2020

A Model for identifying vulnerabilities on critical infrastructures -case of cyber threats in Kenya

Maina, Simon Kuria
Faculty of Information Technology
Strathmore University

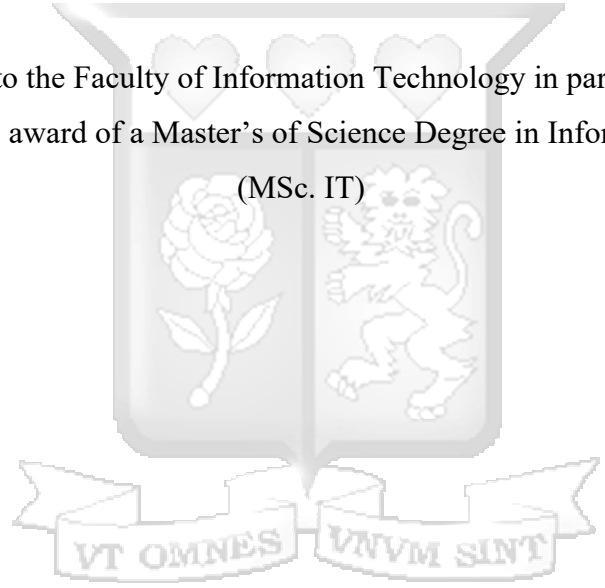
A MODEL FOR IDENTIFYING VULNERABILITIES ON CRITICAL INFRASTRUCTURES: CASE OF CYBER THREATS IN KENYA

BY

SIMON KURIA MAINA

050692

A Thesis submitted to the Faculty of Information Technology in partial fulfilment of the requirements for the award of a Master's of Science Degree in Information Technology (MSc. IT)



Declaration

I, Simon Kuria Maina, declare that this work has not been previously submitted and approved for the award of a degree by this or any other University. To the best of my knowledge and belief, this project dissertation contains no material previously published or written by another person except where due reference is made.

Student Name: Simon Kuria Maina

Sign: _____

Supervisor's Name: Dr. Vincent Omwenga

Sign: _____

Acknowledgement

I would like to express my sincere gratitude to persons who contributed by giving me insights and who spent their resources and time to enable me in forming the outline and strategy of executing this study. I would also like to thank my project supervisor Dr. Vincent Omwenga for the guidance in this field of the study and for most of his time taken to keenly analyze and supervise this project dissertation. I'm highly grateful for his invaluable insights to make this study a success.

Abstract

With advancement in technology, industry-focused technological systems have over time faced the challenge of attacks given their vulnerabilities resulting in denial of services and catastrophic operations for countries. This study focused at analysing the risk exposure on Kenya's Critical Information Infrastructure (CII). A model for identifying the vulnerabilities that critical infrastructures are exposed to by detecting anomalies in the set thresholds was developed. This study adopted the vulnerability system development lifecycle to develop the model. The model was developed following the Rapid Assessment Methodology and used the Common Vulnerability Scoring System (CVSS) to measure the severity of potential vulnerabilities against critical infrastructure. This allowed the model to prioritize responses and resources to remediate against the vulnerability identified. The study found that vulnerabilities pose a security threat on systems that are deemed critical and as such recommends that organisations should invest on vulnerability assessment tools. These will help them detect, remediate and monitor and evaluate vulnerabilities on CIIs.

Keywords: Critical Information Infrastructure, Critical Information Infrastructure Protection, Information Security, Vulnerabilities, Cybersecurity, Cyber threat, threat modelling.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ACRONYMS

ACL - Access Control List

CII - Critical Information Infrastructure

CIIP- Critical Information Infrastructure Protection

COTC - Commercial Over the Counter

DDoS - Distributed Denial of Service

DMZ- Demilitarized Zone

DNS - Domain Name Server

DoS - Denial of Service

DOS - Disk Operating System

IDS - Intrusion Detection System

IPS - Intrusion Prevention System

MMI - Man Machine Interface

NIC - Network Interface Card

NT - New Technology

RTDB - Real Time Database Manager

SCADA - Supervisory Control and Data Acquisition Systems

VMS -Virtual Memory System

Definition of Terms

Assets – These are individual targets in systems whose destruction would not endanger vital systems but could create local disaster or profoundly damage the Nation's morale or confidence. (Moteff & Parfomak, Critical Infrastructure and Key Assets: Definition and Identification, 2004).

Critical Information Infrastructure (CII) - Information and communications systems whose maintenance, reliability and safety are essential for the proper functioning of a country.

Critical Information Infrastructure Protection – This is the steps taken by government, enterprises and societies to keep secure those systems that are considered vital for the country's function and whose insecurity or vulnerability might cause great damage to the country.

Threats – These are occurrences that have the potential of causing damage to a network, information system, databases, etc.

Vulnerabilities – These are loopholes found within systems that give way for threats to occur when exploited by threat actors.

1. CHAPTER 1: INTRODUCTION

1.1. Introduction

The spread of internet and the revolution of information has spearheaded and made easier interdependencies of countries, economic sectors and other vital operations for the sustainability of nations at large. This has led to a great deal of data flowing through the internet with various degrees of protection and at the same time, vulnerabilities and threats experienced on the other hand of technology. Government institutions, private sector and businesses around the world agree that there is need to protect data from malicious activities (United States General Accounting Office, 2004).

To prevent these threats from creating destruction of critical information infrastructure of organizations, there has been a need to model solutions for the threats. However, the complications arising from the challenge of cross matching assets and system vulnerabilities has made critical infrastructure susceptible making these bodies face attacks and sometimes put security and the economy of a country at a risk. Legal instruments in various countries have also made it challenging to act upon malicious attackers of critical infrastructures (Tikk-Ringas, 2015) due to a lack of legal framework, standards and best practices in this sector thus contributing to furthering these attacks. This study outlined the existing cyber security conditions, the vulnerabilities that systems are exposed to and their impact, threat modelling and legal frameworks in cyber space and how Kenya can incorporate an efficient model to help mitigate these vulnerabilities.

1.2. Background to the study

Critical infrastructure, according to ISACA (2015), refers to "physical and virtual assets or facilities, whether owned by private or public entities, which are essential to the provision of vital services to Kenyans for their social and economic wellbeing, and which if destroyed, degraded or rendered unavailable, would impact on the social or economic wellbeing of the nation or affect Kenya's ability to conduct national defence and security." Cyber threat modelling is the process, which most organizations are adopting to mitigate threats. This process involves knowing how a system works, identifying the potential risks and threats that may arise through using the system, identifying potential attackers and profiling them, using their goals and methods for attacks made to the system (Shostack, 2014). The model then assists in identifying the possible solutions to these risks.

There is a distinct difference between critical information infrastructure and information infrastructure. Information infrastructures are the technical, social and political frameworks that encompass the people, technology, tools, and services used to facilitate the distributed, collaborative use of content over time and distance (Borgman, 2010, p. 19). Critical information infrastructure (CII), on the other hand, are information and communications systems whose maintenance, reliability and safety are essential for the proper functioning of a country. In cases where security of the systems is essential, an institution's transactions are well executed to achieve its goals (Republic of Estonia: Information System Authority, 2018). Researchers (Krass, 1991) and (Kim & Solomon, 2014) agree that where there is breach of security and a resultant attack on the system, the institution is in jeopardy and may lead to its collapse altogether.

Over the past two decades, advancements in technology and communications have made quite an impact in the functioning, operations and security practices of governments, business enterprises, research institutions, and defence and security establishments. Information systems are rapidly being incorporated in critical parts of society such as transportation, communication, health, agriculture, finance and other sectors of the economy (Kundishora, 2013). Kenya has, over the recent years, embarked on a strategic push to improve her infrastructure, both physical and digital. The resultant positive impact to the citizens includes faster access to government services through digital platforms such as e-Citizen, education provision through the Digital Learning Programme and a more informed society with the highest population internet penetration rate in Africa of 85% (Communications Authority of Kenya, 2018) which is due to its modern and robust telecommunications industry.

The modern Kenyan society relies upon numerous physical infrastructure that is dependent on technology such as energy production and transmission, telecommunication networks, banks and financial services, healthcare, manufacturing, among others that is very critical to the governance structure of the country. Proper functioning of these critical infrastructure is crucial to the social and economic well-being of Kenya. With time, due to globalization, these infrastructures have grown dependent on each other even across multiple countries. The United Nations General Assembly (UNGA), in its resolutions 58/199 and 64/211, recognizes the importance of information technology in socio-economic development, provision of necessary goods and services, business operations and the exchange of information for governments, businesses, other organisations and

individual users. The resolutions recognise the complexity of the network of critical information infrastructure components that exposes them to a growing number and wider variety of threats and vulnerabilities, hence raising new security concerns. The United Nations urged member states to examine CII, identify interdependencies and understand the vulnerabilities of the networks in use, the relative levels of threat faced by each sector and their management plans.

Despite the many advantages to technological advancement, there has been an equal measure threatening technology and systems (Naughton, 2016). It is in this regard that organizations have taken responsibility in protecting information in the various degrees that information falls, from malicious parties and threats that might collapse the technology in use and consequently the institutions relying on the technology. Today, the skill required to attack a system can be as simple as the use of an Open Source tool, knowledge freely available on the internet and malicious intent. The vulnerabilities of critical infrastructure and their dependence on information infrastructure make them an easy and obvious target for states as well as terrorists to disrupt critical services or functions they give. Successful attacks on CIIs can directly or indirectly cause mass casualties or have serious economic repercussions. In December 2017, it was reported that the Middle Eastern oil and gas petrochemical facility had undergone a safety systems shutdown as a result of a malware attack known as TRITON. For the first time, attackers successfully changed the programming logic of a SIS (Safety Instrumented Systems) controller. SIS systems are the last line of automated defence for a control network, and are designed to ensure a plant shuts down or changes its process so that no harm can come to people or the environment. The TRITON malware framework and many other malware frameworks discovered in the last two years are freely available on the Internet. Persons with basic knowledge on the malware do not struggle in finding it. The malware is also easily adapted by people with relatively low programming skills to create sophisticated attacks.

Apart from cyber-attacks, cyber warfare is another very real and possible outcome of CII sabotage. United States detonated a new kind of weapon, the atomic bomb in 1945. A little over 60 years later, they launched another completely different kind of weapon. Unlike the one in 1945, this was not a physical weapon, but a malicious computer virus that was capable of causing real-world, physical damage. This weapon would come to be known as Stuxnet. Stuxnet was the first publicly known cyber weapon in history to attack the ‘real world’. It was designed to hit the computers that

controlled Iran's nuclear enrichment facility, altering how the centrifuges worked hence causing them to fail. It brought with it a whole range of excitement and ideas for hackers to attack critical infrastructure by revealing the vulnerabilities available in critical information systems. Stuxnet made them a constant target as is evident in the subsequent cyber-attacks on critical infrastructure such as WannaCry (Public Hospitals), TRITON (Energy Plants) and Industroyer (Electricity substations).

Antivirus companies such as Symantec, Kaspersky, among others remain on the front line as an integral part of infrastructure security. They block majority of the standard attacks and curb the spread of malware, but they cannot guarantee complete protection. Eugene Kaspersky explicitly stated that "as we increasingly depend on technology as the backbone of our civilization, we need to ensure our critical infrastructure is built upon a robust architecture that is not only secure but also immune. If we do not adopt a security first approach, we will face a very uncertain future."

In Kenya, the government has realized the significant cases of fraudulent gaining of information through cyber-attacks and threats to her systems and those of businesses and other organizations in the country. According to the Kenya Computer Misuse and Cybercrimes Act, 2018, Critical Information Infrastructures are defined as "information systems, programs or data that support or perform a function with respect to a national critical infrastructure." There is need therefore to model a critical information infrastructure to protect this information to avoid such opportunists on the vulnerabilities of systems.

While cyber threat modelling has many approaches and frameworks, the backbone consists of profiling of the system in an abstract manner, profiling of potential attackers, including their goals and methods they may use to attack the system and gain information and finally, a catalogue of potential threats that may arise from the functionality of the system (Shostack, 2014). A technology system's success is usually measured by the time it offers the services it should render without at any point encountering denial of service and its effectiveness. However, the main challenge that organizations and governments run into is that software engineers are able to create systems that offer functionality but most times fail to incorporate the risks and threats' mitigation during creation. Most critical infrastructure is either based on or monitored and controlled by vulnerable ICT systems, making the information infrastructure become the focal point of CI protection policies in the 1990s (Moteff J. D., Critical Infrastructures: Background, Policy, and

Implementation, 2015). Today, the information infrastructure is still regarded as an easy and vulnerable entry point. This is due to the lack of control system within the infrastructure that can detect vulnerabilities (Cavelty, 2007). However, discovering the threat to CII remains difficult.

Governments have also taken up the role of formulating policy (SATRC Working Group on Policy and Regulations, 2012) to model critical information infrastructure as they are also targeted due to the amount of information they hold of their sectors especially its security and economic sectors and the proper functioning of the country in general. This is also in the realization that there are many private CII owners who are faced with crises on how to go about legal action on breach on the CIIs. There is need therefore for research to study the gap realized of the lack of visibility of vulnerabilities on CIIs and the diminished legal framework pertaining critical information infrastructure. This study sought to study the existing conditions of these vulnerabilities and lack of policy and designed a tool to mitigate the vulnerabilities and threats on CIIs.

1.3. Problem Statement

Similar to other countries with a robust ICT infrastructure, Kenya, now conducts its social, economic, political and security activities on the digital space that has effectively shown its advantages in making services easier, more efficient and effective. These activities have led to the growth of a steady critical infrastructure and their dependence on information infrastructure make them an easy and obvious target for other states as well as terrorists. This leads to disruption of critical services and directly or indirectly causing mass casualties or serious economic repercussions. In May, 2019, Safaricom's M-PESA platform experienced an outage across the country leading to a loss of millions of shillings, in most economic sectors, within two hours of the denial of services. Lack of knowledge by employees on how to stay safe on the internet in these organizations is another very common entry point into systems as was the case in the Foreign Affairs Ministry in Kenya where a phishing expedition helped attackers gain access to their systems where they stole passwords as well as confidential data from their systems. In order to avoid this, effective solutions and techniques to protect critical information infrastructure are needed.

Much of the world's core critical infrastructure is still using legacy technology while carrying out vital processes; thus leaving doors wide open to even the simplest forms of cyber-attacks. The

Kenya Information and Communications Act, 1998, mandates the Communications Authority of Kenya (CA) to develop a national cyber security management framework through the establishment of a national Computer Incident Response Team (CIRT). This is to help institutions that deal with critical infrastructure at all data protection levels report incidences and vulnerabilities of systems to help them mitigate against these reported issues. This, however, has been established to be a slow process into mitigating against risks and losses caused by vulnerabilities that are not easy to identify and hence could not be reported to the response team. By using legacy technology as well as putting little to no effort to secure and patch Critical Infrastructure systems, which is the case in Kenya, many critical systems are at risk of being exploited.

Furthermore, it is important to use products and IT solutions that employ a secure design. Companies, governments, businesses and any other bodies in charge of CIIs should determine what data is truly mission critical and make sure that robust defence measures are in place for these key assets. If these scenarios become our new reality, successful cyber-attacks launched on critical infrastructure could paralyze societies, countries and create chaos. According to the evidence and scenarios outlined, there was urgent need for a cyber-threat model or application for the critical information infrastructure of the critical information systems in Kenya to ensure effective, efficient and longevity of services given to its citizens and hence foster the country's national security and spearhead its economic growth. This study aimed to study these vulnerabilities of critical infrastructures, developed a tool that detected these vulnerabilities and helped create a model that could be used by the Kenyan legal framework to ensure critical information infrastructure is well protected.

