed various recommendations for the questions that were below threshold of 3 from a scale of 5.

5.4 Recommendations

Smart mobile devices are generally exposed to more threats than client devices which are connected to the network. For an organization to develop security solutions against threats that occur through use of smart mobile devices, this study recommend development of system threat models to identify security requirements and specify resources accessed through these devices. University ICT security policy should also be reviewed regularly to address the new threats introduced in the network and as guided by ISO 27001 security guidelines. The university should regularly perform vulnerability scan and penetration test on network and applications to test the security of information systems regularly. Regular audits should be performed to assess compliance with security policies and standards. Analyzing information obtained from these exercises will determine the security controls that need to be put in place or need to be improved.

5.4.1 Recommended Security Requirement

Universities should design and enforce a security policy for smart mobile devices. This will among other things define the type of the organization’s resources to be accessed through smart mobile devices, the type of smart mobile devices to be permitted to access the organization's resources, the degree of access that various categories of smart mobile devices (organization-owned or personally-owned) may have.

The university should also have a centralized smart mobile device management server where applications such as the developed Threat Matrix (TM), Mobile Device Management (MDM) and Network Access Control (NAC) are installed and regularly managed. This will ensure that all smart mobile devices connected to the university network are monitored and maintained accordingly.

While connecting smart mobile devices to university network the user should ensure that:

1) The smart mobile device has a legitimate operating system operating systems that meets the defined minimum standards hence the university should not allow use of jail broken devices.
2) Network authentication should be subject to the University's requirements, whether wireless or wired connection, and authentication via an SSL VPN for remote access to the network.
3) The smart mobile device should support multiple security level such as use of password, pattern of biometric features to control access of information stored on the device. The user should also enable automatic lock whenever the device is left idle for certain period of time.
4) Smart mobile devices should have appropriate anti-virus and antispyware installed which should be updated regularly
5) If the smart mobile device is lost or stolen, the user should report immediately to the relevant office for the next course of action.
6) Any corporate information stored in the smart mobile device should be removed before the device is disposed or sold out.
7) Any applications installed in the smart mobile device should be downloaded from official site to prevent malware infection.
8) To ensure security of the university data, the university should adopt security solutions such as Mobile Device Management (MDM) and Network Access Control (NAC) to enforce certain policies on smart mobile devices such as remote wipe if the device is lost or stolen.

9) The users of smart mobile devices should agree to surrender some limited authority over the device in order to protect university data and access on the device.
10) The university should reserve the right to push and remove university data from user's device to enhance its security and manageability.
11) The user should acknowledge that the university should directly or remotely change security configurations of the device to protect university data and software installed on the device. These changes include among others;
    (a) Decline to register a device that fails to meet minimum security requirements as stated above
    (b) Configure certain security settings
    (c) Prevent user from changing certain security settings
    (d) Apply login code with acceptable level of complexity to enhance access control
    (e) Automatically lock the device after inactive timeout period
    (f) Installing software and digital certificates that are necessary to maintain security
    (g) Encrypting data that is stored on the device and on transit.
    (h) Automatically wiping the university data from the device after a certain number of failed login attempts
    (i) Denial of access to university systems, information and data if security configurations required for proper use the device are removed.
12) The users should acknowledge that any University data stored on their smart mobile devices remains the sole property of the University and that they have an obligation to protect the security of the data.
13) The users should acknowledge that the University has a right to inspect University data held on their personal smart mobile devices.
14) The users should understand that the University may remotely monitor their smart mobile device to ensure security and software configurations are maintained.
15) The users may not be prevented from installing the software or applications of their choice on their smart mobile device. However, the University may block

your access to University information systems if any software/applications/data present a threat to University information or data

16) The University is not liable to nay costs incurred by users through use of their personal smart mobile devices. The University should not reimburse any voice or data charges, software or application acquisition fees, and support or insurance costs associated with user's device.
17) The users have sole responsibility for ensuring no other person has access to University software or data stored on their smart mobile device.
18) The University should not monitor the web browser history on user's smart mobile device when not connected to University network(s), unless the web traffic is directed through the University's network infrastructure.
19) The University may restrict access to internet websites, services or other elements for operational or policy reasons while user's smart mobile device is connected to University networks including either wireless or cabled connections.
20) The University may monitor use of smart mobile device while connected to the University network. This information may be collected and archived and may be subject to public access.

Wiping personal data from user's smart mobile device should be in accordance with the following circumstances:

(a) Your smart mobile device is reported as being lost/stolen
(b) You cease employment/contract or studies with the University
(c) There is a suspected security breach, examples include but are not limited to, modification of the device's operating system, breaching University policies, or detection of viruses or malware on the device.
(d) The University may lock your device to prevent access to University information or data.
(e) Preventing your device from connecting to University ICT services.
(f) Applying either a full or selective wipe of your smart mobile device.

5.5 Suggestions for Further Research

From the developed model, there are areas that need further improvement as describe in section 5.5.1 to 5.5.3 below;

5.5.1 User Authenticity

From the developed model, it is difficult to distinguish between authentic users from other users, this is because the system cannot verify the personal details provided when the user is registering into the system. To improve this, the system should be interconnected with the university databases containing records of students and staff and other stakeholders to verify their details when registering.

5.5.2 Enhancing TM Efficiency

To enhance performance of Threat Matrix, the system needs to be integrated with other ways of managing smart mobile devices such as device management (MDM) system and Bring-Your-Own-Device (BYOD) policy. MDM will optimize the functionality and security of smart mobile devices within the university while simultaneously protecting the university network. BYOD on the other hand provides guidelines to users of smart mobile devices and ICT security experts on how to securely operate these devices.

5.5.3 Likelihood of Attack versus Impact Assessment

The main purpose of the developed Threat Matrix was to determine the possibility of threat attack to the university network. To advance the system operations, further research on how to compute the impact created by the threat in the event that it succeeds in launching the attack. This would help the university ICT security experts to prioritize on the risks that have high impact while employing the countermeasures.

REFERENCES

Abdelrahman, O. H., Gelenbe, E., Görbil, G. & Oklander, B. (2013). Mobile network anomaly detection and mitigation: The NEMESYS approach. In *Information Sciences and Systems 2013* (429-438). Springer, Cham.

Abomhara, M. & Køien, G. M. (2014). Security and privacy in the Internet of Things: Current status and open issues. In *Privacy and Security in Systems (PRISMS), 2014 International Conference on* (1-8). IEEE.

Arabo, A. & Pranggono, B. (2013) malware and smart device security: Trends, challenges and solutions. In *Control Systems and Computer Science (CSCS), 2013 19th International Conference on* (pp. 526-531). IEEE.

Aware, W. T. A., Documentation, T. P. S. & Logical, C. (2005). *Information technology–Security techniques–Information security management systems–Requirements.*

Babar, S., Stango, A., Prasad, N., Sen, J. & Prasad, R. (2011). Proposed embedded security framework for internet of things (iot). In *Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronics Systems Technology (Wireless VITAE), 2011 2nd International Conference on* (pp. 1-5). IEEE.

Barcelo, Y. (2011). Insecurity. *CA Magazine*, pp. 36-38.

Beach, A., Gartrell, M. & Han, R. (2009). Solutions to security and privacy issues in social networking. In *Computational Science and Engineering, 2009. CSE'09. International Conference on*, 4, (1036-1042). IEEE.

Bernabe, J. B., Hernández, J. L., Moreno, M. V. & Gomez, A. F. S. (2014). Privacy-preserving security framework for a social-aware internet of things. In *International Conference on Ubiquitous Computing and Ambient Intelligence* (pp. 408-415). Springer International Publishing.

Bosworth, S., Kabay, M. & Whyne, E. (2009). Physical Threats to the Information Infrastructure. In F. Platt, *Computer Security Handbook.* New York: John Wiley & Sons Inc.

Calder, A. & Watkins, S. (2008). *IT Governance: A Manager's guide to Data Security and ISO27001/ISO 27002, 4th Edition*. London: Kogan Page Limited.

Cisco.com (2014). *Cyber Threat Management from the Boardroom Risk*: Retrieved from blogs.cisco.com: https://blogs.cisco.com/security/cyber-threat-management-from-the-board-room-risk-lost-in-translation.

Cisco.com (2017). *LAN Solutions Guide for Higher Education/Universities.* Retrieved from Cisco.com: https://www.cisco.com/c/en/us/products/wireless/-office-net-software/index.html.

Computer Weekly. (2010). *iTunes hack could affect thousands, say experts.* Retrieved from Computer Weekly: http://www.computerweekly.com/news/1280093237/iTunes-hack-could-affect-thousands-say-experts.

Delac, G., Silic, M. & Krolo, J. (2011). Emerging security threats for mobile platforms. In *MIPRO, 2011 Proceedings of the 34th International Convention* (pp. 1468-1473). IEEE.

Ernest & Young Global Limited, (2015). *The multiplying effect of today's cybersecurity challenges*. Cybersecurity and the Internet of Things.

Friedman, J. & Hoffman, D. (2008). Protecting data on mobile devices: A taxonomy of security threats to mobile computing and review of applicable defenses. *Information Knowledge Systems Management*, 159-180.

Gelenbe, E., Gorbil, G., Tzovaras, D., Liebergeld, S., Garcia, D., Baltatu, M., & Lyberopoulos, G. (2013). Security for smart mobile networks: The NEMESYS approach. In *Privacy and Security in Systems (PRISMS), 2013 International Conference on* (pp. 1-8). IEEE.

Hossain, M. M., Fotouhi, M. & Hasan, R. (2015). Towards an analysis of security issues, challenges, and open problems in the internet of things. In *Services (SERVICES), 2015 IEEE World Congress on* (pp. 21-28). IEEE.

Huang, X., Craig, P., Lin, H. & Yan, Z. (2015). SecIoT: a security framework for the Internet of Things. *Security and Communication Networks*.