1.4. Research Objectives

The main objective of this study was to develop a model for identifying vulnerabilities on Critical Infrastructures by analysing and detecting anomalies on the CII set thresholds by analysing the cyber threats.

Specific objectives of this study included:

1. To classify common characteristics and profiles of CII threats and vulnerabilities.

2. To determine the measure of vulnerabilities against assets of critical information infrastructure.
3. To assess the performance levels of existing applications and models in detecting CII vulnerabilities.
4. To develop and test a model for detection and analysis of vulnerabilities on CII.

1.5. Research Questions

1. What are the common characteristics and profiles of CII threats and vulnerabilities?
2. What is the measure of vulnerabilities against assets of critical information infrastructure?
3. How can performance levels of various models be measured in detecting vulnerabilities on CII?

1.6. Study Justification

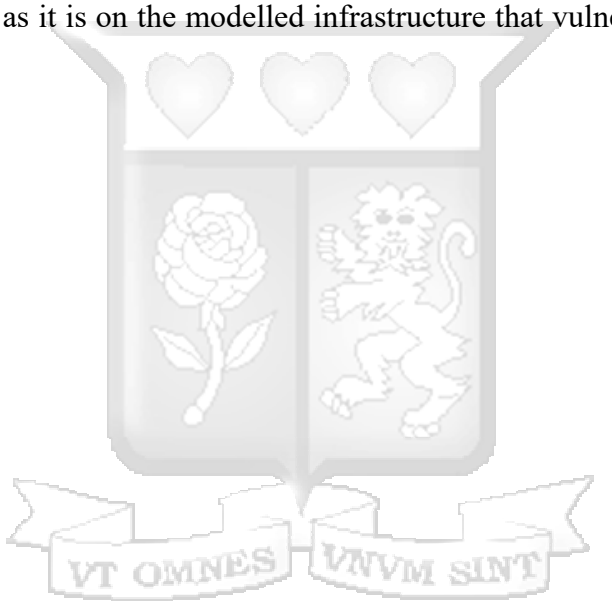
Technological advancement has led to an era where weapons are not just the typical atomic bomb, but also malware. Nations have the technological means as well as capital to conduct and sustain long-term operations, which include espionage, sabotage, data or credentials theft as well as execution and monitoring of attacks. Recently, terrorist organizations are alleged to be capable of conducting attacks on CII, with the ease of access to the professional skills available in the market. There was therefore a pressing need to come up with a comprehensive security model and policy to address the physical, legal, cyber and human aspects of cyber security. Many countries worldwide have realized how challenging it is to get involved in preventing and containing the attacks on critical infrastructure, while still maintaining a sense of resilience in the critical infrastructure and the corresponding information infrastructure.

Kenya's rapid modernization of both public and privately controlled critical infrastructure continuously faces evolving cyber threats as a result of technological advancements. Cyber threats exploit numerous vulnerabilities in the software and hardware design, human resources and physical systems of CII. This concern requires significant attention by governmental agencies, CII owners and citizenry as a whole. Without requisite legislation that can define the standards and measures for assessing cyber risks and threats, this study aimed to provide a base assessment of the risk exposure on Kenya's CII. This was to provide information on the gap that was lacking in the risk identification and risk management of vulnerabilities, cyber threats and attacks on critical systems hence mitigating them far ahead of the functionality of the system. This ensured effective

and efficient systems that do not run obsolete in a short time and most importantly offer services as required without exposing vulnerabilities easily to attackers thus safeguarding critical information of organizations, enterprises and governments enhancing reliability and sustainability.

1.7. Scope of Study

Given the many frameworks for models on critical information infrastructure that have been researched and documented, this study was limited to models that cover the risk analysis and mitigation aspect in relation to cyber threats on critical information in Kenya. This enabled the study to clearly outline the visibility of the threats and vulnerabilities on the CII and how it went about remedying them. The study focused more on critical information infrastructure than the information system itself as it is on the modelled infrastructure that vulnerabilities occur and are exposed to attackers.



2. CHAPTER 2: LITERATURE REVIEW

2.1. Introduction

As the world becomes more networked and more interdependent on information systems, more susceptibilities are encountered in the networks and systems. ICT in Kenya contributes to more than 10% of the GDP and the sector has the second largest share of the national budget after the education sector as per the 2018/2019 budget at 24% (The National Treasury, 2019). This has made the country the Silicon Valley of Africa due to its innovations that are highly used in both public and private entities. This is a significant contribution given the amount of business transactions that the sector carries out. It is therefore in this regard that the Kenyan government is putting effort in protecting critical information infrastructure to ensure security for the government, enterprises and individuals in the cyberspace. It is doing so by coming up with formulation of the Critical Infrastructure Policy, 2016 and Bill (ISACA, Kenya Chapter, 2016)

This chapter analysed critical information infrastructure, the element of criticality in CII, common characteristics and profiles of CII threats and vulnerabilities, measure of vulnerabilities against assets of critical information infrastructure, existing threat and vulnerability identification frameworks, methodologies and models among other aspects of CII.

2.2. Critical Information Infrastructure (CII)

For this paper to analyse and classify the characteristics and profiles of CII threats and vulnerabilities, there was need to first understand what CII is. The concept of infrastructure has over time evolved within policymakers and has become a concept of interest to various stakeholders. Infrastructure, for such a long time, is a term that referred to physical amenities like roads, hospitals, schools, etc. before it became of such great interest. Due to the nature of the public goods associated with this term, infrastructure has over time been understood as public goods and services (Torrisi, 2009). Conversely, in other countries, such as Britain or the US, private entrepreneur-built network utilities serving the public (Newbery, 2000).

Infrastructure as known to many made primary socio-economic conditions of a community ranked as good or bad depending on the state of those infrastructure. In recent years, however, it has been noted that infrastructure goes beyond these physical amenities (Henckel & McKibbin, 2017). It has become a policy concern for nations, businesses and individuals as a whole. This has therefore led to great importance of the context of infrastructure.

Today, with the heavy use of technology across sectors, more and more data and information is at stake. It is becoming increasingly important to protect information acquired through transactions and exchange across information systems. Some information systems tend to be more essential than others and as such make the system more vulnerable given the nature of information that they process (Revnivykh & Fedotov, 2016). The more essential information a system contains, the more vital the system is and hence their information infrastructure that makes this processes effective and efficient for the users require protection.

With time, information infrastructure has necessarily become an integral part of critical infrastructure of many nations across the world making critical infrastructure highly dependent on information technology i.e. the telephone network, internet and wireless networks, computers, networks, servers and storage systems (Moteff, Copeland, & Fischer, Critical Infrastructures: What Makes an Infrastructure Critical?, 2003). Therefore, the part of information infrastructure that is essential for the proper functioning of critical infrastructure is what is considered critical information infrastructure (Cavelty, 2007). Principally, CII is part of the critical infrastructure of a nation that includes components such as computers, software, the internet, satellites as well as fibre optics (Cavelty, 2007).

The African Union (AU) Convention on Cyber Security and Personal Data Protection under Article 1 outlines the concept of Critical Cyber/ICT Infrastructure as "the cyber infrastructure that is essential to vital services for public safety, economic stability, national security, international stability and for the sustainability and restoration of critical cyberspace" (African Union, 2014). While this convention does not specifically reference CII, the definition falls within the internationally accepted taxonomy of CIIs. Additionally, the International Telecommunication Union (ITU) defines critical infrastructures (CI) as the key systems, services and functions whose disruption or destruction would have a debilitating impact on public health and safety, commerce, and national security, or any combination of those matters (International Telecommunication Union, 2012). This definition closely mirrors the USA PATRIOT and Homeland Security Act of 2001 which as well defines "critical" infrastructure as systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.

In Kenya, there has been effort for the government to define what critical infrastructure is. Though it has been a slow progress, the National Cyber Security strategy describes CI as assets that are essential for the functioning of a society and economy (Ministry of Information, Communications and Technology, 2014). These assets may span from transportation systems to telecommunications infrastructure. The critical infrastructure community includes public and private owners and operators, and other entities with a role in securing the Nation's infrastructure. As outlined earlier, CII is all information systems, programs or data that supports or performs a function with respect to national critical infrastructure. (Computer Misuse and Cybercrimes Act No 5, 2018).

Kenya may be lagging behind in terms of autonomous critical infrastructure management but with the Kenya Vision 2030 in place, the Ministry of Information Communications and Technology set up a National ICT masterplan to provide direction towards attaining this cause. The document contains plans such as the e-government set up, national ICT infrastructure among other services. As a country, most critical information infrastructure is on the hands of private investments and telecommunication companies. This makes it even more demanding that the infrastructure is protected as the government and citizens heavily depend on their reliability and security. Some examples of critical information infrastructure in Kenya include telecommunications networks (Safaricom, Telkom, JTL etc.), air traffic control systems in the country's airports, railway control and scheduling as in the SGR, highway and traffic control systems, financial sectors such as banks and SACCOs and industrial control systems. To determine what makes an asset critical, a critical assessment must be made of it.

2.3. The Element and Variables of Criticality in CIIs

Critical assessment of an asset is basically the estimation of how important it is compared to other assets based on factors such as its purpose (Gheorghe, Masera, Weijnen, & Vries, 2006) and the extent to which systems, functions, facilities and resources are at risk if the said asset was to malfunction. The asset's importance to the economy, government as well as public safety must also be assessed.

John Sullivant describes the process of determining the criticality of an asset as four dimensional. The first dimension is that of "enterprise perspective" where the asset's importance to a business and its customers is of utmost value. Who does this asset serve directly? How much damage would the customers face if said asset were to malfunction? This makes the main element of criticality of the asset pertain the dependency of key functions or key business processes on the asset and the

difficulty in restoring its services in cases of damage or malfunction. The second dimension covers "vulnerability of the asset" and regards the obsoleteness of the asset and its access. This dimension seeks to understand whether the asset is indispensable or not and whether there could be alternative software or hardware to be used with it in case of its malfunction. Thirdly, the asset's "attractiveness to the adversary" determines its criticality since it gives away its values to its attackers. If the asset is highly attractive to attackers and is an easy target, then it makes it highly critical. This dimension seeks to identify the value of the asset as perceived by the attacker. Lastly, the "public reaction" dimension, which is hard to determine refers to when public safety is endangered. It shows that there is an adverse effect on a society or community if an asset were to be attacked and if it tends to lower the confidence of people on the said asset, it shows of how highly critical it is to the society. This dimension mostly covers the behaviour especially of the stock market and financial sector, issues of liability, etc. (Sullivant, 2007).

In determining what is critical, most countries use and build on the example of the first official publication of the United States of America on CI protection to equate critical infrastructure with the business sector of industries (President's Commission on Critical Infrastructure Protection, 1997) .

There are also other variables and parameters that have been used by researchers (Theoharidou, Kotzanikolaou, & Gritzalis, 2009) to determine the criticality of assets and infrastructure. These variables are important since they determine a system's criticality under certain circumstances, at a specific moment of use or failure, etc. Some of the most important variables include the degree of impact of a system's malfunction or failure, its ICT dependency, threshold time to restore services in case of a malfunction, redundancy and interdependency with other assets. The figure below shows the relationship of these five variables with the criticality of the assets.

The degree of impact is one variable of measuring criticality of an asset in CII. An asset is considered critical if its disruption, malfunction or unavailability could cause an immense amount of damage, disrupt operations of an entire facility (Riedman, 2016). This variable could be quantified in terms of percentage population affected, percentage of services disrupted or by the number of people affected by its malfunction. Impact could also be divided further into factors based on different CII definitions by different nations who value degree of physical damage rather than the social aspect, public health safety, economic and social well-being of its people.

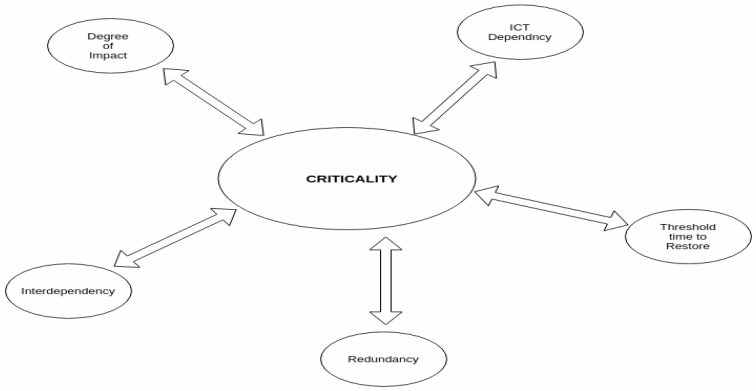


Figure Error! No text of specified style in document.**-1: Variables of Criticality. Adapted from Sharma, M., 2017**

Categorizing critical information infrastructure is important for any given institution or nation. However, there is no standard as to how to categorize and classify CII (European Union Agency for Network and Information Security, 2015). Most countries that have done the classification have therefore classified CII into sectors that are vital in the running of the countries' economy and sectors in security. The main sectors identified in most of the countries as having critical infrastructure include energy, information communication technology, transportation, food and agriculture, health, water, finance and banking, state and administration. Most of these sectors, from research indicate that they have to work interdependently to enhance effectiveness and a reliable environment for the economy and security of the countries. In the context of CII, interdependency can be defined as "a bidirectional relationship between two infrastructures through which the state of each infrastructure influences the state of the other (Rinaldi, Peerenboom, & Terrence, 2001)."

Given the classification of these critical information infrastructures, there is a high chance of collaboration between them to enhance development and optimum use of resources. This results in interdependence of these critical infrastructures. Interdependency is perhaps the most crucial and complex aspect of critical information infrastructure protection. Previous research (Bloomfield, Popov, Salako, Stankovic, & Wright, 2017), (Tøndel, Foros, Kilskar, Hokstad, & Jaatun, 2018) shows that assets with a lot of interdependence seem to be quite a target naturally because attackers can not only cause their disruption but also that of their interdependencies.

Interdependencies are one of the greatest weaknesses of modern infrastructure systems, as they significantly increase the vulnerability of corresponding infrastructure giving rise to multiple access channels for attackers from one asset to another (Velasquez, 2016). The electricity blackout in August 2003 in the United States and Canada illustrated the interdependencies between electricity and other elements of the energy market such as oil refining and pipelines, as well as communications, drinking water supplies, etc. which almost collapsed the water, health and energy sectors of the two countries (Moteff J. D., Critical Infrastructures: Background, Policy, and Implementation , 2015).

2.4. Profile and Characteristics of Vulnerabilities and Threats in CII

The International Journal for Information Security Research (IJSR, 2014) defines a cyber-threat as a potential malicious attempt to exploit vulnerabilities in critical information infrastructure in order to infiltrate or disrupt them. This is done with the aim of stealing, corrupting, destroying or making information unavailable to users. According to the National Institute of Standards and Technology (National Institute of Standards and Technology, 2018), cybersecurity threats exploit the increased complexity and connectivity of critical infrastructure systems, placing a nation's security, economy, public safety and health at risk. A vulnerability, on the hand is a bug, flaw, weakness or exposure of a system or a protection mechanism that exposes systems to cyberattacks (Whitman & Mattord, 2012). These vulnerabilities, if exploited, may lead to harm or loss for a community, business or country (Pfleeger, 1997).

2.4.1. Profile of Threats in CII

At such a time as this when the world is at such great heights in regard to technology, it is unfortunate that information infrastructure, which is the driving force of technology, is still regarded as an easy and vulnerable entry point to critical infrastructure. Many scientists are very fixated on creating the next big thing but forget that security of these creations is quite paramount. The spectrum of potential attackers to CII ranges from the amateurs following tutorials online all the way to expert hackers, all with different motives. This has resulted in profiling of threats with regard to the nature of external and internal threats, where the attacks originate, and the likelihood of the threat occurring. Threats on CII can originate from various sources including natural threats like floods and earthquakes, environmental threats like pollution, and human threat which is the most common threat on CII.

Human Threat

Human threats include all actors who maliciously try to gain access to information infrastructure with the intent to cause harm or damage. The human element to CII insecurity can classified into the following categories:

The inside man: This could be an employee of the company, a service provider or even a business partner within the organisation who has enough privileges, possesses credentials or security clearance within the organisation to access and sabotage CII. These actors' motives are normally fuelled either by monetary gain, greed, jealousy or ideological motivation. There are however, some insiders who are completely unaware of their role in fuelling attacks. Such insiders could be compromised victims or careless users who click on anything online. Such users are prone to phishing and social engineering attacks.

Conspiracy: This happens when an outsider colludes with an insider to execute an attack. The insider is expected to share credentials and other useful information that will help the outsider gain access. Most of the work is done off-site. In some cases, also, the insider is coerced into unconsciously or unwillingly share information

Outsider: This is a person who is completely not associated with the organisation being targeted. This attacker conducts the operation without any inside information relying solely on his skills and publicly available information. Motivation to such attackers range from monetary gain, hacktivism or as a professional service to another party.

Terrorists: They can be local to the country's infrastructure under attack or acting on behalf of another state. The most common motivation especially among the youth they recruit is radicalization as is the case with Somali youth enrolled into Al-Shabab which is the terrorist group associated with Kenyan terrorist attacks. Some of these groups have access to sophisticated human resources possessing good working knowledge of computers, networks and programming. As a matter of fact, some of the groups such as the Islamic State of Iraq and Syria (ISIS) and Lashkar-e-Taiba are known to have developed their own secure communication applications for smartphones. (Munish, 2016)

2.4.2. Characteristics of Vulnerabilities in CII

The need and struggle towards automation of systems alongside technological development has made the ability to incorporate safety features such as prevention and detection of system vulnerabilities rather difficult in critical infrastructure systems. Vulnerabilities created by these

systems not only affect utility services but also databases and systems that maintain a variety of sensitive and confidential information (Moteff, Copeland, & Fischer, Critical Infrastructures: What Makes an Infrastructure Critical?, 2003). As earlier outlined, most countries have encountered vulnerabilities in their systems especially in the security and economic dockets. These vulnerabilities have been exploited through human threats like terrorism, hacking into the financial sectors of countries and other critical sectors like water and energy.

In Kenya, many of the critical infrastructures are vulnerable to natural threats especially bad weather which has been quite frequent in the recent years leading to damage of infrastructure, loss of services, etc. Such occurrences can be deliberately replicated by attackers through the information infrastructure that serves these critical infrastructures. CII has become especially targeted by hackers, criminals, state actors and even terrorists. The main tools used to attack critical systems are malware (computer viruses, worms, trojans) that modify and destroy information or make the computer systems inaccessible as in the case of ransomware. Other tools eavesdrop on information exchanged between computers, others modify the normal function of the computer network while others block access to its services and are widely used for destructive purposes. These automated tools allow intrusions from remote systems to be done within a few seconds which makes Internet attacks easy to launch and increasingly hard to trace. Some common characteristics of vulnerabilities on Critical infrastructure are discussed as follows.

2.4.3. Software Vulnerabilities

Software vulnerabilities make up majority of all reported security incidents. They are security-related bugs that exist in software and can be exploited by an attacker to perform actions it is not supposed to. Since they are so common, a great deal of research has been done on software vulnerability and tools developed to detect vulnerabilities or their exploitation, some of which are open source.

(a) Unpatched systems

Unpatched systems are programs/ systems for which a patch -software that fixes a flaw in a system- has not been applied or could be unavailable. Systems go through several upgrades and development cycles in the course of their life cycle, even after they have been dispatched to users. When a vulnerability is discovered or published, it is required of the vendor to provide a patch for that bug as soon as possible. Unpatched systems pose great risk to their owners especially those who have their vulnerable CII exposed to the internet due to inappropriate network configurations.

Lack of patches, is a major risk in information security mainly because the "need for patching" means that the bug is known to exist therefore giving attackers an easy way in.

(b) Lack of input validation

This is when an attacker intentionally sends unusual input with an aim of "confusing" the application with something it does not expect or understand. This will lead to parts of the system receiving unintended input causing an altered flow of information, arbitrary control of a resource or arbitrary code execution.

(c) Buffer overflow

This is caused by improper management of memory by the software developers. This attack is executed by passing as much data as possible into an input field, causing data to overflow into adjacent storage which causes the application to crash. To avoid this, a developer should enable "bounds checking"

2.4.4. Password vulnerabilities

(a) Default passwords

Often, for testing purposes, developers have inbuilt passwords set on a system/software. When testing is complete, this password should be deleted/disabled before the system is rolled out to the public. Often times, this is not the case unfortunately and attackers know this and take advantage of this situation, making systems susceptible to any cyber threats thrown at them by said attackers.

(b) Password policies

Password policies are rules set by the administrative unit of an organisation, in this case ICT, to help increase the level of security of their systems. They define when passwords must be used, how strong they must be, and how they must be maintained. Without a password policy, systems might not have appropriate password controls, making unauthorized access to systems more likely. Many organisations do not enforce strong password policies to protect their users which has led to an increase in the number of vulnerable systems.

Good password policies should consider:

1. Timeouts and screen locking to alleviate opportunism on an unattended desktop
2. Password expiration and denial to use old passwords to reduce the use of compromised passwords.
3. Measures to ensure a strong password is used; ensure both uppercase and lowercase letters as well as spaces, numbers and special characters.

4. Secure password transmission to avoid password capture in the case of remote systems.
5. Use of single sign-on and local password management using for example active directory to manage password policies.

(c) No password

At no point in time should users be allowed to log in to their systems without passwords. Although this vulnerability is rare, some organisations still do not disable the "no password login" feature for its users making some systems in it susceptible to intruders/attackers.

2.4.5. Network protocol vulnerabilities

a) Weak network security architecture

The network infrastructure environment of CII is often being developed and modified based on business and operational requirements, while barely considering the potential security impacts of these configurations. Over time, security gaps may have been unintentionally introduced within particular parts of the infrastructure. If not amended, these gaps may present backdoors into the CII.

b) Improper firewall configurations.

Firewalls, when improperly configured, could allow unauthorized data to be passed between networks that shouldn't be able to communicate with each other for example corporate network and control systems network. This presents a loophole that could allow an attacker to move from a compromised computer on the corporate network to for example a SCADA network that should have its own segregated DMZ network. This way malware can be spread between networks and sensitive data can be exposed to espionage activities.

c) Lack of data flow controls

Data flow controls, such as access control lists (ACL), are needed to restrict which systems can directly access network devices. Generally, only authorized personnel should be able to access CII devices directly. Data flow controls should ensure that other systems cannot directly access the infrastructure.

d) Lack of IDS/IPS

Intruders can capture, modify, delete data or incorrectly execute control commands making systems/ services unavailable to its users. IDS/IPS software may stop or prevent various types of attacks, including DoS attacks, and also identify attacked internal hosts, such as those infected

with worms. IDS/IPS software must be tested prior to deployment to determine that it does not compromise normal operation of the CII.

Cyber threats on CIIs are basically potential security threats that could exploit vulnerabilities in software or hardware design posed on them by means of the cyberspace. These cyber threats to CII, are perpetrated by various entities ranging from multinational APT's, national hacktivists, criminal hackers and script kiddies. They may be categorized as cyber espionage, cybercrime, cyber warfare and cyber terrorism depending on the actor and intent.

2.5. Measure of Assets versus Vulnerabilities

The National Strategy for Physical Infrastructure Protection defines key assets as "individual targets whose destruction would not endanger vital systems but could create local disaster or profoundly damage the Nation's morale or confidence." (Moteff & Parfomak, Critical Infrastructure and Key Assets: Definition and Identification, 2004). Most countries took up this definition and as such, key assets have been termed to be national heritage or that which unites a country but its destruction could bring losses and huge economical damage to the country. Key assets also include individual or localized facilities that deserve special protection because of their destructive potential or their value to the local community. Assets have therefore been prioritized according to the critical sectors of a nation, business or community.

According to (Busuttil & Warren, 2006), asset identification is an important stage for any critical infrastructure. The asset list contains entries of all assets relevant to the infrastructure and the system's processes and procedures which are underlined to be vital. All assets identified should then be coded into categories Software, Hardware, Data, Administrative, Communications, Human Resources and Physical (Nosworthy, 2000). Since it is not easy to categorize all the assets, priority should be given to the most critical and depending on the scope of the CII. Inevitably, categorization of assets shows that there are many interdependencies amongst the assets and as such, make the systems even more prone to vulnerabilities. Critical information infrastructure is made up of quite a few assets therefore possible entry/attack points are quite a number. A few of them include network infrastructure; routers, servers (DNS), switches; satellite network communication systems; web portals; SCADA systems and databases. Due to the importance of assets in any CII, the proposed model will be developed in a manner that automatically identifies assets on CII to enable prioritization of vulnerabilities detected on them, if any, and resolve the matter of security as soon as they are detected.

2.6. Existing tools for vulnerability detection

Cyber ecosystems are overwhelmingly having to deal with new threats and attacks with more advancements in technology and information systems. Consequently, vulnerability detection has become a core element that needs to be incorporated in the security of every system. This has shifted vulnerability detection from a theoretical perspective to a globally recognized standard in the quest to solve instances of cyber threats and attacks. To achieve these solutions, studies have been carried out to show the kind of vulnerability detection tools that are required for different organizations given the nature of their functions and systems and rise of new threats to the information infrastructure. Some of the most common tools for vulnerability detection of critical systems and infrastructure are discussed below.

2.6.1. Open VAS

The Open Vulnerability Assessment Scanner (OpenVAS) is an open source tool used to scan for vulnerabilities on networks and web browsers. This tool was developed by Greenbone Networks in 2009. According to (GmbH, 2010), OpenVAS is a scanner that has over 50,000 vulnerability tests and has a vulnerability management commercial product.

This tool incorporates the use of client-server architecture over SSL and is a remote scanner hence it does not have to be configured on a target for it to test for vulnerabilities. The scanner executes network vulnerability tests (NVT) which are updated regularly using the NVT feeds. The OpenVAS manager gives the vulnerability scanned and the management aspect of the vulnerability. The manager controls the database for central storage. The OpenVAS administrator is a full service daemon whose task is user management and feed management. Figure 2-2 below shows the system architecture for OpenVAS.

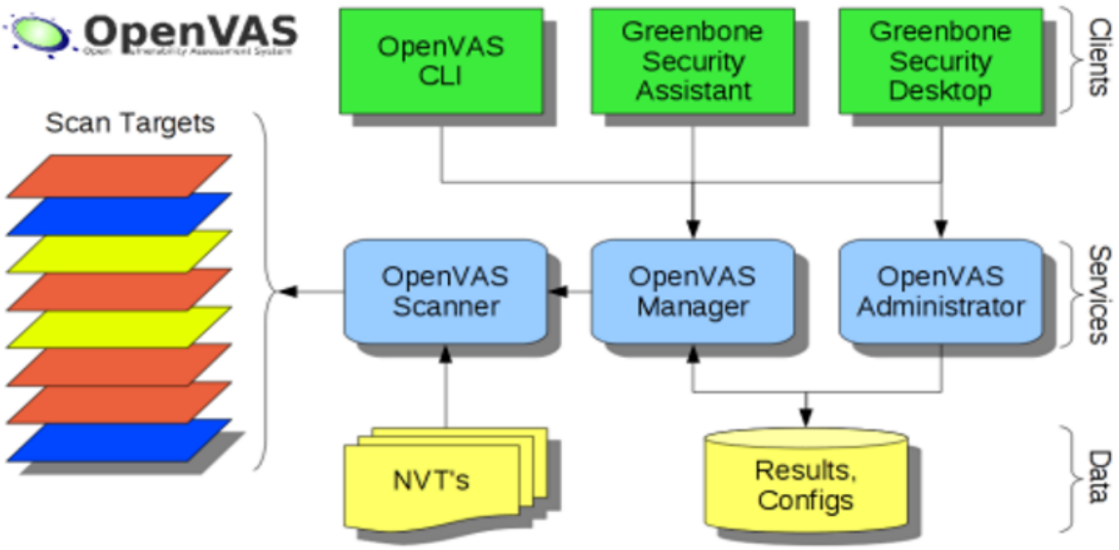


Figure Error! No text of specified style in document.**-2: OpenVAS Architecture (Adapted from Jhala, 2014)**

2.6.2. Nessus

Nessus is a vulnerability scanner that grades vulnerabilities present in the remote host. Nessus undertakes internal (scanning of hosts with a particular router) and external (remote) scanning of the vulnerabilities. Nessus also provides for testing web applications. Scanning can be done at the first instance or a template created and launched to be run against that host (Bairwa, Mewara, & Gajrani, 2014). Once a scan is run successfully, results reports are generated and classified by host. These reports are used to identify the vulnerabilities and fix them accordingly. Nessus also incorporates iterative network evaluations between scans. Just like OpenVAS, Nessus is based on client–server architecture where each session is controlled by the client and the test is run on the server side.

2.7. National Perspectives on CIIP

A comparison of conceptualization and understanding CIIP in various countries showed that the perception CIIP varied considerably (Wigert & Dunn, 2003). There was a lack of distinction between CIP and CIIP in many instances and both concepts were used interchangeably and randomly. This shows that the understanding of criticality of infrastructure is still a discipline that

is in progress in discussions in most countries. This subject is still being shaped as a policy field and there is need for definitions and conceptual frameworks that need to be found.

Given the nature of interdependencies between sectors, enterprises and governments, information has been at the centrepiece of both the governments' and the private sectors' efforts over the past several years to protect critical information systems (National Academy of Sciences, 2003). There have been vital questions about whom the information belongs, who should share it, when, how, why and with whom. The private sector especially, has raised concerned over the low progress due to the lack of clarity regarding benefits and liabilities involved in sharing of this information between sectors and governments. One of the most cited reasons why there is ambiguity is due to the revelation of weaknesses and vulnerabilities that erode consumer confidence and invite attackers to the systems.

Overcoming these concerns requires an informed position on the existing legal framework—an imperfect understanding of the law is both excuse and explanation for some observed limits to sharing. Most countries have invested in coming up with robust legal frameworks to help regulate the cyberspace. It is however worthy to note that the legal space has been marred with ambiguities that have contributed to this low progress on how to deal with the liabilities associated with the protection of critical information infrastructure.

2.7.1. CIIP in the US

CIIP in the United States was spearheaded by the Presidential Commission on Critical Infrastructure Protection (PCCIP), set up by former US president Bill Clinton in 1996, and to some extent by the preparations for anticipated problems on the threshold of the year 2000. The United States government facilitated the formation of the National Infrastructure Simulation and Analysis Centre (NISAC) by the United States Patriotic Act 2001 and was incepted into the department of Homeland and Security. The NISAC conducts modelling, simulation, and analysis of the nation's critical infrastructures. NISAC analysts assess critical infrastructure risk, vulnerability, interdependencies, and event consequences (Department of Homeland Security, 2016).