Jha, A. & Sunil, M. C. (2014). Security considerations for Internet of Things. *L&T Technology Services*.

Kim, D. H., Cho, J. Y., Kim, S., & Lim, J. (2015). A Study of Developing Security Requirements for Internet of Things (IoT). *Advanced Science and Technology Letters*, *87*, 94-99.

Kim, J. T. (2015). Requirement of Security for IoT Application based on Gateway System. *International Journal of Security and Its Applications*, *9*(10), 201-208.

Kim, J. & Lee, J. W. (2014). OpenIoT: An open service framework for the Internet of Things. In *Internet of Things (WF-IoT), 2014 IEEE World Forum on* (pp. 89-93). IEEE.

Koh, E. B., Oh, J. & Im, C. (2014). A study on security threats and dynamic access control technology for BYOD, smart-work environment. In *Proceedings of the International MultiConference of Engineers and Computer Scientists*. 2, (pp. 1-6).

KPMG, (2015). *Focus on Security, Privacy and Trust*. Security and the IoT Ecosystem

Lee, Y. & Kim, D. (2015). Threats Analysis, Requirements and Considerations for Secure Internet of Things. *International Journal of Smart Home*, *9*(12), 191-198.

Madakam, S. & Date, H. (2016). Security mechanisms for connectivity of smart devices in the internet of things. In *Connectivity Frameworks for Smart Devices* (pp. 23-41). Springer International Publishing.

Mateski, M., Trevino, C. M., Veitch, C. K., Michalski, J., Harris, J. M., Maruoka, S. & Frye, J. (2012). Cyber threat metrics. *Sandia National Laboratories*.

Miller, K. W., Voas, J. & Hurlburt, G. F. (2012). BYOD: Security and privacy considerations. *It Professional*, *14*(5), 53-55.

Milligan, P. M. & Hutcheson, D. (2008). Business Risks and Security Assessment for Devices. *Information Systems Control Journal*, 1-5.

Mohammed, L. A. (2010). ICT Security Policy: Challenges and Potential Remedies. *Handbook of Research on Information Communication Technology Policy: Trends, Issues and Advancements: Trends, Issues and Advancements*, 337.

Newman, J. (2011). *4 Security Tips Spurred by Recent Phishing Attacks.* Retrieved from PC World:http://www.pcworld.com/article/229361/4_security_tips_spurred_by_recent_phishing_attacks_on_gmail_hotmail_and_yahoo.html.

NIST, G. S., Goguen, A. & Fringa, A. (2002). Risk Management Guide for Information Technology Systems. *Recommendations of the National Institute of Standards and Technology*.

NZ Business. (2011). Are mobile devices compromising your business security? *NZ Business*, p. 60.

O'Dell, J. (2010). *New Study Shows the Web Will Rule by 2015.* Retrieved from Mashable: http://mashable.com/2010/04/13/-web-stats.

Open Web Application Security Project (OWASP) (2014). *IoT Top Ten Vulnerabilities*. Retrieved from DOI https://www.owasp.org/ images/ 7/71/Internet_of_ Things_Top_Ten_2014- OWASP.pdf

Pinola, M. (2012). *Internet Access Comparison.* Retrieved from About.com Office Technology: Pros and cons of different Internet-on-the-Go options: http://office.about.com/od/wificonnectivity/a/wireless-internet-comparison.html.

Riahi, A., Challal, Y., Natalizio, E., Chtourou, Z. & Bouabdallah, A. (2013). A systemic approach for IoT security. In *Distributed Computing in Sensor Systems (DCOSS), 2013 IEEE International Conference on* (pp. 351-355). IEEE.

Sabale, R. G. & Dani, A. R. (2012). Comparative study of prototype model for software engineering with system development life cycle. *IOSR Journal of Engineering*, 2(7), 21-24.

Saif, I., Peasley, S. & Perinkolam, A. (2015). *Being secure, vigilant and resilient in the connected age*. Safeguarding the Internet of Things. *The Internet of Things*, 41 retrieved from https://dupress.deloitte.com/dup-us-en/deloitte-review/issue-17/internet-of-things-data-security-and-privacy.html.

Shafagh, H. & Hithnawi, A. (2014). Security Comes First, A Public-key Cryptography Framework for the Internet of Things. In *Distributed Computing in Sensor Systems (DCOSS), 2014 IEEE International Conference on* (pp. 135-136). IEEE.

Shukla, I. (2011). *Advantages of Computing.* Retrieved from Buzzle.com: http://www.buzzle.com/articles/advantages-of--computing.html.

Sopori, D., Pawar, T., Patil, M., & Ravindran, R. (2017). Internet of Things: Security Threats.

Souppaya, M. & Scarfone, K. (2013). Guidelines for managing the security of devices in the enterprise. *NIST special publication, 800*, 124.

Suo, H., Wan, J., Zou, C., & Liu, J. (2012). Security in the internet of things: a review. In *Computer Science and Electronics Engineering (ICCSEE), 2012 international conference on* 3, (pp. 648-651). IEEE.

TechTarget.com. (2012). *Search Computing.* Retrieved from Techtarget.com: http://searchcomputing.techtarget.com

U.S. Department of Homeland Security, (2016). *Prioritizing IoT security*. Strategic principles for security Internet of Things (IoT) version 1.0 retrieved from https://www.dhs.gov/.../Strategic_Principles_for_Securing_the_Internet_of_Things.

Vermesan, O. & Friess, P. (Eds.). (2013). *Internet of things: converging technologies for smart environments and integrated ecosystems*. River Publishers.

Warwick, A. (2010). *Millions downloaded suspicious Android wallpaper.* Retrieved from Computer Weekly: http://www.computerweekly.com/news/1280093401/Millions-download-suspicious-Android-wallpaper.

Westervelt, R. (2011). *Android app security: Study finds developers creating flawed Android apps.* Retrieved from SearchSecurity: http://searchsecurity.techtarget.com/news/2240112235/Android-app-security-Study-finds--developers-creating-flawed-Android-apps.

Westervelt, R. (2011). Top 5 phone security threats in 2012. Retrieved from Search Security: http://searchsecurity.techtarget.com/news/2240112288/Top-5--phone-security-threats-in-2012.

Youker, B. W. (2014). Goal-free Evaluation and Goal-Based Evaluation. *The Foundation Review 5(4) 50-61.*

Zaidi, S. F. A., Shah, M. A., Kamran, M., Javaid, Q. & Zhang, S. (2016). A Survey on Security for Smartphone Device. *International Journal of Advanced Computer Science and Applications-2016.*

Zhao, K. & Ge, L. (2013). A survey on the internet of things security. In *Computational Intelligence and Security (CIS), 2013 9th International Conference on* (pp. 663-667). IEEE.

APPENDICES

Appendix 1: Questionnaire

Instructions

I am student at Kabarak University studying Masters of Science in Information Security and Audit. My area of research is on threat matrix for smart mobile devices in a university network towards a secure local area network ecosystem. Confidentiality was highly observed in this questionnaire your responses were only be used for academic purposes. Therefore you are requested to fill this questionnaire in the most free and honest way possible.

Please tick [√] the appropriate answers in the boxes provided and also write down the appropriate answers in the spaces provided. Do not write your name on the questionnaire. Thank you in advance for your time and cooperation.

SECTION 1: General Questions

1. Are you a staff or a student?

   Staff □ Student □ Other (specify) □

2. Do you own any smart mobile devices (eg Smart Phone, Laptop, Tablet etc)

   Yes □ No □

3. How often do you use your smart mobile device to connect to the Internet through corporate network (eg through Wi-Fi)?

   Hourly □ Daily □ Weekly □ Never □

4. Have you ever lost your smart mobile device or has it ever been stolen?

   Never □ Once □ More than Once □

5. Have you ever attended smart mobile device security and privacy awareness training? □ □

   Yes No

SECTION 2:

In a scale of 1 to 5, please tick the most appropriate answer to the questions here below related to how you use smart mobile device. (***KEYS****: **1**=strongly disagree**, 2=**Disagree**,* ***3****=Neutral**, 4**=Agree**, 5**=strongly Agree**)***

No.	Question	1	2	3	4	5
A.	**Information Security Policy**					
1.	The university has an ICT security policy which is implemented and enforced					
2.	I have read and clearly understood the university security policy					
3.	The university security policy permits use of personally-owned devices					
4.	The university security policy requires all smart mobile devices to have an approved operating system					
5.	The university security policy requires all smart mobile devices to have latest security patches and upgrades					
B.	**Asset Management**					
1.	My smart mobile device characteristics are registered in the university database					
2.	The security policy clearly specifies penalties for unauthorized use of smart mobile devices					
3.	The university security policy prohibits leaving smart mobile device unattended when attached to a corporate computer					
4.	The university insures smart mobile devices against loss, theft, or damage					
5.	The university security policy outlines reporting procedures for lost, stolen, or damaged smart mobile devices					

6.	The university maintains a secured inventory of all smart mobile devices.					
7.	My smart mobile device can be locked if lost or stolen					
8.	Whenever I am selling my smart mobile device, I always reset my device to factory setting and clear any saved data					
C.	**Access Control**					
1.	My smart mobile device undergoes authentication process before connecting to the university network					
2.	All smart mobile devices within the university network are monitored for unauthorized activities					
3.	My smart mobile device can hide data, after pre-defined number of failed logon attempts					
4.	My smart mobile device has a unique name and password which is not known by anyone else					
5.	My smart mobile device is set to lock screen whenever not in use for a certain period of time					
6.	I always disable or protect remote access to my smart mobile device whenever connected to the network					
7.	Allocation and reallocation of passwords is controlled through a formal management process					
8.	My smart mobile device uses password protection when not in use					
9.	My smart mobile device has multiple authentication mechanisms eg Password, Fingerprint, on-screen pattern etc					
D.	**Operations Security**					
1.	My smart mobile device contain both personal and university data					