The US government has made enormous effort in trying to come up with proper strategic and legislation requirements to help in protecting assets of CII. The legislation that the government has put in place has however seen a rise in various task forces and commissions in trying to prioritize the protection of critical infrastructure. For instance, at the federal level, legal acts empowering strategic CIIP efforts are the Executive Orders of the President (also called Presidential directives),

the first of which was issued in 1998 (U.S. White House, 1998). This directive acknowledged certain assets of infrastructure at the national level as critical for both the country's economy and security, laid down a process to safe keep and laid the foundational requirements for a public-private partnership framework. The Directive, updated in 2003, elaborated on provisions to identify, prioritize, and protect critical infrastructure (U.S. White House, 2003). Since 2013, Executive Order 13636, Improving Critical Infrastructure Cybersecurity, and the Presidential Policy Directive on Critical Infrastructure Security and Resilience (PPD-21) have governed the CIIP framework of the United States (U.S. White House, 2013). In 2002, the United States also adopted legislation reorganizing and centralizing security functions at the federal level and aiming to meet existing threats and challenges, the Homeland Security Act (HSA). This act leads the coordination and protection of critical infrastructure. HSA also facilitated the Critical Infrastructure Information Act 2002 (CII Act), which regulates information exchange between critical infrastructure operators and public sector agencies.

At the government level, the US considers protection of CII a shared responsibility among the federal and SLTT entities along with public and private owners of these infrastructures. At the sector level, CIIP mandate is with the SSAs who have institutional knowledge and expertise about the sector, possess familiarity and relationships among the sector actors, and thus also play a critical role in maintaining partnerships and dialoguing with the critical infrastructure operators.

Due to these many governing bodies tasked with the protection of CII, it has become complex for the US to effectively and efficiently protect its CII due to the many bodies that have come up with different legislation and regulation for CII protection. It is therefore worthy to note that there is need for clarity in the regulation aspect to avoid ambiguities that come with many bodies regulating the same aspect of protection. There is need for clarity and use of one CIIP policy and framework which other governing bodies can rely upon to regulate the sectors with critical infrastructure.

2.7.2. CIIP in Malaysia

Like many countries, Malaysia considers CIIP important and essential for a prosperous e-economy and e-society and as such is a national security issue. According to ITU, the Malaysian government determined that critical national information infrastructures were likely to become attractive targets especially for terrorist activities (Hashim, 2009). In January 1997, Malaysia Computer Emergency Response Team (MyCERT) was formed and started its full operation on March 1, 1997. The entity formed as part of the government's approach to protect the country's CII provides

a point of reference for the Internet community in Malaysia to deal with computer security incidents. Later in 2009, the Cyber Threat Research Centre was formed to help in analysing malware and computer security threats.

Malaysia has made great progress in its legislation to protect critical infrastructure. In 2005, MOSTI formulated the National Cyber Security Policy and saw its adoption and implementation in 2006. The objectives of this policy were to address the risks that were associated with the critical national information infrastructure, ensure that these infrastructures were protected to levels commensurate with the risks and to finally develop and establish a series of frameworks to help in protection of CII.

This implemented policy saw the enforcement of a proper governance structure to spearhead the cyberspace protection. At the bottom was the National Cyber Security Working Group that received reports about incidents and threats, this was managed by the National Cyber Security Coordination Committee and the National Cyber Security Advisory Committee. All these committees report to the National IT council (Hashim, 2009).

Regulation and legislation are made by the Cyber Law Review of Malaysia and this helps in identification of risks and concerns in the cyberspace environment, assessing of the legislation in place and how it helps keep the cyberspace secure and finally, if need be, amend the current legislation and recommend thee amendments.

Malaysia is among the best three countries according to the ranking by Global Cyber Security Index (GCI). Global Cyber security Index (GCI) is an ITU-ABI research joint project to rank the cyber security capabilities of nation states (ITU, 2014). It was also ranked among the best countries in Technical Performance Index of the GCI. This shows that Malaysia's model around legislation and collaborations between the government, private owners of critical infrastructure and the people is a good example of a working model.

2.7.3. CIIP in South Africa

Africa in general has embraced an evolving era of the internet and use of computing power by the governments and businesses. In South Africa, there has been a major evolution of two eras. The first from 1995 to 2005 that saw the country the first decade of commercial internet. Curiosity was high and national security was stable and not threatened. The second phase however saw the second decade of commercial internet where most adversary attacks were reported and recognized as a threat to the nation's security and economy. It is within this second evolution that the country

put effort in coming up with regulations to help protect the various sectors that were identified to be critical to the country.

In 2015, the legislature passed the critical infrastructure protection bill. This bill outlines that it will provide for the identification and declaration of infrastructure as critical infrastructure; to provide for guidelines and factors to be taken into account to ensure transparent identification and declaration of critical infrastructure; to provide for measures to be put in place for the protection, safeguarding and resilience of critical infrastructure; to provide for the establishment of the Critical Infrastructure Council and its functions; the administration of the Act under the control of the National Commissioner as well as the functions of the National Commissioner in relation to the Act; ; to provide for the establishment of committees and their functions; to provide for the designation and functions of inspectors; to provide for the powers and duties of persons in control of critical infrastructure; to provide for reporting obligations; to provide for transitional arrangements; to repeal the National Key Points Act, 1980 (Act No. 102 of 1980) (Republic of South Africa, 2015)

The critical information infrastructure protection report of 2016 (Wolfpack Information Risk, 2016) showed that 35% industrial control systems rely on external audit to detect vulnerabilities in their systems, 81% do not have a "red team" to identify potential attack scenarios, 50% have not established risk management processes, 25% lack technical audits, 50% have outdated backups and disaster recovery plans while 76% have not established a full time monitoring capability. These statistics are worrying as they put most of the identified critical infrastructure at risk and may cause a great negative impact on the country as a whole. There is therefore need for implementation and adoption of proper legal structures and regulation to enhance protection of these infrastructures.

2.7.4. CIIP in Kenya

As Kenya matures into an information society, the nation faces an increasingly evolving cyber threat landscape. The Government of Kenya reported that there was exploitation on ICT vulnerabilities in Kenya. While these actors seek to illicitly access, alter, disrupt, or destroy sensitive personal, business, and government information, the country faces a struggle to evolve the means of protecting information in order to counter threats.

The National Cybersecurity Strategy stipulates that the Kenyan government recognizes the need to improve its cybersecurity posture. This is evident through the establishment of the Kenya

Information and Communications ACT, CAP 411A as amended by The Kenya Information and Communication (Amendment) ACT, 2014; the formation of the National Kenya Computer Incident Response Team Coordination Centre (KE-CIRT/CC), and the establishment of the National Certification Authority Framework, which provides a foundation for public key infrastructure implementation and partnership with regional and international cybersecurity bodies and forums including the International Telecommunications Union (ITU) and the East Africa Communications Organization (EACO).

While these activities and initiatives will help the Kenyan government evolve its cybersecurity posture, overall, the country's cybersecurity posture is still relatively immature in the face of the growing complexity and sophistication of cyber threats. There is therefore need for the government, businesses and individuals to help mature this posture by providing a strategic cybersecurity direction for the government with accompanying implementation actions to secure the nation's critical cyber infrastructure against existing and emerging threats.

2.8. Critique of Literature Review and Research Gap

Critical information is important for any government, business or community. Automation and technological advancement of systems that handle this critical information have resulted to complex systems and infrastructure supporting them to require protection. Literature revealed that studies have been done by institutions, governments and individuals to see how best to improve and safeguard security of these critical information infrastructures. Most scholars and governments agree that vulnerabilities of systems are best detected on systems through conducting regular risk assessments on the systems.

From past research, scholars agreed that the various tools that have been developed are a good start to providing security on critical infrastructure. For the OpenVAS tool for instance, being free and open source makes it easier for organizations to access a tool that is good enough to prevent critical information from being violated. The tool is easily configured and has a high common vulnerabilities and exposures (CVEs) and provides for a detailed documentation and detailed tutorials on how to implement it. The fact that most people can contribute towards its upgrade continuously is also an advantage as it helps in fixing several problems encountered from various persons making it more authentic to use. However, when compared to Nessus, OpenVAS has less CVEs making Nessus more a more trusted tool. This implies that the tool would easily miss some vulnerabilities on a system.

Nessus, on the other hand, being a commercial tool has a wide database of vulnerabilities thus making it more trusted. It also comes with customer support and professionalism in case clients need help. The tool is simple to use and productive. Nessus offers real time data visibility as vulnerabilities are detected on systems and takes less time to update these vulnerabilities on its database. It is important to however note that the cost of Nessus is very high locking out organizations with critical information who cannot afford to get the commercial tool. The complexity of the tool also requires expertise to use the tool's full potential and gain best results.

In Kenya, it is worthy to note that businesses and communities do not have a clear methodology that is able to detect vulnerabilities effectively and efficiently before an attack is made on them. In Kenya and Africa in general, cybersecurity is still a new concept and as such there is still a struggle in implementation of proper legal structures and modelling of critical information infrastructures to enable secure these systems and critical information. This study therefore sought to develop a tool that would help Kenya's businesses, communities and government to secure their critical information by detecting and assessing vulnerabilities on their systems and help in fixing them. The tool would also aid policy makers in the formulation of policy that would be adopted and implemented to help strengthen and secure the critical information infrastructure in the country.

2.9. Conceptual Framework

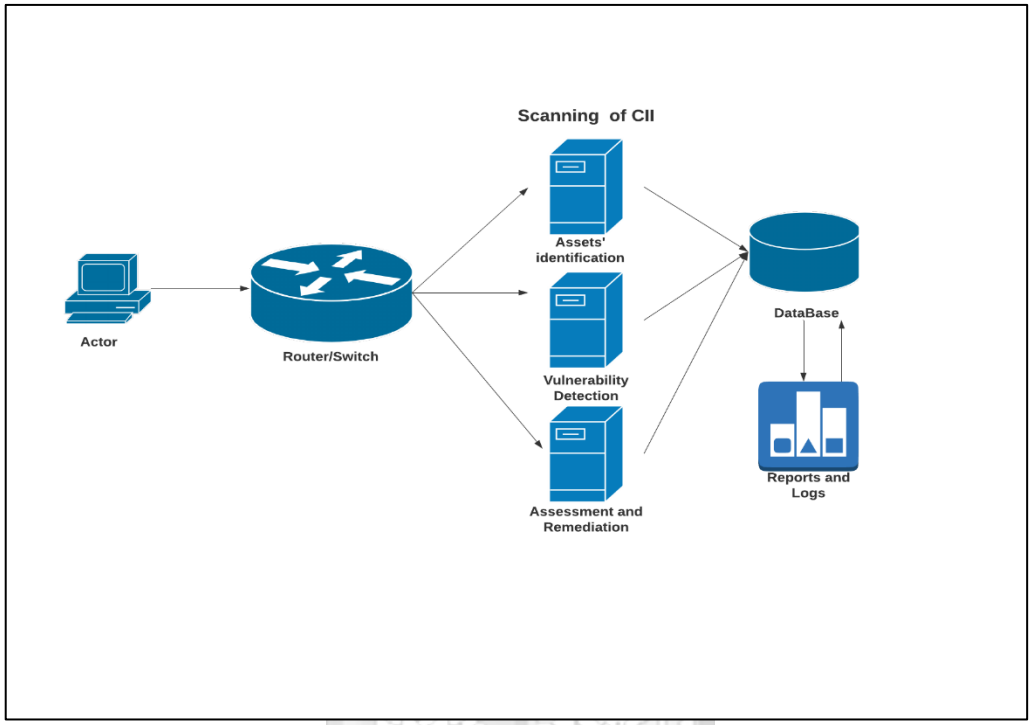


Figure Error! No text of specified style in document.**-3: Conceptual framework**

The conceptual framework presented in figure 2-3 illustrates the solution that this study sought to achieve. Given the existing tools for vulnerability detection that were discussed earlier, the main component that stood out is that of the client-server. The solution adopted this technology as well. However, for better reliability, the risk assessment and remediation component needed to be included in the system. This ensured that once assets and vulnerabilities were identified, the system automatically ranked the vulnerabilities against the assets in which they were identified. Depending on the nature of the vulnerability, the vulnerabilities were either fixed automatically or an alert message sent to the system administrator to resolve the issue. The reports and logs module was used to update the assets' and vulnerabilities' database to avoid duplication and helped to maintain accuracy and reliability. This conceptual framework was therefore based on the theoretical frameworks studied in the literature review with an additional module that filled the gap of the literature studied.

3. CHAPTER THREE: METHODOLOGY

3.1. Introduction

This chapter presents the methodological approaches that were employed in respect to the system analysis, system development, system design and the deliverables of the system. The chapter details vulnerabilities and the threat they pose on CII, the increased interdependence among infrastructure, need for automation and ultimately how to mitigate these vulnerabilities on CII.

This study adapted a mixed risk oriented cyber threat modelling methodology. This methodology followed the basic vulnerability assessment methodology (VAM) to detect and identify vulnerabilities in the system CII, if any. This made it a unique wholesome oriented methodology that identified possible vulnerabilities, classified them and did a proper analysis and possible mitigation while at the same time focusing on the objectives of the organizations that should be offered by the information system.

3.2 Research Design

The research in this study entailed the analysis of both qualitative and quantitative data. The study primarily studied relevant literature that was used for qualitative analysis. Quantitative data was collected by the developed model to fill the literature knowledge gap and answer the research questions outlined in Chapter 1. According to Bryman (2012), quantitative research entails collecting primary data to demonstrate a relationship between theory and reality through deductive analysis with an objectivist perspective. Qualitative research, on the other hand, entails an inductive approach with a subjectivist perspective in line with past research findings. The primary data that was collected through experiments set up by this model aided the analysis of the effectiveness of the model and compared it with other studies to determine whether it met its research objectives.

3.3 System Development Methodology

This is the way of studying a system with an eye of solving its problems using a specific method that has been identified by studying related literature. This study took on the Rapid Application Development (RAD) methodology that was decomposed into stages of developing a vulnerability detection model as studied by Kritikos et.al (2019) and shown in figure 3-1 below. This methodology was also used by the study since it well supports the system architecture adopted.

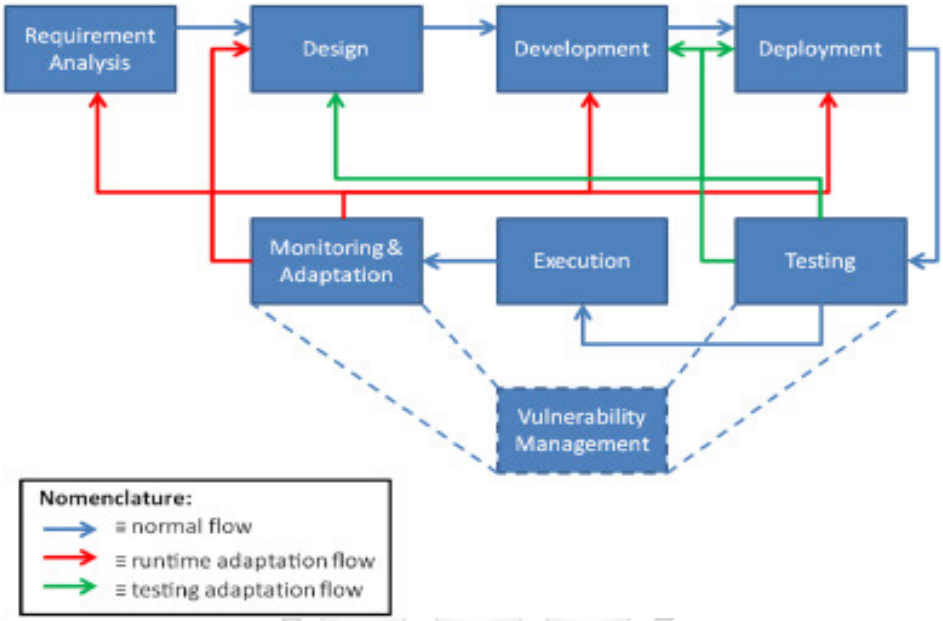


Figure Error! No text of specified style in document.**-4:The Vulnerability system development lifecycle (adapted from Kritikos et.al, 2019)**

According to (Coleman & Verbruggen, 1998), the output of software applications can be of good quality once the software process under the RAD methodology is defined. The RAD methodology has four main phases. The requirements planning is the first stage where the problem is identified, its needs assessment done and the project scope identified and outlined by the users, managers and I.T. staff who will interact with the software. With the study's methodology, this fell under the requirements' analysis phase. Prior research (Martin Maguire & Nigel Bevan, 2002) showed that getting to comprehend user requirements is a vital part of the system's development and is always critical to the achievement of good interactive systems. Specifying requirements is not easy hence classifying them according to the needs assessment of the problem is necessary. The researcher, during the study, identified and documented assets of information systems. This allowed the study to detail and profile the system in its information architecture and critical infrastructure. Possible threats and vulnerabilities from the enterprise and attacker's perspectives were then listed and documented. These risks, vulnerabilities and threats were consequently rated and possible defence solutions formulated to mitigate the system against them (Cavelty, 2007).

The second phase of the RAD methodology is the user design where the developer interacts with the users of the system and builds models and prototypes of the proposed model. The design of

this study was based on the client-server architecture. This means that a user was able to request a service and the service provided as requested. However, if the service was not provided to the user, then the model detected this as a vulnerability and automatically fixed it or alerted the necessary authority for support and fixing.

The third phase of the RAD methodology is the construction of the system. This involves the model development, coding, unit integration and testing. For this study, this phase encompassed development, deployment and testing. These three processes are iterative in nature in that during development, when a module has been coded, the researcher deploys and tests it to ensure it met the needs and objectives of the study. Due to the different components developed for the system and their integration, the researcher used the bootstrap framework, coding the model using the CSS and JavaScript libraries within the framework. This was for the client side of the model. For the server side, the study used an Apache server that was reached through using MySQL queries. The researcher developed and tested the model on test websites before deploying it on the target critical information infrastructure. The researcher had to edit iteratively the configuration files when required to ensure that the model worked effectively on all select organisations. When the expected outcome was not achieved, the researcher had to keep debugging till the outcome was realized. The server side used the same technique of testing. The Apache server was set up with the correct credentials and tested to ensure proper running in the chosen environment. During integration, the researcher ensured that all the modules developed using the Bootstrap framework worked together correctly and that proper data was stored to the server in terms of logs, vulnerabilities detected and assets identified.

The final phase in RAD will be the cutover phase that will involve data conversion, full scale testing, system changeover and user training. For this study, the researcher implemented the model at this stage and monitored and evaluated its use. During execution, the model needed to be able to perform asset identification, vulnerability scanning and detection and remediation as stipulated. The researcher then used the data collected from the logs to monitor and adapt it to the current problematic situation. As such, scanning was continuously performed as there could be configuration changes, OS updates or even security incidents that took place such that they had to be checked again for vulnerabilities to be then properly handled.

3.4 Experimental Set-Up, Data collection and analysis

This study targeted organisations' online systems that are part of Kenyan sectors that are critical to its stability and development. The factors that determined the criticality of these sectors include their functions and interdependencies, reliability, availability and current controls of the systems in various sectors. This implies that if a system is used across more than one sector and its functions are necessary for the sectors' operations, it is a critical sector. For instance, the financial sector is critical since its infrastructure is needed across the other sectors like government, health, energy and agriculture. Therefore, when the financial infrastructure is unavailable or unreliable due to a failure, all other sectors suffer potential threats and vulnerabilities.

These sectors were then divided into strata since each sector had its unique characteristics. The strata included government services, financial services, retail, insurance, healthcare, tourism, education, agriculture and the Kenyan airspace. The study targeted any online critical infrastructure under these sectors as its experimental frame. Further, the study sought to detect vulnerabilities including but not limited to Cross-Site Scripting (XSS), X-Path injection, Cross-Site Request Forgery, Command Injection, Cross site tracing, file inclusion, Remote file inclusion.

For the experiment, the study was setup in different testbeds to demonstrate the applicability and practical use of the model. The experimental setup was based on the benchmark of the Nessus Attack Scripting Language (NASL). NASL was used as the benchmark since it has been adopted by Nessus and OpenVAS vulnerability detection tools. These tools have been used over time by many organisations to detect vulnerabilities in systems that are critical. NASL has over time collected information on common vulnerabilities and how they should be fixed. Using a benchmark allowed evaluating and comparing the proposed detection model according to standard criteria. The developed model was able to characterize the vulnerabilities that exist in the identified assets of the web services, databases and other hosts in the networks of the selected organizations. Data collection was achieved through observation and examination of the logs stored in the database by the researcher. The table below shows the main variables of the data captured under the experiments set-up for the model.

Data Variable
Plugin ID
CVE
CVSS
Risk
Host

Entity
Protocol
Port
Name
Synopsis
Description
Solution
See Also
Plugin Output
Asset UUID
Vulnerability State
IP Address
FQDN
NetBios
OS
MAC Address

Plugin Family
CVSS Base Score
CVSS Temporal Score
CVSS Temporal Vector
CVSS Vector
CVSS3 Base Score
CVSS3 Temporal Score
CVSS3 Temporal Vector
CVSS3 Vector
System Type
Host Start
Host End

The main metrics that were collected included the number of assets identified, the vulnerabilities detected, accuracy of detection, stability of the system and consistency. This data was then analysed and used to determine the effectiveness of the developed model against the open source ones that were reviewed in Chapter 2.

3.5 Model development and Data analysis

Threat modelling is a process to identify security threats to software applications. There are limitations for rigorous analysis of various threats and vulnerabilities that have been aforementioned and that maybe analysed in all the existing threat modelling approaches. Therefore, the need for automated analysis of threats and vulnerabilities is what this study developed to solve the problem of having to suffer vulnerabilities that could be avoided. Based on the research of the technologies that support existing possible models to this model and the kind of methodologies required, this system was developed using the DevSecOps (Development, security and operations) methodology to cover four components.

3.5.1 Vulnerability identification

This component of the system scans systems and identifies potential vulnerabilities. The research relied on vulnerability databases, vendor vulnerability announcements, asset management systems and threat intelligence feeds to identify security weaknesses on targeted systems.

3.5.2 Vulnerability Analysis

This component enabled the research determine the cause of the vulnerabilities identified. Thus the component showed the vulnerabilities with their associated particular parts of the system to allow for fixing of that specific component or part.

3.5.3 Vulnerability risk assessment

This was the most crucial component of the developed model. This module analysed vulnerabilities on the basis of the risk incurred on the critical information on the system. The tool identified which data and assets are at risk, the functional components of the systems at risk, ranked the risks associated with the vulnerabilities from low to high and showed the potential damage the organisation might suffer as a result of the vulnerability.

3.5.4 Data Analysis

Data collected by the proposed tool was analysed using descriptive statistics including mean, modes and measures of dispersion. Further, based on the vulnerabilities' CVSS ranking, the data was further analysed to provide a combined risk rating and score. The risk rating gave a simple negligible, low, moderate, or high value for all five components together, while the score was a numeric value between 0 and 10. The score was also used to determine the kind of mitigations to be chosen to effectively fix the vulnerabilities. Data from literature was also analysed qualitatively using an inductive approach.

3.6 Research Quality

This research sought to ensure valid and quality detection of vulnerabilities on critical information infrastructure/systems in identified sectors that are vital for communities and running of the country, Kenya. The research borrowed from the best practices used by previous works that have gone into the deployment of various vulnerability assessment tools. (Kritikos, Magoutis, Papoutsakis, & Ioannidis, 2019) indicated that a vulnerability tool should meet some criteria for it

to be considered reliable and ensure valid and health systems. These criteria are based on support, functionality and configuration.

A pilot vulnerability assessment was done by the researcher on a simple website with deliberate vulnerabilities on it. This according to (Xynos, Sutherland, Read, Everit, & Blyth, 2010) enables a study to map a network and systems connected to it, identification of services and a listing of vulnerable systems and vulnerabilities associated with the system. This pilot was necessarily conducted to ensure validity and reliability of the model and necessary recommended corrections were made before deploying of the final model developed.

3.7 Ethical Consideration

Considering the nature of this study, the researcher appreciated that this is a sensitive area of study that required following the ethical considerations laid down. The researcher had to first send in the proposal for study to Strathmore University Institutional Ethics Review Committee to conduct ethics review for this study's research design and protocols internally. The study also sought ethical review and approval from the National Commision for Science, Technology and Innovation (NACOSTI) by applying for a resrach licence from the commission. This ensured that the research met the ptotocols set for research to be conducted. Once reviewed by both boards, the study implemented the required changes for it to meet the required ethical research guidelines. The researcher also ensured that the study conformed to the stipulated Computer misuse and cybercrime Act, 2018 to ensure that no harm was caused during implementation of this study.

Before implementing this study in the various sectors selected, the researcher consulted and asked for permission to assess the organizations' systems for vulnerabilities. There was an introduction letter to introduce the researcher and the purpose of the study to the organizations sampled. Once the organization was made aware, the researcher gave the representatives of the organizations a consent letter for approval. This was to formally acknowledge that they were aware of the intentions of the researcher as outlined in the consent form. Subsequently, the researcher deployed the tool on their systems after receiving the authorization to collect data from the targeted institutions. The researcher was resolute to advice and notify affected parties in case of any alarming and harmful vulnerabilities identified on their systems. The targeted organizations' information was kept confidential and under no circumstances was it dissemminated to the public.

4. CHAPTER 4: SYSTEM ANALYSIS AND DESIGN

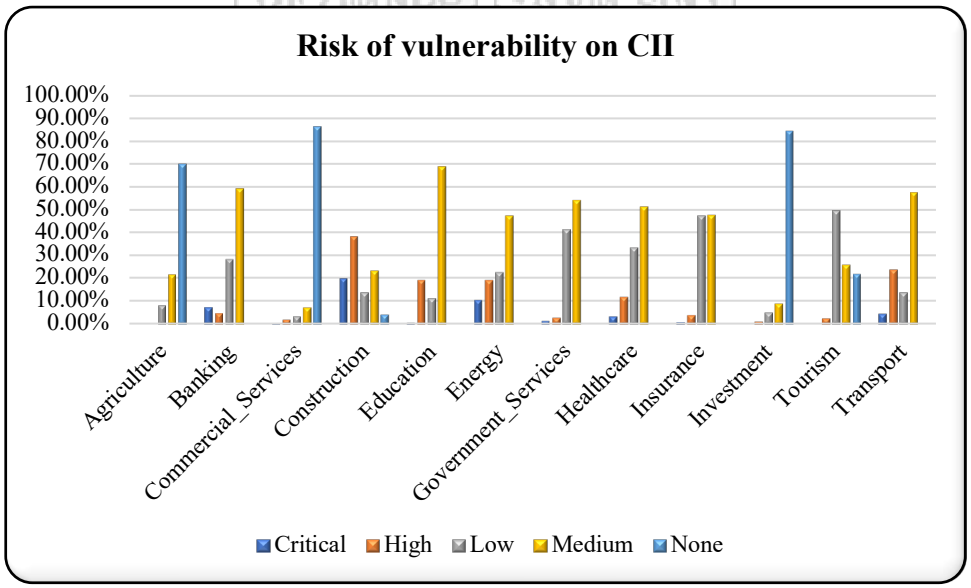
4.1 Introduction

This chapter will detail steps the researcher undertook in designing the model, herein known as the "TraceMe" system. TraceMe is a software model that was built to help organizations and institutions be able to detect vulnerabilities on their critical information infrastructure. This chapter will outline the system requirements, system environment under which it would be setup and help detect vulnerabilities. The chapter will also show the system operations by use of use case diagrams.

4.2 Requirement analysis

The model developed under this study was able to collected data on the main modules required in its functionality. These data included assets assessment and identification on critical systems, vulnerability detection, risk assessment of the vulnerabilities and their remediation. The following data analysis shows some of the data that was collected by the model.

To determine the risk and impact of the detected vulnerabilities on the CII, the model used the CVSS scoring framework. Scoring of vulnerabilities is done mathematically by getting an average of a score of set of variables of the system's components. For this study, the CVSS score was done by getting the average of the CVSS Base Score and the CVSS Temporal Score as discussed in this chapter.



4.3 System Requirements

The TraceMe model was designed to meet requirements described below so as to ensure that it is a system that will detect vulnerabilities on critical information infrastructure effectively. From the literature review of the study, the researcher identified the requirements possible for the design and implementation of this system.

4.3.1 Functional Requirements

The system should be able to:

i. Scan through a critical information infrastructure or system
ii. Identify vulnerabilities on the said CII.
iii. For every specific vulnerability identified, the system should be able to generate a report about it.
iv. The system should rank the vulnerability in priority standards.
v. The system should also give a report on the identified vulnerabilities.

4.3.2 Non-functional Requirements

This system was designed to let the establishing and customizing of sets of rules and to implement those rules on organizations' online critical information infrastructure. As such, the system should be able to detect vulnerabilities in a timely manner and the system should be able to address no delays for its users.

The system was also designed with scalability in mind hence it should be implemented to any web and network environment and operation with very minor changes applied to it. Based on the experimental setup, the researcher found that the system can be used in real-life scenarios with minor changes made to the system.

<Check on non-functional requirements like security and availability that will be key in systems of the kind you are proposing>

4.4 System Analysis and Architecture

This section shows how the system, from the study's literature review was designed according to the proposed conceptual framework.

4.5 Diagrammatic Representation of the System

4.5.1 System Architecture

The developed vulnerability detection tool is represented in the architecture in figure 4-1 below. The figure shows a system user on an organisation's CII, in this case the researcher, who uses and manages the system.