2.	My smart mobile device is automatically examined for compliance with the university security policy once I connect to its network					
3.	The university security policy specifies the types of information that can and cannot be stored, processed, and transferred on smart mobile devices					
4.	The security policy outlines approved Modes of Operation: wired and wireless					
5.	I regularly synchronize my smart mobile device with university computer or network, for backup purposes					
6.	My smart mobile device has password expiration feature that allows password to expire after pre-defined time length					
7.	My smart mobile device contain an updated antivirus software that scans files as they are opened					
8.	Manufacturer debugging features on my smart mobile device are disabled					
9.	My smart mobile device has some unapproved software and applications					
10.	Smart mobile devices are monitored when connected to the university computer or network					
11.	My smart mobile device is updated and configured to install new updates whenever available					
12.	When downloading applications, I always use the official downloading sites					
E.	**Communications Security**					
1.	Smart mobile device is not used to store, process, or transfer sensitive, proprietary, or classified data, unless encryption is used					

2.	The university security policy prohibits use of public or untrusted network access points					
3.	The university security policy provides protective measures against social engineering and other security attacks					
4.	The university security policy require all smart mobile devices to use a password to synchronize to an organizational computer or network					
5.	Updated signatures are installed on my smart mobile device each time they synchronize to a university computer or at regular intervals via a secure network connection					
6.	The university implements encryption to protect information on smart mobile devices					
7.	The university implements a firewall on smart mobile devices					
8.	The university implements VPN software for smart mobile devices, for remote network connections					
9.	Unneeded network connections within the university network are disabled					
10.	Unneeded applications and services within the university network are disabled					
11.	I always connect my smart mobile device to free public Wi-Fi whenever available					

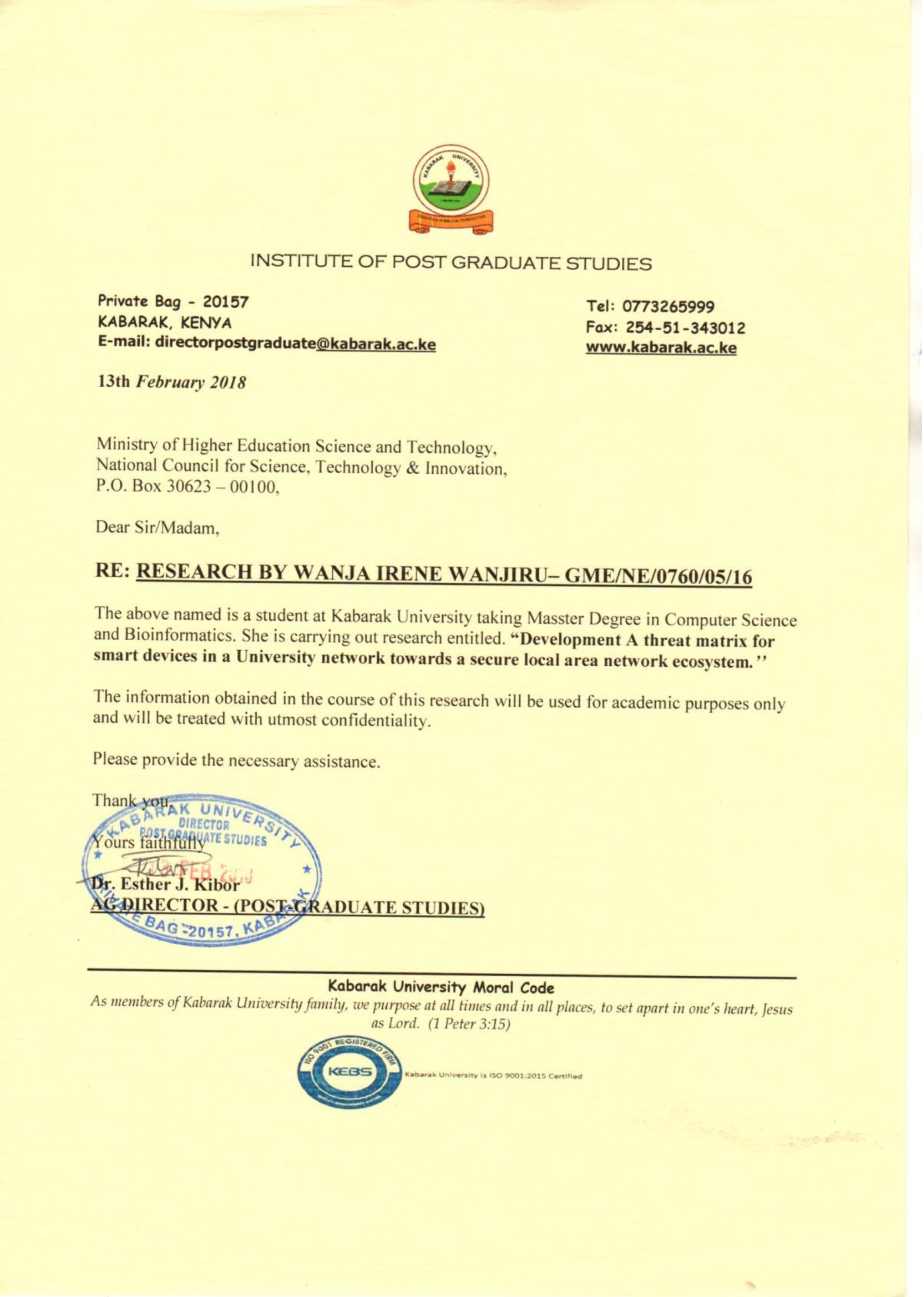
SECTION 3: Likelihood of Attack Questions

In a scale of 1 to 5, please tick the most appropriate answer to the questions here below related to likelihood of attack. (***KEYS**: **1**=strongly disagree, **2=**Disagree, **3=**Neutral, **4=**Agree, **5=**strongly Agree)*

No.	Question	1	2	3	4	5
1.	My smart mobile device enables me to access information from university database and other internal resources					
2.	I use my smart mobile device to access links sent through emails while connected to the university network					
3.	I have been attending cyber security awareness campaigns organized by the university					
4.	The university controls the security setup in my smart mobile device					
5.	My smart mobile device is protected against theft and loss					
6.	The advanced technologies in devices such as high storage and high internet speed has enhanced the operations on my smart mobile device					
7.	I always select strong password on my smart mobile device and use different passwords for different websites					
8.	I only download secure applications on my smart mobile device					
9.	I am well aware of security issues involved with wireless connections					

Thank you for your time and response

Appendix 2: Authority to Collect Data from Kabarak University



INSTITUTE OF POST GRADUATE STUDIES

Private Bag - 20157
KABARAK, KENYA
E-mail: directorpostgraduate@kabarak.ac.ke

Tel: 0773265999
Fax: 254-51-343012
www.kabarak.ac.ke

13th *February 2018*

Ministry of Higher Education Science and Technology,
National Council for Science, Technology & Innovation,
P.O. Box 30623 – 00100,

Dear Sir/Madam,

RE: RESEARCH BY WANJA IRENE WANJIRU– GME/NE/0760/05/16

The above named is a student at Kabarak University taking Masster Degree in Computer Science and Bioinformatics. She is carrying out research entitled. **"Development A threat matrix for smart devices in a University network towards a secure local area network ecosystem."**

The information obtained in the course of this research will be used for academic purposes only and will be treated with utmost confidentiality.

Please provide the necessary assistance.

Thank you,

Yours faithfully

KABARAK UNIVERSITY
DIRECTOR
POST GRADUATE STUDIES
FEB 20
BAG -20157, KABARAK

Dr. Esther J. Kibor
AG DIRECTOR - (POST-GRADUATE STUDIES)

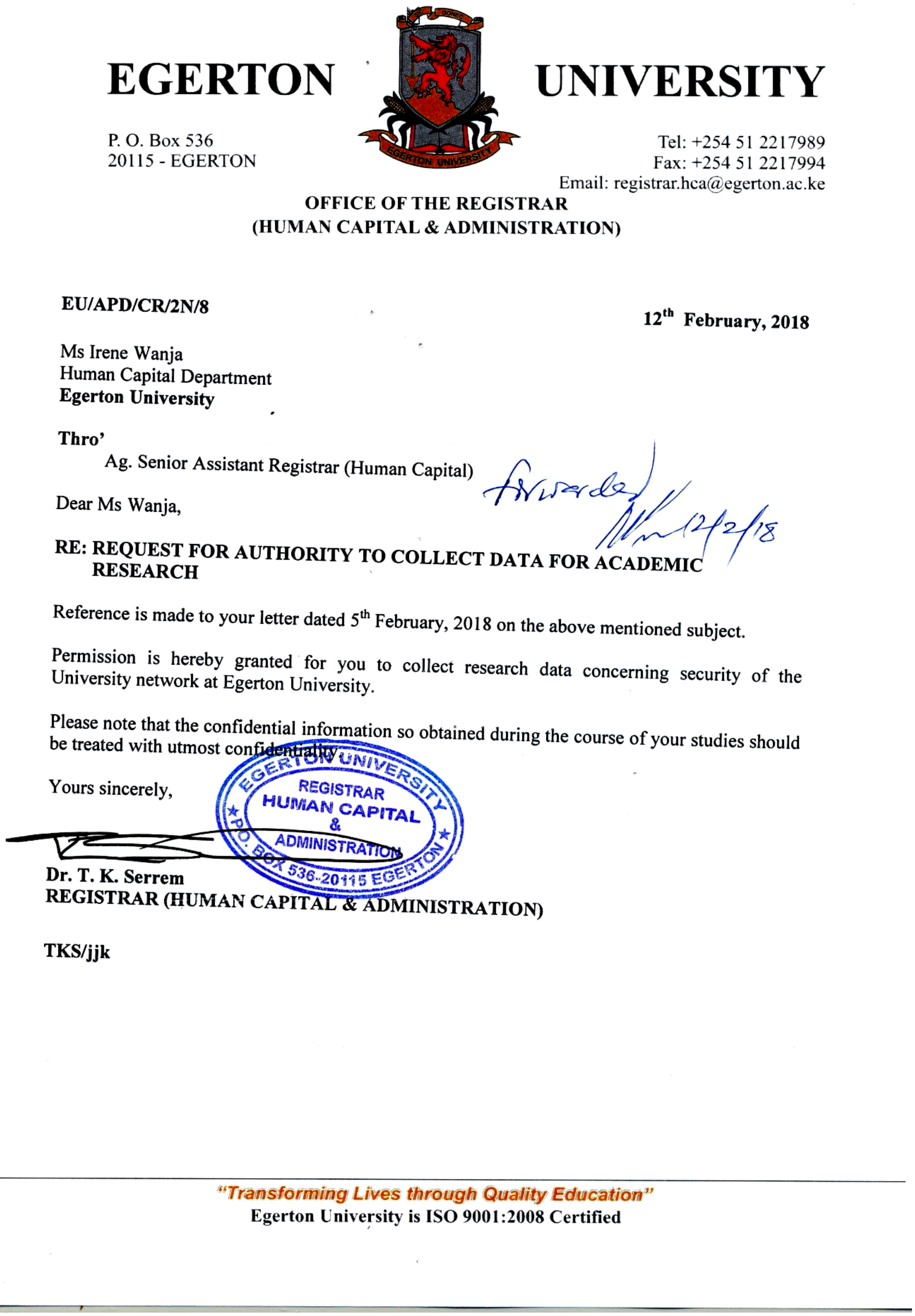
Kabarak University Moral Code

As members of Kabarak University family, we purpose at all times and in all places, to set apart in one's heart, Jesus as Lord. (1 Peter 3:15)

ISO 9001 REGISTERED FIRM KEBS

Kabarak University is ISO 9001:2015 Certified

Appendix 3: Authority to Collect Data from Egerton University



EGERTON UNIVERSITY

P. O. Box 536
20115 - EGERTON

Tel: +254 51 2217989
Fax: +254 51 2217994
Email: registrar.hca@egerton.ac.ke

OFFICE OF THE REGISTRAR
(HUMAN CAPITAL & ADMINISTRATION)

EU/APD/CR/2N/8

12th February, 2018

Ms Irene Wanja
Human Capital Department
Egerton University

Thro'
Ag. Senior Assistant Registrar (Human Capital)

Forwarded
12/2/18

Dear Ms Wanja,

RE: REQUEST FOR AUTHORITY TO COLLECT DATA FOR ACADEMIC RESEARCH

Reference is made to your letter dated 5th February, 2018 on the above mentioned subject.

Permission is hereby granted for you to collect research data concerning security of the University network at Egerton University.

Please note that the confidential information so obtained during the course of your studies should be treated with utmost confidentiality.

Yours sincerely,

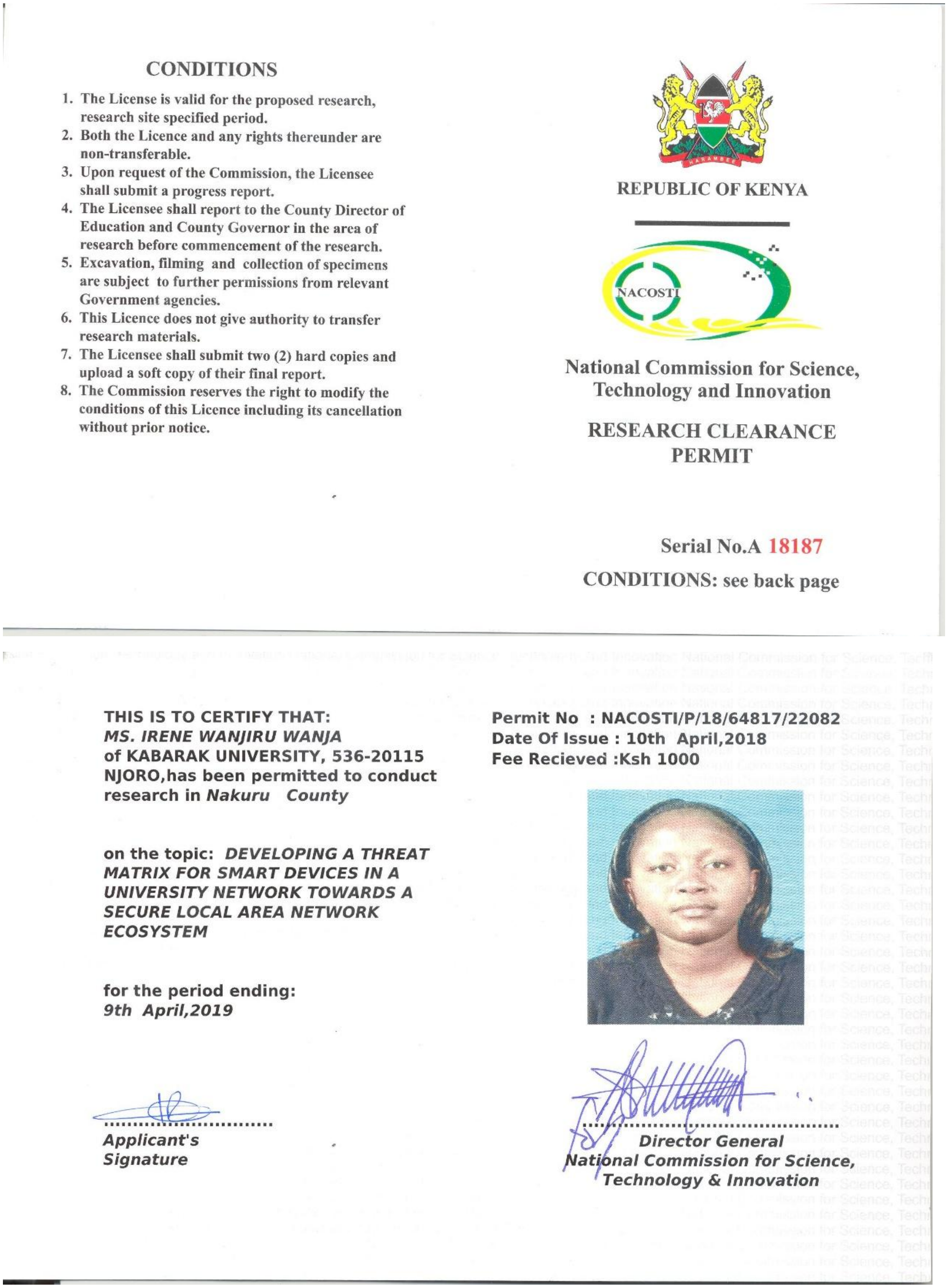
EGERTON UNIVERSITY
REGISTRAR
HUMAN CAPITAL
&
ADMINISTRATION
P.O. BOX 536-20115 EGERTON

Dr. T. K. Serrem
REGISTRAR (HUMAN CAPITAL & ADMINISTRATION)

TKS/jjk

"Transforming Lives through Quality Education"
Egerton University is ISO 9001:2008 Certified

Appendix 4: NACOSTI Research Clearance Permit



CONDITIONS

1. The License is valid for the proposed research, research site specified period.
2. Both the Licence and any rights thereunder are non-transferable.
3. Upon request of the Commission, the Licensee shall submit a progress report.
4. The Licensee shall report to the County Director of Education and County Governor in the area of research before commencement of the research.
5. Excavation, filming and collection of specimens are subject to further permissions from relevant Government agencies.
6. This Licence does not give authority to transfer research materials.
7. The Licensee shall submit two (2) hard copies and upload a soft copy of their final report.
8. The Commission reserves the right to modify the conditions of this Licence including its cancellation without prior notice.

REPUBLIC OF KENYA

NACOSTI

National Commission for Science, Technology and Innovation

RESEARCH CLEARANCE PERMIT

Serial No.A 18187

CONDITIONS: see back page

THIS IS TO CERTIFY THAT:
MS. IRENE WANJIRU WANJA
of KABARAK UNIVERSITY, 536-20115
NJORO,has been permitted to conduct research in *Nakuru County*

on the topic: *DEVELOPING A THREAT MATRIX FOR SMART DEVICES IN A UNIVERSITY NETWORK TOWARDS A SECURE LOCAL AREA NETWORK ECOSYSTEM*