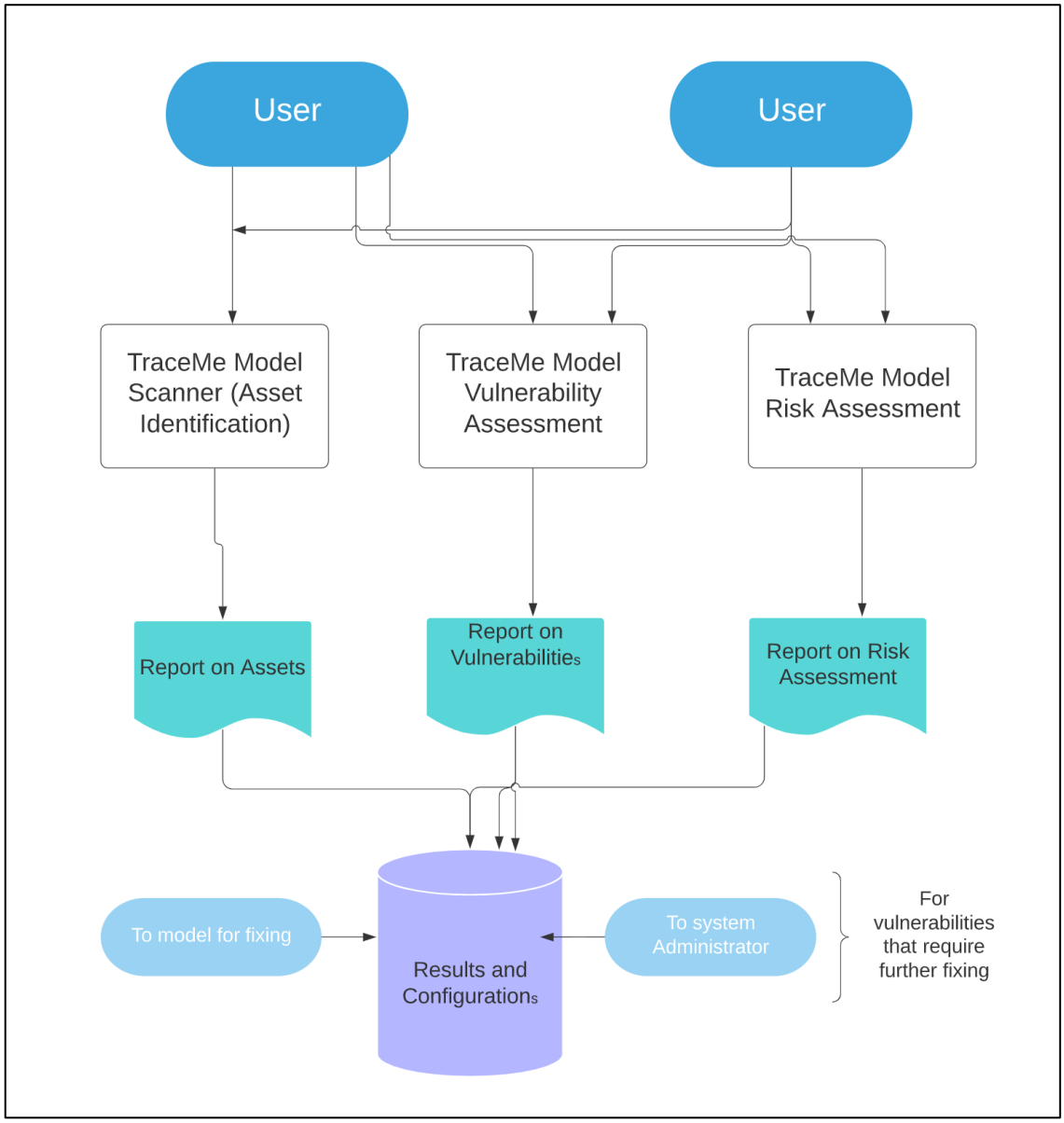


Figure Error! No text of specified style in document.**-5: System Architecture**

The figure outlines how the system was designed to function. The user activates the system though a web/network interface. The integrated developed model is then triggered using the assets identification module and uses the vulnerability assessment module to scan for vulnerabilities on the organisations' CII. The model then identifies the assets of the CII and potential vulnerabilities on it. The model then checks with the databases of the vulnerabilities, in case of new cases, they are stored and remediated, old cases are automatically fixed and updated. In the case where the model is unable to fix a vulnerability, it is sent to the system administrator for further assessment and remediation.

4.5.2 Context Diagram

The user/system administrator for this study was the researcher while the vulnerabilities are from real set-ups in various sectors in which the model was deployed.

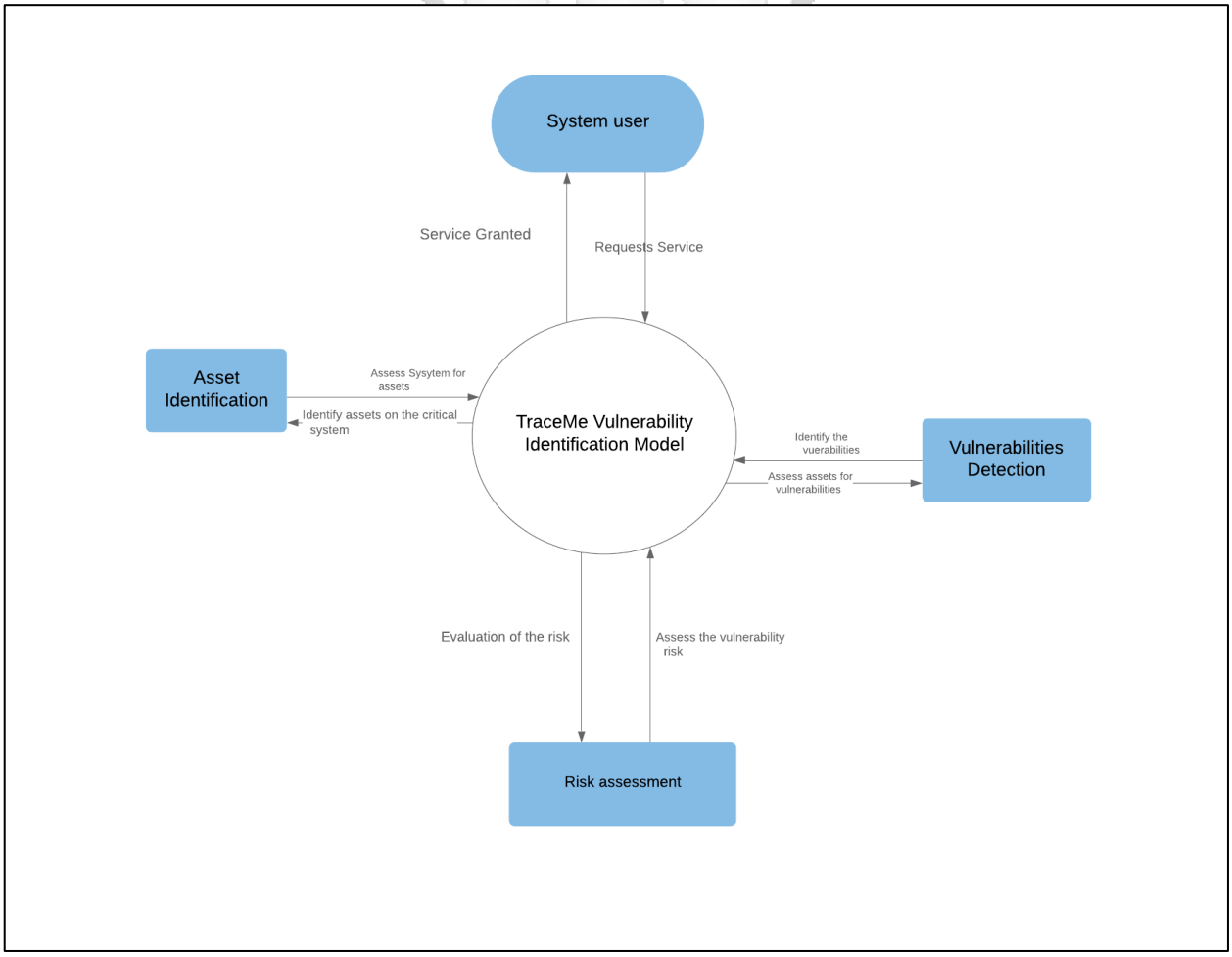


Figure Error! No text of specified style in document.**-6: Context Diagram**

The model allows a user to request a service and depending on authentication and controls, is granted or denied the service. The model then initiates assets' identification and vulnerability detection on the critical system in use by the user. It lists all the assets and the vulnerabilities associated with each. In cases of vulnerabilities, the model sends the logs to a database for fixing and updating by the system administrator. The model also runs a risk assessment of the vulnerabilities identified and for those that cannot be fixed, they are sent to the system administrator for fixing. The administrator queries from these vulnerabilities stored in a database to help in fixing and updating the CII. The figure 4-2 shows this context.

4.5.3. Data Flow Diagram (DFD)

Figure 4-3 below shows the main interactions that took place in the system once it was deployed on various sectoral CII of different organisations. The diagram shows that a user initiates a request to use the system for whatever services they seek. If successful, the system grants the service, if not, the system denies the service. In both cases, the model gets the details of the plugin on CII on which potential vulnerabilities occur. The model identifies the assets on the CII, vulnerabilities and their associated risk.

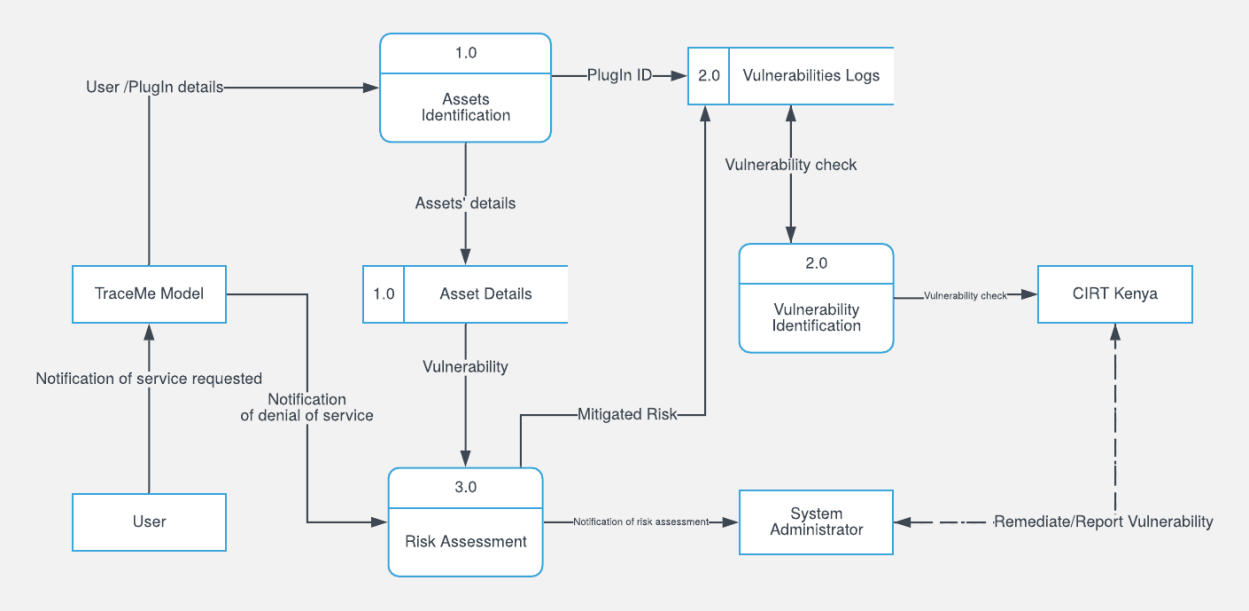


Figure Error! No text of specified style in document.**-3:Data Flow Diagram**

The vulnerabilities are then remediated and updated and a continual monitoring and evaluation of the same happens to avoid a recurrence of vulnerabilities that might have high impact on the CII.

4.5.4. Sequence Diagram

The sequence diagram on figure 4-4 shows the interaction between users, objects and the vulnerability assessment tool developed by the study. The figure illustrates the events and processes that happen when the system has been deployed and is being tested.

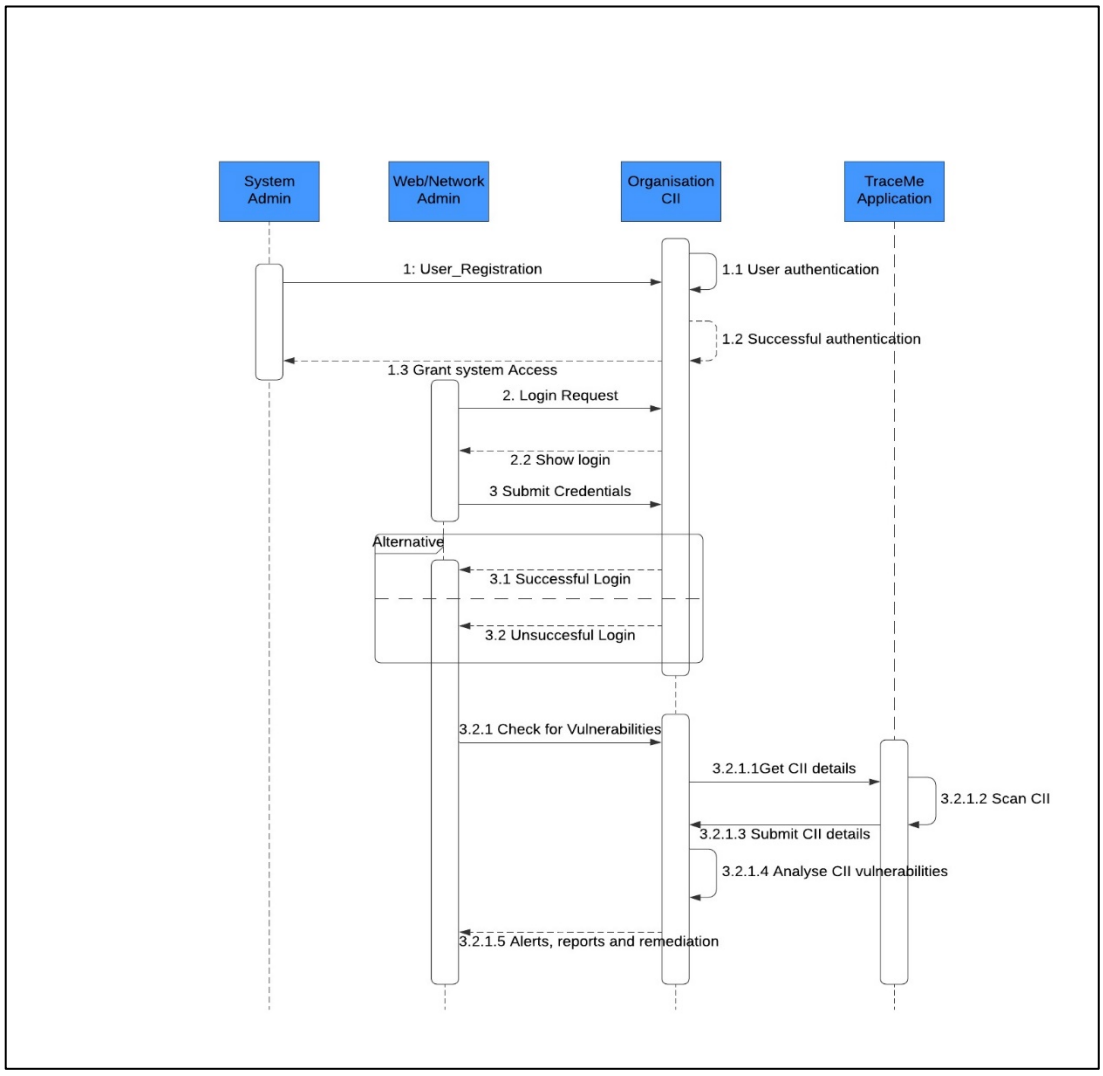


Figure Error! No text of specified style in document.**-7:Sequence Diagram**

TraceMe scans the CII and sends the system administrator reports on any vulnerabilities and threats on it. The reports are parsed by the various OSINT tools and changes the formats into a CVS file format and sends them to the Apache web server for storage. The administrator or user can then query from this database for purposes of remediation and update including monitoring and evaluation of vulnerabilities.

5. CHAPTER 5: SYSTEM IMPLEMENTATION AND TESTING

5.1. Introduction

This chapter discusses the implementation and testing of the TraceMe system in various sectors in Kenya. The proposed system requirements were discussed in the previous chapter. The implementation environment for the model and data transformation and analysis will be described in this section in an attempt to give a clear understanding of how the prototype works.

5.2. System Implementation

TraceMe model was implemented in a web application that runs on any browser, making it possible to cluster vulnerabilities for entities in different sectors and based on several attack vectors. The system highlights entities that are critical and that have the most urgent issues across various industries and sectors. The following algorithm was used to score vulnerabilities in the assets of the critical systems.