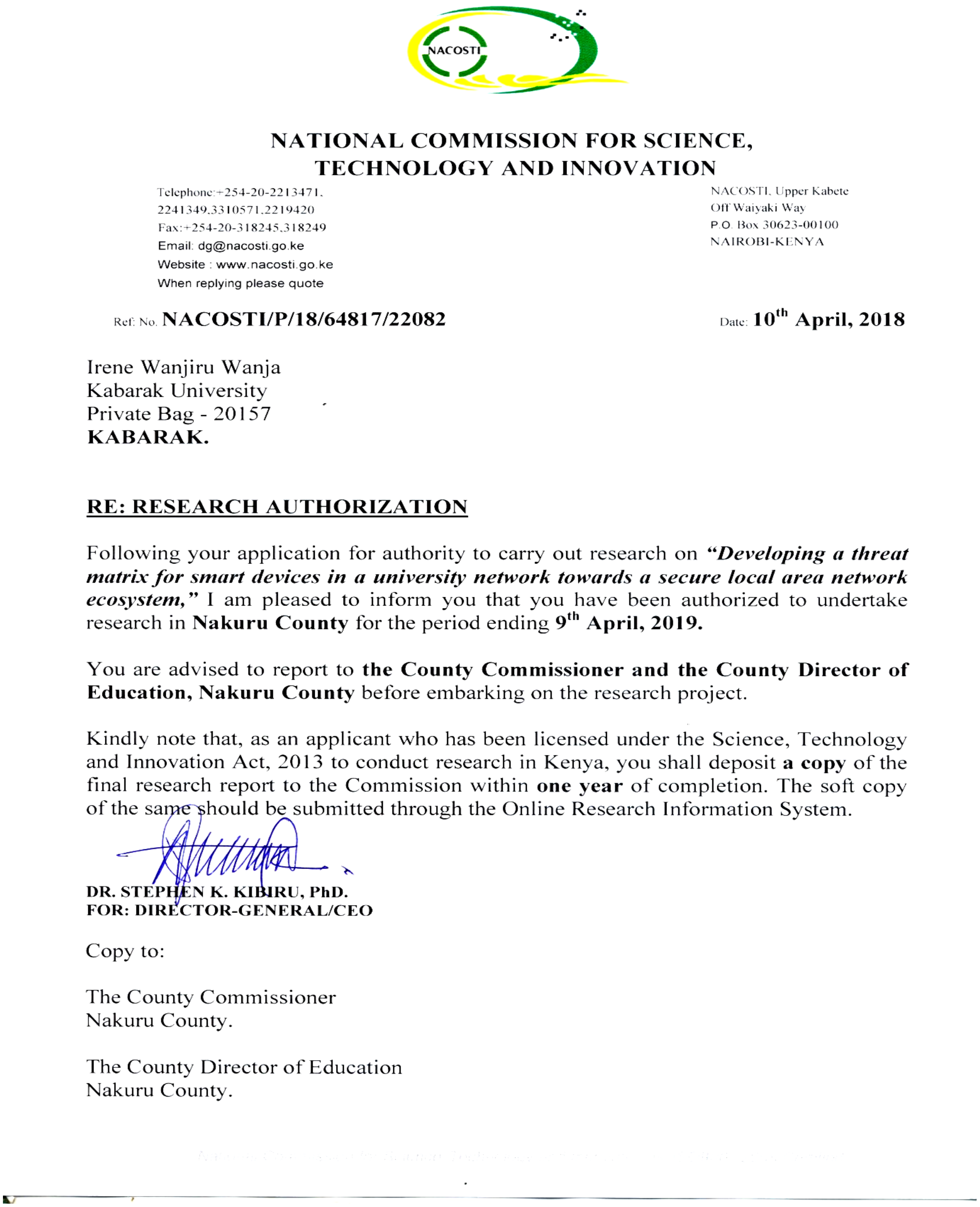
for the period ending:
9th April,2019

Permit No : NACOSTI/P/18/64817/22082
Date Of Issue : 10th April,2018
Fee Recieved :Ksh 1000

....
Applicant's Signature

....
Director General
National Commission for Science, Technology & Innovation

Appendix 5: NACOSTI Research Authorization



NATIONAL COMMISSION FOR SCIENCE,
TECHNOLOGY AND INNOVATION

Telephone:+254-20-2213471,
2241349,3310571,2219420
Fax:+254-20-318245,318249
Email: dg@nacosti.go.ke
Website : www.nacosti.go.ke
When replying please quote

NACOSTI, Upper Kabete
Off Waiyaki Way
P.O. Box 30623-00100
NAIROBI-KENYA

Ref: No. **NACOSTI/P/18/64817/22082**

Date: **10th April, 2018**

Irene Wanjiru Wanja
Kabarak University
Private Bag - 20157
KABARAK.

RE: RESEARCH AUTHORIZATION

Following your application for authority to carry out research on ***"Developing a threat matrix for smart devices in a university network towards a secure local area network ecosystem,"*** I am pleased to inform you that you have been authorized to undertake research in **Nakuru County** for the period ending **9th April, 2019.**

You are advised to report to **the County Commissioner and the County Director of Education, Nakuru County** before embarking on the research project.

Kindly note that, as an applicant who has been licensed under the Science, Technology and Innovation Act, 2013 to conduct research in Kenya, you shall deposit **a copy** of the final research report to the Commission within **one year** of completion. The soft copy of the same should be submitted through the Online Research Information System.

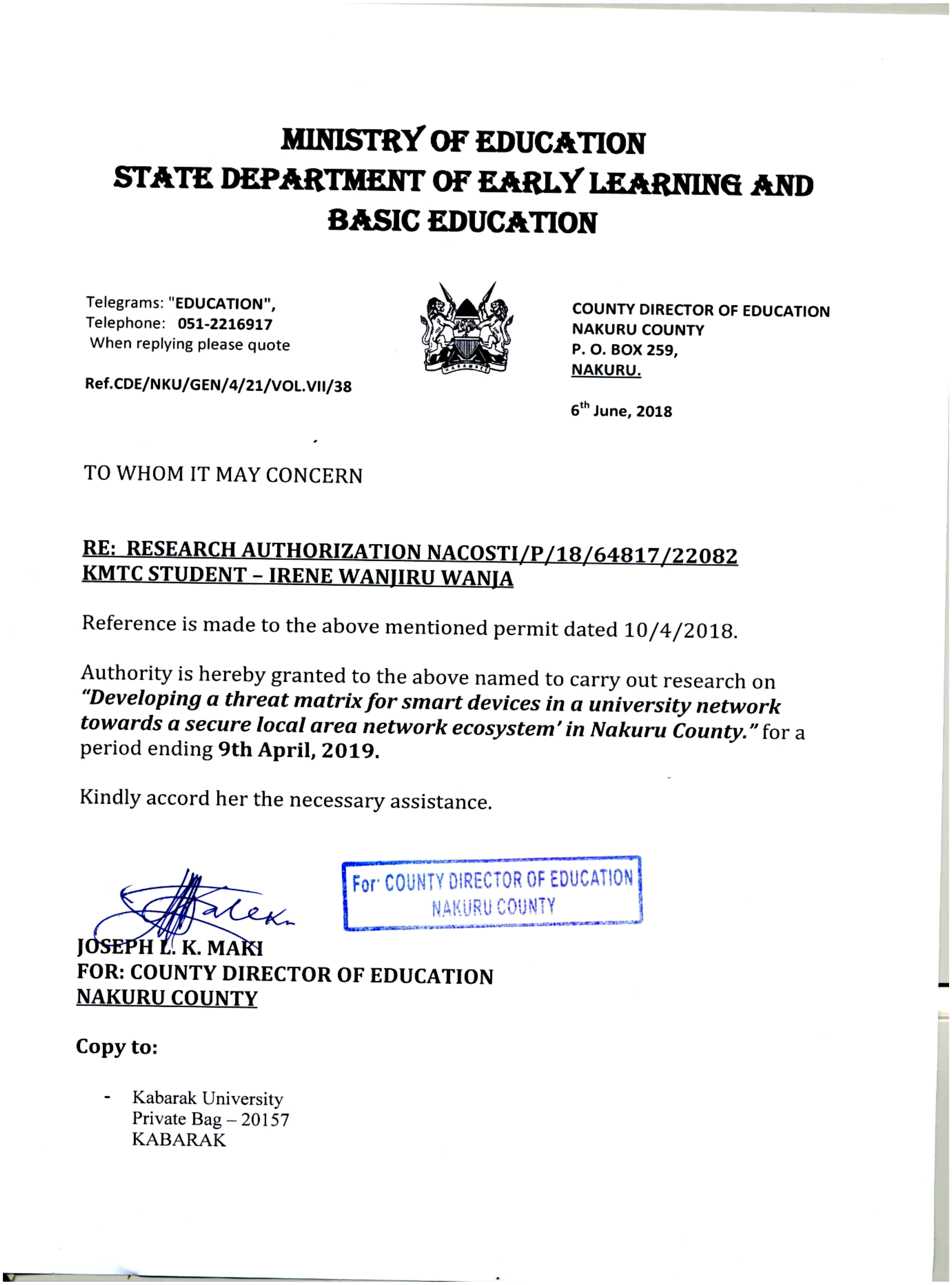
DR. STEPHEN K. KIBIRU, PhD.
FOR: DIRECTOR-GENERAL/CEO

Copy to:

The County Commissioner
Nakuru County.

The County Director of Education
Nakuru County.

Appendix 6: Research Authorization from County Director of Education Nakuru County



MINISTRY OF EDUCATION
STATE DEPARTMENT OF EARLY LEARNING AND BASIC EDUCATION

Telegrams: "EDUCATION",
Telephone: 051-2216917
When replying please quote

Ref.CDE/NKU/GEN/4/21/VOL.VII/38

COUNTY DIRECTOR OF EDUCATION
NAKURU COUNTY
P. O. BOX 259,
NAKURU.

6th June, 2018

TO WHOM IT MAY CONCERN

RE: RESEARCH AUTHORIZATION NACOSTI/P/18/64817/22082
KMTC STUDENT – IRENE WANJIRU WANJA

Reference is made to the above mentioned permit dated 10/4/2018.

Authority is hereby granted to the above named to carry out research on ***"Developing a threat matrix for smart devices in a university network towards a secure local area network ecosystem' in Nakuru County."*** for a period ending **9th April, 2019.**

Kindly accord her the necessary assistance.

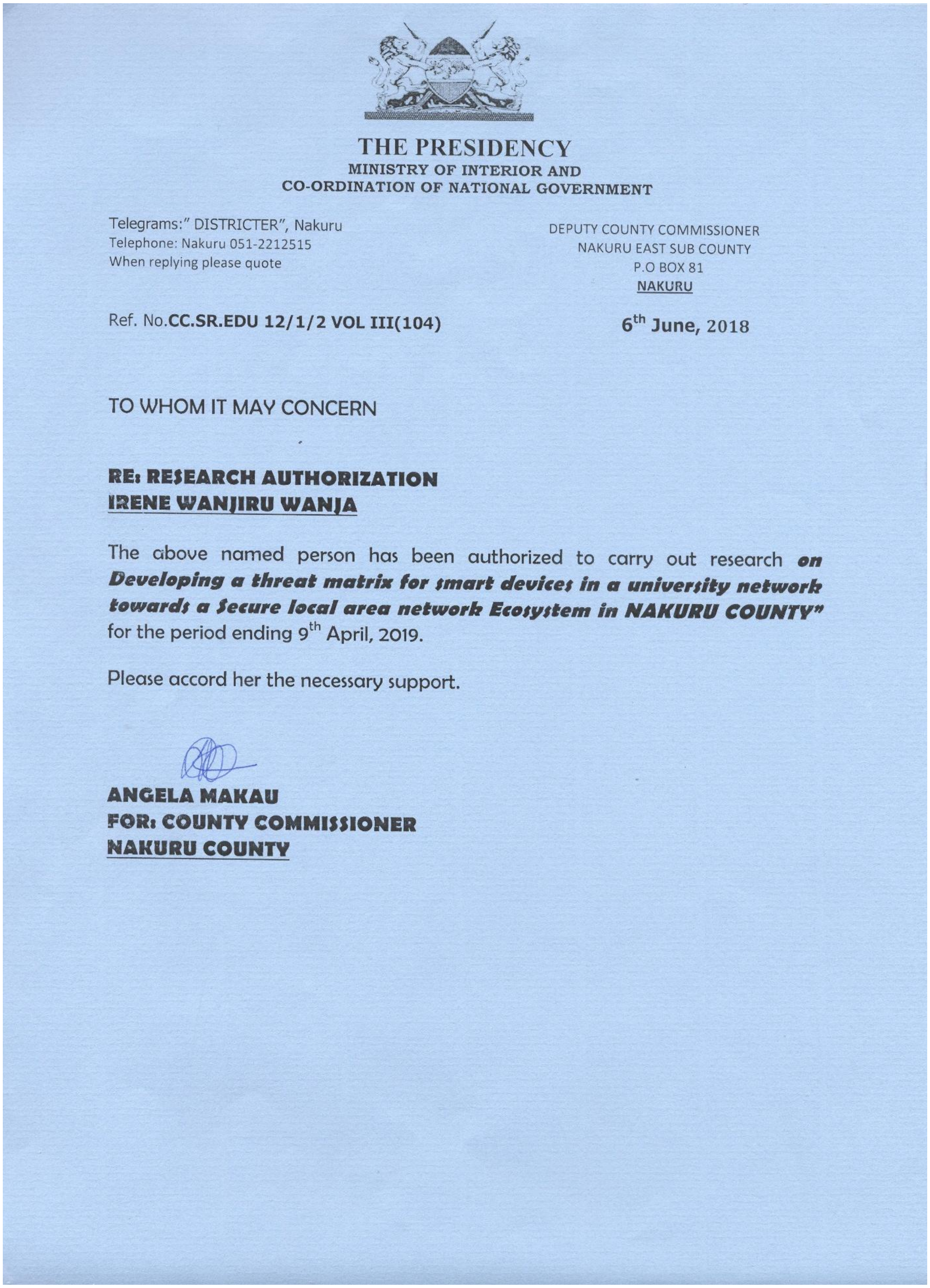
For COUNTY DIRECTOR OF EDUCATION
NAKURU COUNTY

JOSEPH L. K. MAKI
FOR: COUNTY DIRECTOR OF EDUCATION
NAKURU COUNTY

Copy to:

- Kabarak University
  Private Bag – 20157
  KABARAK

Appendix 7: Research Authorization from County Commissioner Nakuru County



THE PRESIDENCY
MINISTRY OF INTERIOR AND
CO-ORDINATION OF NATIONAL GOVERNMENT

Telegrams:" DISTRICTER", Nakuru
Telephone: Nakuru 051-2212515
When replying please quote

DEPUTY COUNTY COMMISSIONER
NAKURU EAST SUB COUNTY
P.O BOX 81
NAKURU

Ref. No.**CC.SR.EDU 12/1/2 VOL III(104)**

6th June, 2018

TO WHOM IT MAY CONCERN

RE: RESEARCH AUTHORIZATION
IRENE WANJIRU WANJA

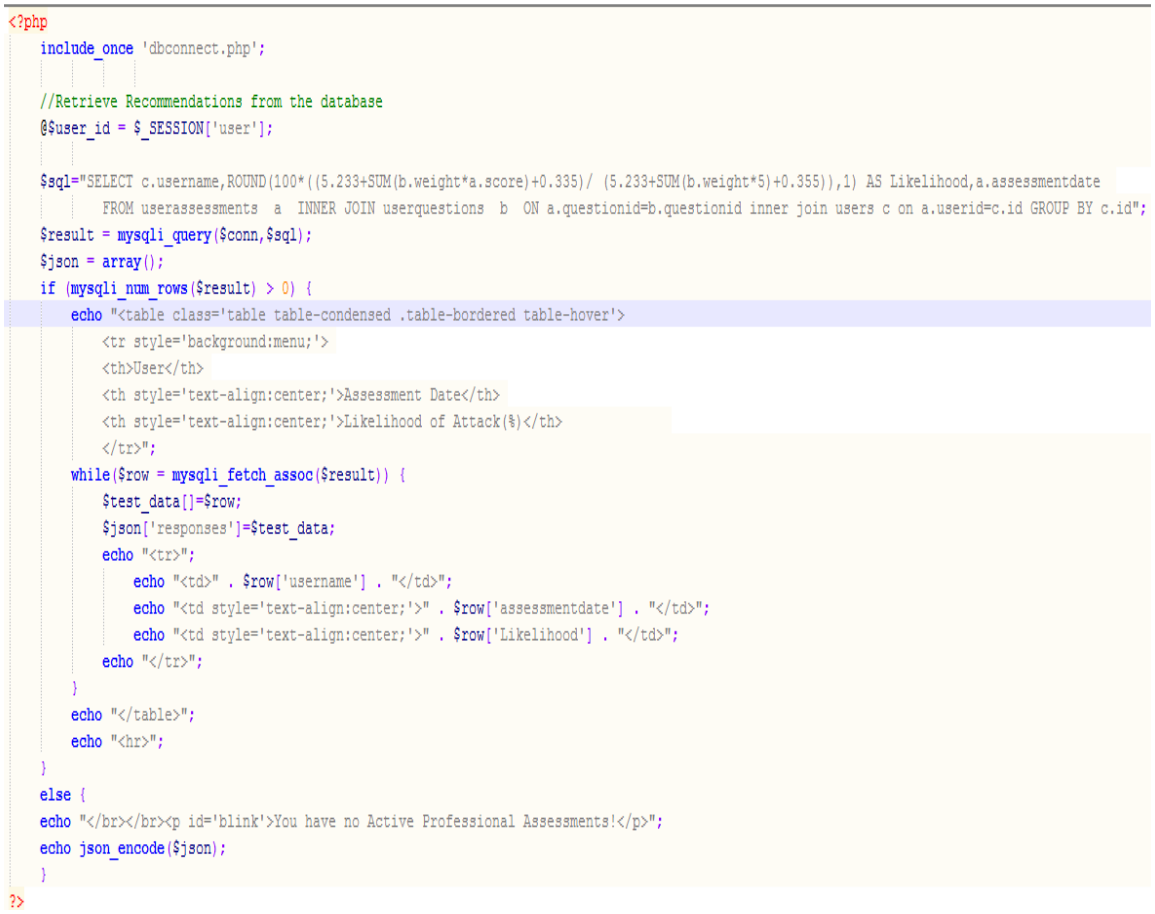
The above named person has been authorized to carry out research ***on Developing a threat matrix for smart devices in a university network towards a Secure local area network Ecosystem in NAKURU COUNTY"*** for the period ending 9th April, 2019.

Please accord her the necessary support.