The main component of the system is that of assessing the vulnerabilities detected and prioritizing them in terms of risk, severity and impact of the vulnerability on CII. (Mell, Scarfone, & Romanosky, 2006) show that the CVSS score is given by getting the average of CVSS Base Score and the CVSS Temporal Score. They show the computation of the two as follows:

BaseScore = round to 1 digit of 10 * (case AccessVector of local: 0.7 remote: 1.0) * (case AccessComplexity of high: 0.8 low: 1.0) * (case Authentication of required: 0.6 not-required: 1.0) * ((case ConfidentialityImpact of none: 0 partial: 0.7 complete: 1.0) * (case ImpactBias of normal: 0.333 CNFDNTLTY: 0.5 INTGRTY: 0.25 AVLBLTY: 0.25) + (case IntegrityImpact of none: 0 partial: 0.7 complete: 1.0) * (case ImpactBias of normal: 0.333 CNFDNTLTY: 0.25 INTGRTY : 0.5 AVLBLTY : 0.25) + (case AvailabilityImpact of none: 0 partial: 0.7 complete: 1.0) * (case ImpactBias of normal: 0.333 CNFDNTLTY: 0.25 INTGRTY : 0.25 AVLBLTY : 0.5))

TemporalScore = round to 1 digit of BaseScore * (case Exploitability of unproven: 0.85 proof-of-concept: 0.9 functional: 0.95 high: 1.00) * (case RemediationLevel of official-fix: 0.87 temporary-fix: 0.90 workaround: 0.95 unavail: 1.00) * (case ReportConfidence of unconfirmed: 0.90 uncorroborated: 0.95 confirmed: 1.00)

The base score shows vulnerability severity while temporal score gives the urgency at specific system points.

5.2.3. Front-end System

The front end part of the web application which the user most interacts with was built using HTML5 and D3 JavaScript library that facilitate the development of interactive data visualizations in modern web browsers with a data-driven approach. It also utilized the Apache Web Server that uses MySQL technology for its database and querying entities.

5.2.4. Back-end system (The dashboard)

This component provides a compact interface that manifests all its valuable fulfilment through the web application. It shows the average vulnerability score for any critical information infrastructure (CII) selected from the pool and its Common Vulnerability Scoring System (CVSS) vectors. The average score is determined by taking the average of entities CVSS score on various attack vector of its publicly available records. Figure … shows how the dashboard works to achieve this scoring.

The dashboard facilitated the administration of the model and visualization of vulnerabilities on CII in various sectors, which is the core feature of the solution. The researcher used HTML5 to meet the system design needs to ensure a great user experience. The dashboard is divided into three columns; one to hold the data sources, a presentation area, and the reporting column for entity-specific summaries.

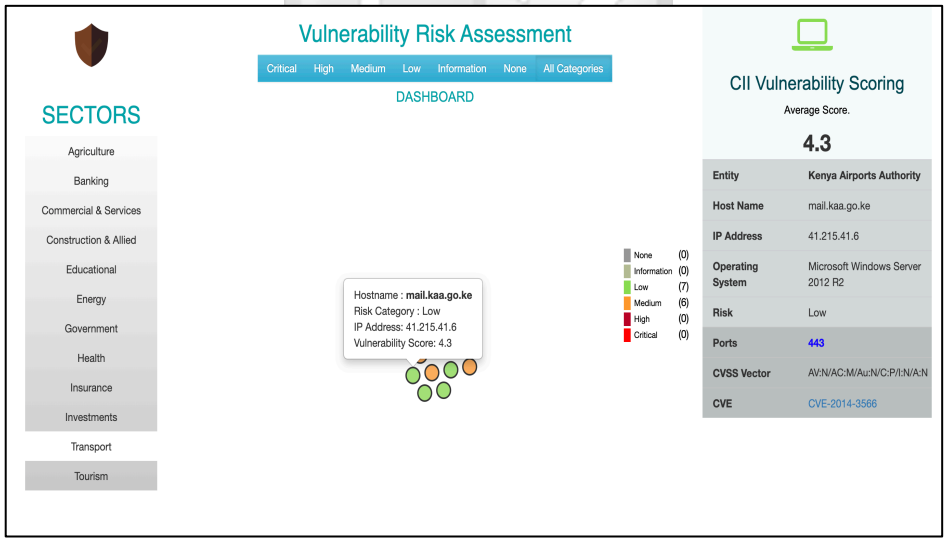


Figure Error! No text of specified style in document.**-8: System Dashboard**

The developed TraceMe model allows information security users to make a selection of their different data categories to visualize and make decisions on which entities to focus on. This made

it possible to have a solution that is simple to use without complexity as the data is loaded from CSV files once parsed by the various OSINT tools that collect data. This meant that this data could be obtained from different sources, then using the templates provided and transformation gave rise to data that could easily be utilised by the system users.

Below is a snippet of how the initial data load was executed at launch and took the first sector as the default allowing the users to start making their preferred selections.

```
d3.csv(dataSource, function(error, data) {
    console.log(data);
    data.sort(function(a, b) {
        return b.RC - a.RC;
    });
    var bubble_data = [];
    var ip_dict = make_uniq(data);

    for (entry in ip_dict) {
        var scores = ip_dict[entry]["total_score"];
        var av_score = get_average(scores);
        ip_dict[entry]["Category"] = get_category(av_score);
        bubble_data.push(ip_dict[entry]);
    }
    //set bubble padding
    var padding = 8;
    //set the margins for transformation
    for (var j = 0; j < data.length; j++) {
        data[j].radius = 10;
        data[j].x = Math.random() * width;
        data[j].y = Math.random() * height;
    }
    var maxRadius = d3.max(_.pluck(data, 'radius'));
    var getCenters = function(vname, size) {
        var centers, map;
        centers = _.uniq(_.pluck(data, vname)).map(function(d) {
            return {
                name: d,
                value: 1
            };
        });
        map = d3.layout.pack().size(size);
        map.nodes({
            children: centers
        });
        return centers;
    };
```

Figure Error! No text of specified style in document.**-9: Data load code**

Using D3 functions in the system, there was fundamental system data transformations. This enabled the study to maintain unique records and group together data from the same sources to avoid duplication of records. Fields like port and description were held in an array of JSON objects as it is key-value formation.

CVSS scores are important for this study as they are used to show the risk and impact of potential vulnerabilities and threats on CII. The scores were used to calculate the averages per every key pair. An asset could have multiple vulnerabilities which presents different scores, to achieved one

score per a record an average computation of the CVSS is taken. The records are classified under

Severity	Base Score
None	0
Informational	1.0 – 2.4
Low	2.5 – 4.9
Medium	5.0 – 7.4
High	7.5 – 8.9
Critical	> 9.0

the following classes. The figure 5-3 below shows the CVSS scale break down of vulnerabilities.

Figure Error! No text of specified style in document.**-10: CVSS Score code**

Visualization of the severity of each detected vulnerability was then achieved by ingesting the data into a bubble chart and creating the entity visual with different shades based on the severity score of each record. A tooltip was added to the dashboard to provide more information on the vulnerability when hovering on the entity visualization. A two-way data binding pipeline was implemented that whenever a user made a selection and/or hovers on any entity, its details are automatically applied on the summaries chart as well as its severity score.

The severity score is used to create clusters of assets that fall under the same baseline score with navigation between the different clusters if data is available. This makes it easier to select a visual of any cluster, also a legend has been provided to give a quick update of how many assets fall under each of the severity levels.

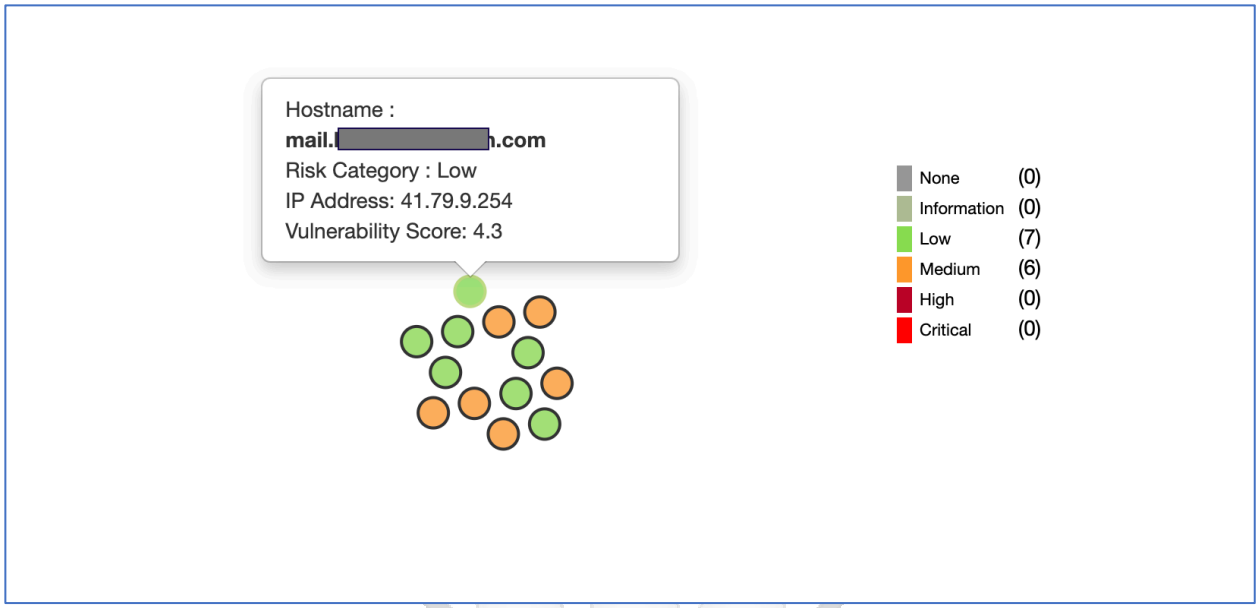


Figure Error! No text of specified style in document.**-11: CVE details code**

From the summaries table, the study was able to drill down and launch the CVE details on a new tab for more information, as shown in the figure 5-4 above. The CVSS scores per port and its descriptions were also recorded and visualized as seen on figure 5-5 below.

CVSS	DESCRIPTION
5	The remote host supports the use of SSL ciphers that offer medium strength encryption. Nessus regards medium strength as any encryption that uses key lengths at least 64 bits and less than 112 bits, or else that uses the 3DES encryption suite. Note that it is considerably easier to circumvent medium strength encryption if the attacker is on the same physical network.
5	The remote host supports the use of SSL ciphers that offer medium strength encryption. Nessus regards medium strength as any encryption that uses key lengths at least 64 bits and less than 112 bits, or else that uses the 3DES encryption suite. Note that it is considerably easier to circumvent medium strength encryption if the attacker is on the same physical network.

Figure Error! No text of specified style in document.**-12: CVSS Description**

5.3.3 Reporting and remediation

This module documented the threat or vulnerability assessed by the model to ensure it is fixed and that the vulnerability database was updated appropriately. Documenting helped responsible personnel derive, apply and analyse countermeasures of the vulnerabilities identified and detected

by the model hence strengthen the system against those vulnerabilities and secure the organizations' critical information and assets.

5.3. System Testing

5.3.3. Introduction

This section describes tests performed on the developed vulnerability detection model. Tests were done against the functional and non-functional requirements of the model.

5.3.4. Usability Testing

This was to determine whether the model was user friendly. 93% of the targeted users agreed that the developed model was easy to use and learn. This test was used to gauge how easy a new user could understand the model before interacting with it. The significant things checked were that the system flow was easy to understand.

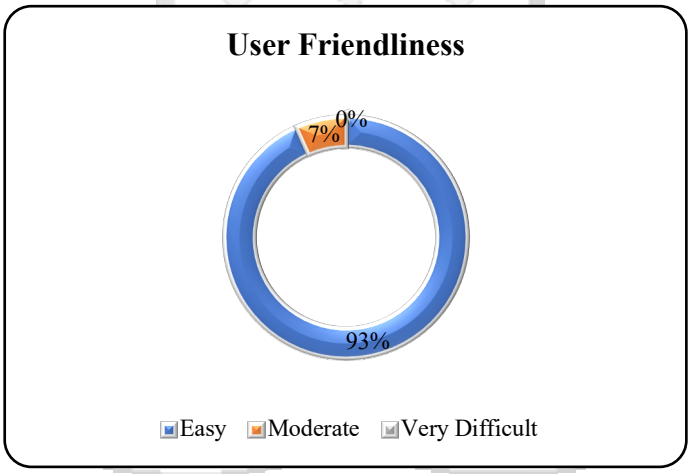


Figure Error! No text of specified style in document.**-13: User friendliness**

Browser Testing

The results showed that the model can be used on any web browser.

Table Error! No text of specified style in document.**-1: Browser Testing**

Browser	Compatibility
Safari	Yes
Google Chrome	Yes

Microsoft Edge	Yes
Mozilla Firefox	Yes

Acceptability Testing

User acceptance was carried out to ascertain if the model was a great accomplishment. A total of 87% of the potential users were satisfied with the system's capabilities. About 7% were unconvinced about the use, which meant that they had different ideas on some features of the developed solution. This acceptance test showed that many potential users acknowledged the model.

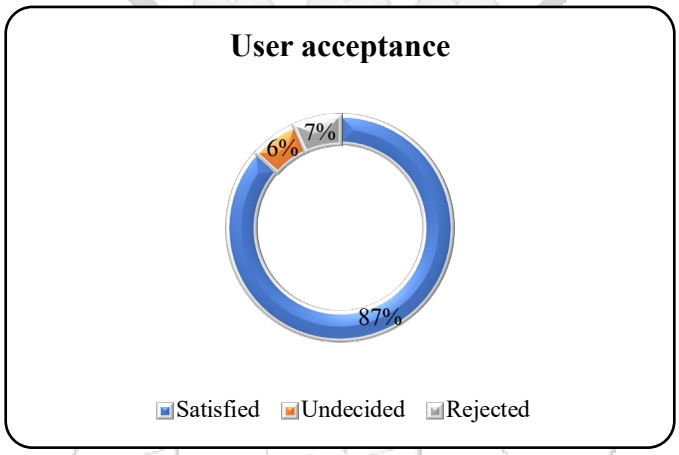


Figure Error! No text of specified style in document.**-14: User Acceptance**

5.4. Validation

Validation was carried out to check whether the proposed system addressed the challenges of early and easy detection of vulnerabilities on CII in key areas of Kenyan sectors that were identified as critical. TraceMe allowed the users to focus on protecting critical infrastructures and save on time taken previously to make a decision on fixing, monitoring and evaluating vulnerabilities. Interviews conducted with potentials users in the industry showed that the implementation of the tool was useful and important.

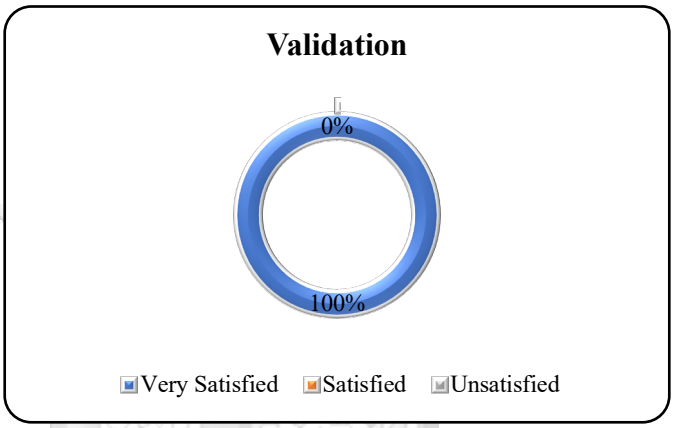


Figure Error! No text of specified style in document.**-15: User validation**

5.5. Sectoral Testing and Data Analysis

This section will describe findings from the data analysed in various sectoral CII in Kenya once the proposed tool was deployed in the various sectors.