ANGELA MAKAU
FOR: COUNTY COMMISSIONER
NAKURU COUNTY

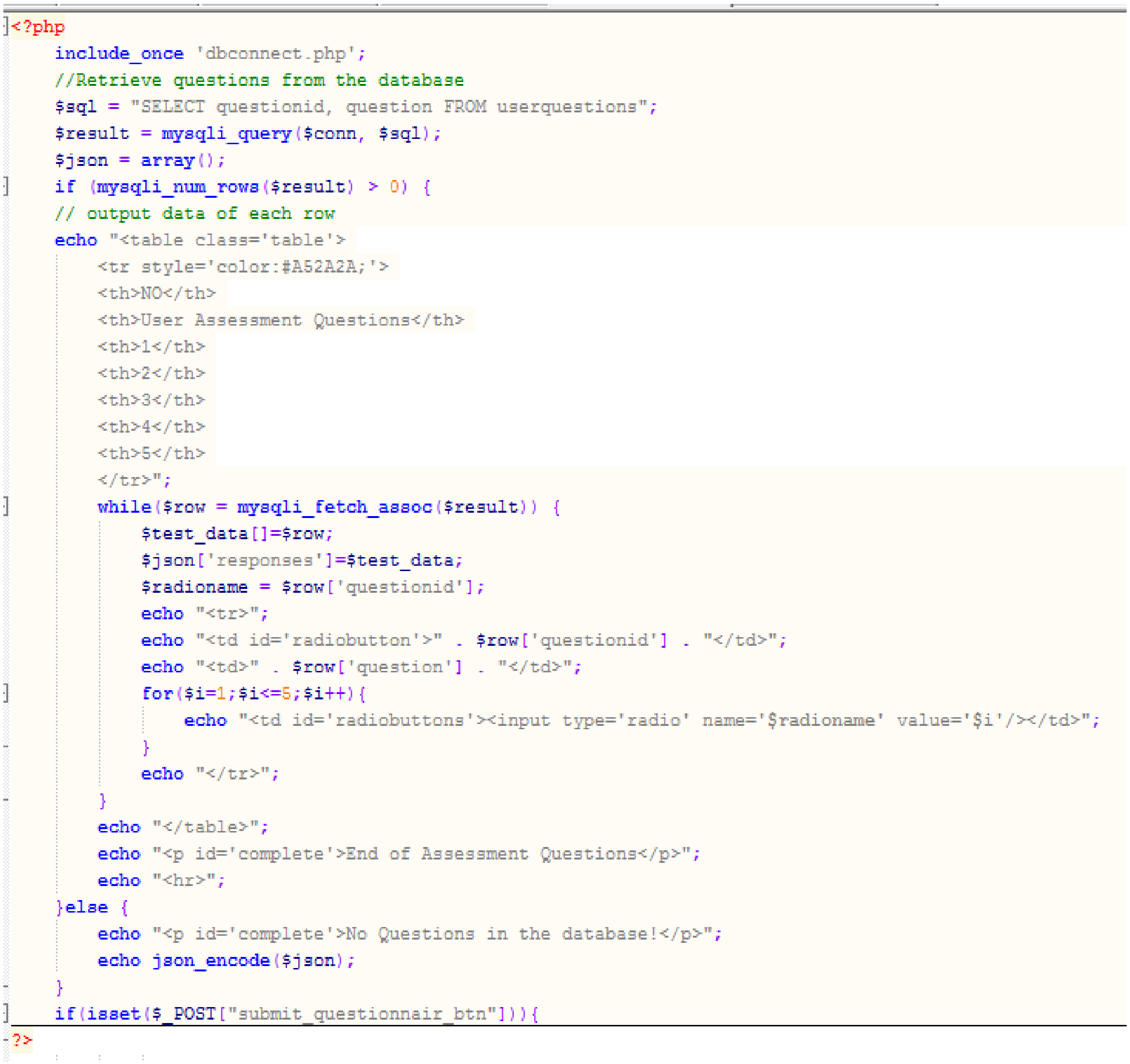
Appendix 8: System Code

Users and Scores Code



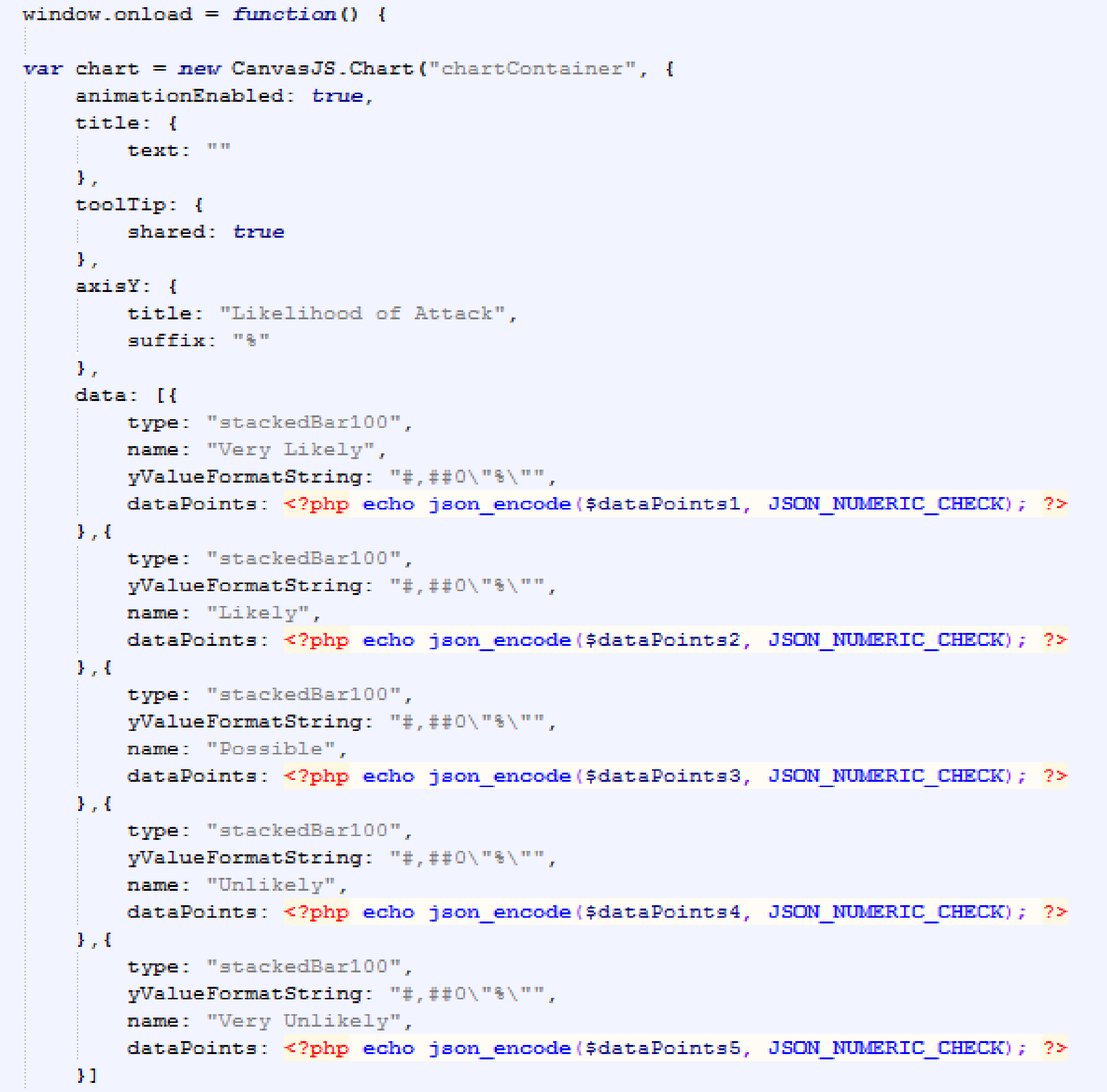
```php
<?php
    include_once 'dbconnect.php';

    //Retrieve Recommendations from the database
    @$user_id = $_SESSION['user'];

    $sql="SELECT c.username,ROUND(100*((5.233+SUM(b.weight*a.score)+0.335)/ (5.233+SUM(b.weight*5)+0.355)),1) AS Likelihood,a.assessmentdate
            FROM userassessments  a  INNER JOIN userquestions  b  ON a.questionid=b.questionid inner join users c on a.userid=c.id GROUP BY c.id";
    $result = mysqli_query($conn,$sql);
    $json = array();
    if (mysqli_num_rows($result) > 0) {
        echo "<table class='table table-condensed .table-bordered table-hover'>
            <tr style='background:menu;'>
            <th>User</th>
            <th style='text-align:center;'>Assessment Date</th>
            <th style='text-align:center;'>Likelihood of Attack(%)</th>
            </tr>";
        while($row = mysqli_fetch_assoc($result)) {
            $test_data[]=$row;
            $json['responses']=$test_data;
            echo "<tr>";
                echo "<td>" . $row['username'] . "</td>";
                echo "<td style='text-align:center;'>" . $row['assessmentdate'] . "</td>";
                echo "<td style='text-align:center;'>" . $row['Likelihood'] . "</td>";
            echo "</tr>";
        }
        echo "</table>";
        echo "<hr>";
    }
    else {
    echo "</br></br><p id='blink'>You have no Active Professional Assessments!</p>";
    echo json_encode($json);
    }
?>
```

User Assessment Code



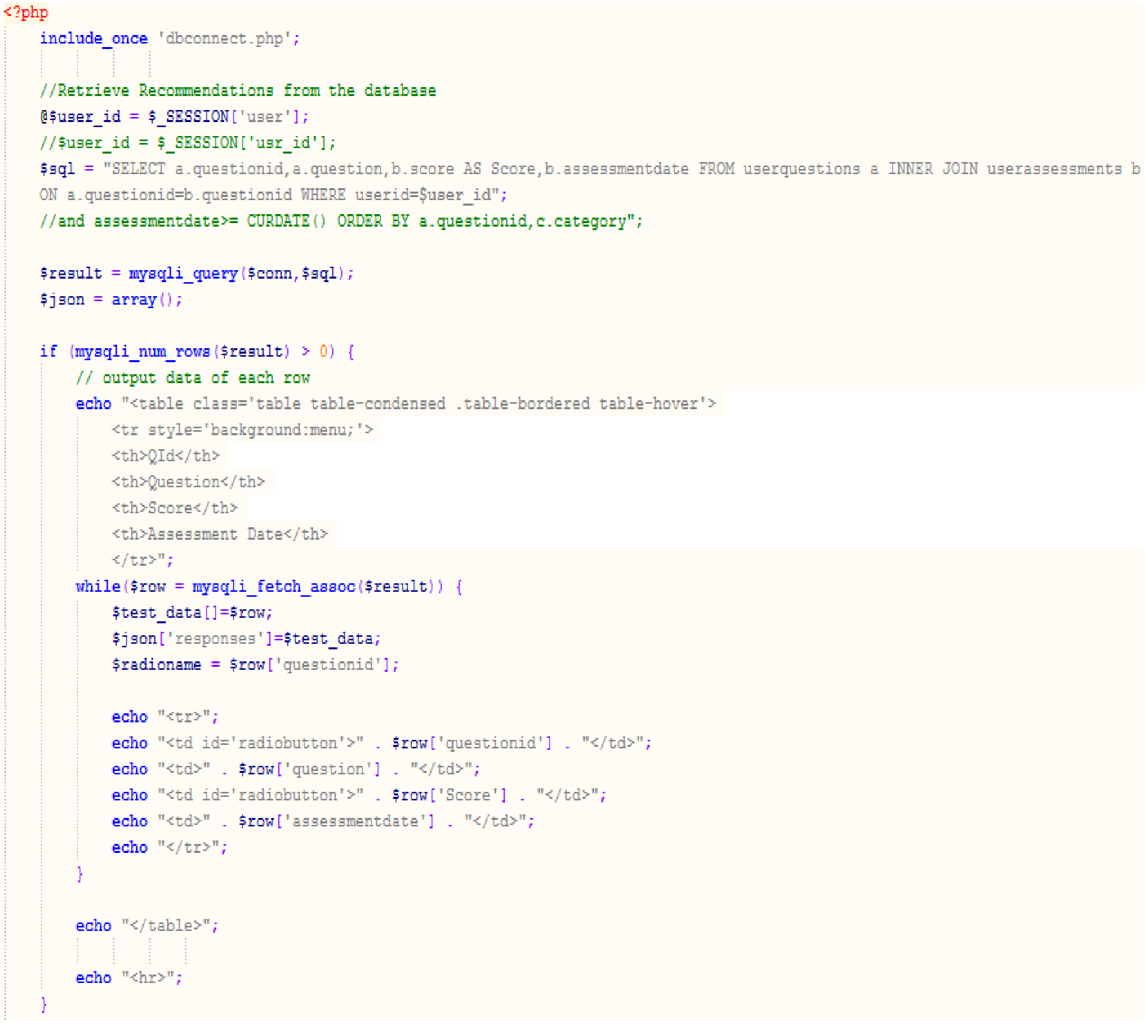
```
<?php
    include_once 'dbconnect.php';
    //Retrieve questions from the database
    $sql = "SELECT questionid, question FROM userquestions";
    $result = mysqli_query($conn, $sql);
    $json = array();
    if (mysqli_num_rows($result) > 0) {
    // output data of each row
    echo "<table class='table'>
        <tr style='color:#A52A2A;'>
        <th>NO</th>
        <th>User Assessment Questions</th>
        <th>1</th>
        <th>2</th>
        <th>3</th>
        <th>4</th>
        <th>5</th>
        </tr>";
        while($row = mysqli_fetch_assoc($result)) {
            $test_data[]=$row;
            $json['responses']=$test_data;
            $radioname = $row['questionid'];
            echo "<tr>";
            echo "<td id='radiobutton'>" . $row['questionid'] . "</td>";
            echo "<td>" . $row['question'] . "</td>";
            for($i=1;$i<=5;$i++){
                echo "<td id='radiobuttons'><input type='radio' name='$radioname' value='$i'/></td>";
            }
            echo "</tr>";
        }
        echo "</table>";
        echo "<p id='complete'>End of Assessment Questions</p>";
        echo "<hr>";
    }else {
        echo "<p id='complete'>No Questions in the database!</p>";
        echo json_encode($json);
    }
    if(isset($_POST["submit_questionnair_btn"])){
?>
```

Threat matrix code



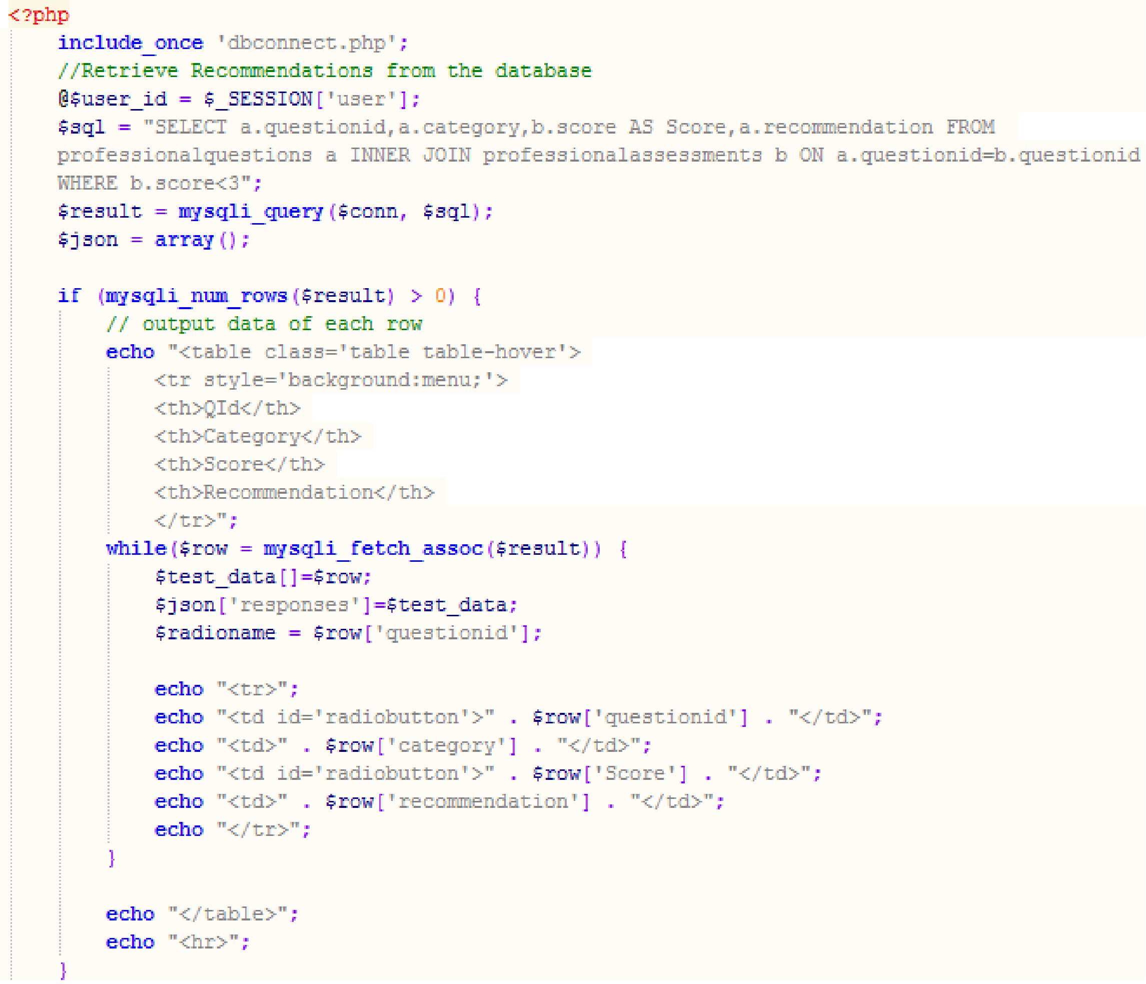
```
window.onload = function() {

var chart = new CanvasJS.Chart("chartContainer", {
    animationEnabled: true,
    title: {
        text: ""
    },
    toolTip: {
        shared: true
    },
    axisY: {
        title: "Likelihood of Attack",
        suffix: "%"
    },
    data: [{
        type: "stackedBar100",
        name: "Very Likely",
        yValueFormatString: "#,##0\"%\"",
        dataPoints: <?php echo json_encode($dataPoints1, JSON_NUMERIC_CHECK); ?>
    },{
        type: "stackedBar100",
        yValueFormatString: "#,##0\"%\"",
        name: "Likely",
        dataPoints: <?php echo json_encode($dataPoints2, JSON_NUMERIC_CHECK); ?>
    },{
        type: "stackedBar100",
        yValueFormatString: "#,##0\"%\"",
        name: "Possible",
        dataPoints: <?php echo json_encode($dataPoints3, JSON_NUMERIC_CHECK); ?>
    },{
        type: "stackedBar100",
        yValueFormatString: "#,##0\"%\"",
        name: "Unlikely",
        dataPoints: <?php echo json_encode($dataPoints4, JSON_NUMERIC_CHECK); ?>
    },{
        type: "stackedBar100",
        yValueFormatString: "#,##0\"%\"",
        name: "Very Unlikely",
        dataPoints: <?php echo json_encode($dataPoints5, JSON_NUMERIC_CHECK); ?>
    }]
```

User Scores Code



```
<?php
    include_once 'dbconnect.php';

    //Retrieve Recommendations from the database
    @$user_id = $_SESSION['user'];
    //$user_id = $_SESSION['usr_id'];
    $sql = "SELECT a.questionid,a.question,b.score AS Score,b.assessmentdate FROM userquestions a INNER JOIN userassessments b
    ON a.questionid=b.questionid WHERE userid=$user_id";
    //and assessmentdate>= CURDATE() ORDER BY a.questionid,c.category";

    $result = mysqli_query($conn,$sql);
    $json = array();

    if (mysqli_num_rows($result) > 0) {
        // output data of each row
        echo "<table class='table table-condensed .table-bordered table-hover'>
            <tr style='background:menu;'>
            <th>QId</th>
            <th>Question</th>
            <th>Score</th>
            <th>Assessment Date</th>
            </tr>";
        while($row = mysqli_fetch_assoc($result)) {
            $test_data[]=$row;
            $json['responses']=$test_data;
            $radioname = $row['questionid'];

            echo "<tr>";
            echo "<td id='radiobutton'>" . $row['questionid'] . "</td>";
            echo "<td>" . $row['question'] . "</td>";
            echo "<td id='radiobutton'>" . $row['Score'] . "</td>";
            echo "<td>" . $row['assessmentdate'] . "</td>";
            echo "</tr>";
        }

        echo "</table>";

        echo "<hr>";
    }
```

Recommendations Code



```
<?php
    include_once 'dbconnect.php';
    //Retrieve Recommendations from the database
    @$user_id = $_SESSION['user'];
    $sql = "SELECT a.questionid,a.category,b.score AS Score,a.recommendation FROM
    professionalquestions a INNER JOIN professionalassessments b ON a.questionid=b.questionid
    WHERE b.score<3";
    $result = mysqli_query($conn, $sql);
    $json = array();

    if (mysqli_num_rows($result) > 0) {
        // output data of each row
        echo "<table class='table table-hover'>
            <tr style='background:menu;'>
            <th>QId</th>
            <th>Category</th>
            <th>Score</th>
            <th>Recommendation</th>
            </tr>";
        while($row = mysqli_fetch_assoc($result)) {
            $test_data[]=$row;
            $json['responses']=$test_data;
            $radioname = $row['questionid'];

            echo "<tr>";
            echo "<td id='radiobutton'>" . $row['questionid'] . "</td>";
            echo "<td>" . $row['category'] . "</td>";
            echo "<td id='radiobutton'>" . $row['Score'] . "</td>";
            echo "<td>" . $row['recommendation'] . "</td>";
            echo "</tr>";
        }

        echo "</table>";
        echo "<hr>";
    }
```