5.5.3. Risk and Impact of vulnerabilities

To determine the risk and impact of the detected vulnerabilities on the CII, the model used the CVSS scoring framework. Scoring of vulnerabilities is done mathematically by getting an average of a score of set of variables of the system's components. For this study, the CVSS score was done by getting the average of the CVSS Base Score and the CVSS Temporal Score as discussed in chapter 4 of this study.

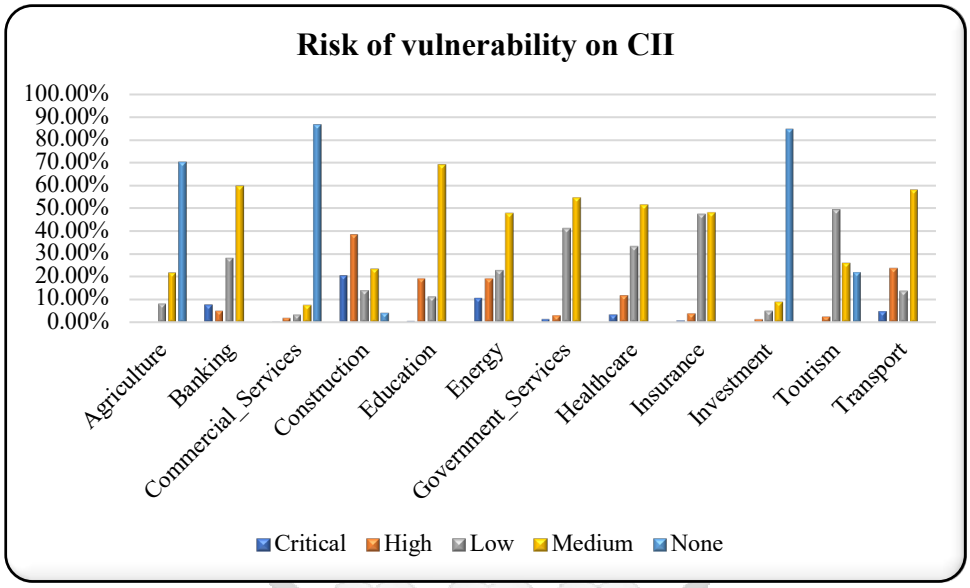


Figure Error! No text of specified style in document.**-16: Risk of vulnerability on CII**

From the results, it is worthy to note that most sectors experience medium risk of vulnerabilities on CII. This accounts for 40.44% of the vulnerabilities in all sectors with the leading sector being education followed by banking and transport. High risk vulnerabilities were detected to be high in the Construction sector followed closely by Transport and lastly Energy and Education. The high risk vulnerabilities accounted for 11.62% of all vulnerabilities in all sectors. The critical risk vulnerabilities on CII were realised in Construction, Energy and Banking sectors in the respective order. They accounted for 2.18% of vulnerabilities across all sectors. No risk and low risk vulnerabilities accounted for 31.63% and 14.14% respectively of all vulnerabilities across the tested sectors. From these impacts, the researcher determined that: None risk vulnerabilities on CII showed no potential for property damage while low risk vulnerabilities indicated that a successful exploit of this vulnerability could result in light property damage or loss. Medium risk vulnerabilities showed that a successful exploit of this vulnerability would result in significant property damage or loss while high and critical risk vulnerabilities noted for successful exploits of this vulnerabilities resulted in catastrophic property damage and loss.

5.5.4. Vulnerability Status

This test was to show the status of the vulnerability after an alert is sent to the system users (administrators). Most sectors showed that the vulnerabilities were known and were active on the

CII. Only the transport sector reported new cases of vulnerabilities on their CII as shown in figure 5-10 below.

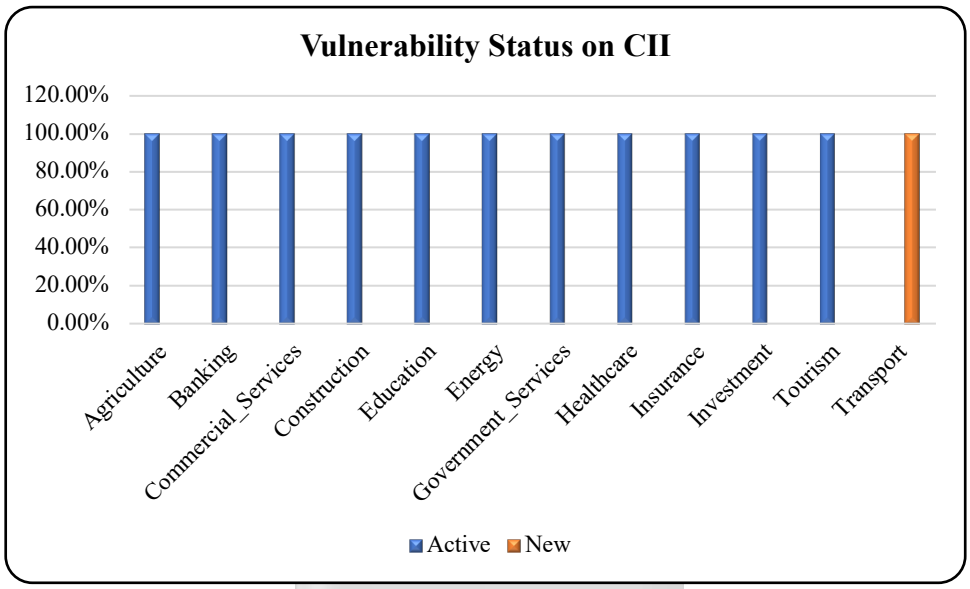


Figure Error! No text of specified style in document.**-17: Vulnerability Status on CII**

5.5.5. System Type

This component tested the type of systems used in various sectors in Kenya and detected vulnerabilities on their CII once their assets were determined by the developed model. The results showed that most systems were not categorized according to their function and this accounted for 57.51%. Of the remaining 42.49%, 39.86% were general-purpose systems which means they are systems that can be used for different types of functions due to their flexibility. 1.35% were recorded to be embedded systems thus implying specialized function computers that were focused on specialized functions to run. The rest 0.73% were firewalls helping in the security of organisations' networks.

5.5.6. Plugin Type per Sector

The plugin type shows how the system was designed to allow efficient and grouping of similar security checks. This allows for quick fixing of specific bulk of plugin of the host being scanned by the vulnerability detection tool. The figure below shows the types of plugins used by the system developed in various sectors.

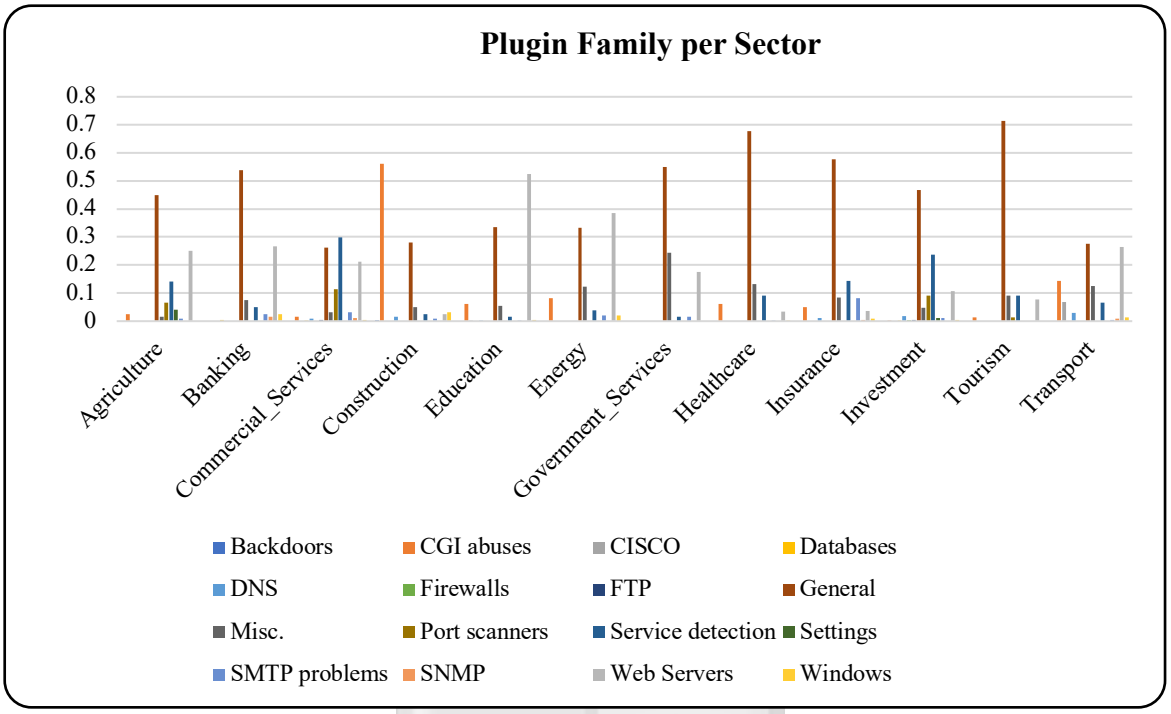


Figure Error! No text of specified style in document.**-18: Plugin Family per Sector**

The table below gives a summary of the types of plugins that were incorporated by the system.

Table Error! No text of specified style in document.**-2: Plugin Family Description**

Plugin family	Description
Backdoors	Plugins that detect high-profile backdoors, Trojan Horse programs, Worm infections, and systems with signs they have been compromised.
DNS	Plugins that test DNS servers such as ISC BIND and PowerDNS for known vulnerabilities. This family includes several tests that look for common issues in all DNS servers, regardless of vendor.
STMP Problems	Checks related to the Simple Mail Transfer Protocol (SMTP) and mail servers.
SNMP	Checks related to the Simple Network Management Protocol (SNMP) for a wide variety of vendors and common configuration errors.
Firewalls	Plugins that detect the presence of firewall devices and vulnerabilities in various commercial firewall devices, free firewall software, and proxy software.

CGI abuses	Checks for web-based CGI programs with publicly documented vulnerabilities. These checks include SQL injection, Local File Inclusion (LFI), Remote File Inclusion (RFI), Directory Traversal, and more. This family does not include checks for cross-site scripting (XSS).
FTP	Checks that look for vulnerabilities in FTP servers. These include common issues and misconfigurations regardless of vendor, as well as vendor specific issues that have been publicly disclosed.

6. CHAPTER 6: CONCLUSIONS AND FUTURE WORK

6.1. Overview

This chapter gives conclusions of the experimental findings of the data analysis of the study described in Chapter 5. This chapter also gives a scope of future work that can be done in this area of study and recommendations drawn from the finding are finally suggested by the researcher.

6.2. Discussion

Data collected from the system shows why vulnerability detection is important for CII. From the test results, the model is able to identify assets as it collects details of the CII and encrypts the details of the identified CII. The model is then able to scan for potential threats and vulnerabilities against the assets identified and give alerts for fixing, update and monitoring to avoid severity of vulnerability impact if not dealt with on detection.

By use of great development tools (HTML5 and D3), the system proved to be user friendly. The use of Apache MySQL Database was also handy in storing and querying of vulnerability records. The detection model worked efficiently on the identified organisations' CII by collecting data from the CIIs. The data was parsed to the database in CVS file format which made it easier for the user to analyse and make decisions on how to remediate vulnerabilities, update, monitor and evaluate them through the CII.

6.3. Conclusions

Given the dynamic nature of technology, every organisation is keen on ensuring safety of their CII. It was therefore important for this research to study common characteristics and profiles of CII threats and vulnerabilities. The study found that generally, on one hand, threats have been profiled with regard to their external or internal nature, that is, where the threats are likely to originate and their likelihood of happening. Internal threats include human threats while external threats include natural hazards and pollution. On the other hand, vulnerabilities then arise from the threats that are likely to occur and are exploited to cause damage on CII and the services they offer. For instance, in human threats, the vulnerabilities identified include system hacking which is exploited maliciously by the hacker to deny services to users. The model developed by this study was able to identify various vulnerabilities which could be classified by the characteristics discussed in chapter 2.

Vulnerability detection models that offer good vulnerability assessment and management are key in evaluating and monitoring critical systems in organisations. This study sought to determine the measure of vulnerabilities against assets of critical information infrastructure. The model developed by the researcher successfully identified assets on the critical systems. Once identified, the model scanned these assets for vulnerabilities and ranked them in order of the risk severity. This was necessary to determine the impact the vulnerabilities would cause on the system and how best to fix the vulnerabilities.

For the study to come up with an effective model for identifying vulnerabilities on CIIs, it sought to assess performance levels of existing applications and models. This helped the study look up research gaps and how best to contribute to these gaps. The study realised that there are different applications in use for vulnerability detection. Most of these applications use the Nessus attack scripting language (NASL) and incorporated the CVSS to score vulnerabilities. However, these models left out the risk assessment part of the vulnerabilities on the CII. This research therefore sought to build and contribute on closing this gap by developing a model that incorporated the risk of vulnerabilities on the CII's assets other than vulnerability and assets identification.

To conclude, the study developed a model that was used to identify vulnerabilities on CIIs. This model's functions included assets' identification, vulnerability detection on respective assets, the risk associated with each vulnerability and automated fixing of the vulnerabilities. The system took note of the synopsis of the vulnerability and checked in the database how to fix as most vulnerabilities were common and repetitive on the systems. In instances where the system could not use the vulnerability logs to fix it, a message was sent to the system administrator for remediation.

The developed model has therefore attempted to address a gap in information security which is detection and analysis of vulnerabilities of CII and their risk assessment.

Recommendations

The use of a good vulnerability detection, assessment and management model is an efficient way to ensure that CII is protected against potential threats and vulnerabilities as they are easily detected in time and fixed before they can cause critical damage to a critical system. This helps in

remediation, monitoring and evaluation as well as updating of the detected vulnerabilities which are ways of mitigating the risks associated with vulnerabilities on CII.

From the findings of this thesis, the researcher recommends organisations with CIIs to model their vulnerability identification systems to classify assets threats and vulnerabilities on the CII. This will help identify the common threats associated with the CII and the vulnerabilities arising and being exploited as a result. The researcher also recommends that policy guidelines be drawn and implemented so as to guide organisations on the standards required for threat and vulnerability profiling. In instances where new threats and vulnerabilities are not able to be profiled, an incident report should be sent to the Computer Incident Response Team (CIRT) for further study.

Secondly, this study recommends adopting technology that allows for a measure of CII assets and the vulnerabilities associated with these assets. The importance of this is that organisations can easily determine the risk and the severity of vulnerabilities on systems in a timely manner that allows for remediation.

Thirdly, most organizations have invested in various vulnerability detection systems and applications. However, the researcher found that most of these applications did not give a risk assessment of the vulnerabilities and their associated assets. The researcher recommends that vulnerability identification models should be developed with a module that determines the risk associated with the identified assets. This helps organizations to know which of their assets are more vulnerable and how they can mitigate against these vulnerabilities before they are exploited.

Finally, the study recommends that organisations need to embrace vulnerability detection models that have automated risk assessment of vulnerabilities and vulnerabilities remediation mechanisms that will minimise the ever-growing list of vulnerabilities. The importance of having the risk assessment module is to determine the risk impact of the assets and mitigate against the possible risk.

6.4. Future Work

For future research, an evaluation algorithm should be created to analyse the effectiveness of the model developed in mitigating the identified vulnerabilities and threats on CIIs and their assets. This would ensure a more productive and comprehensive threat modelling, detection and

remediation model. The data would be then represented in the best way for completeness, accuracy and clarity of the detection and remediation tool.

REFERENCES

African Union. (2014, June 27). *AFRICAN UNION CONVENTION ON CYBER SECURITY AND PERSONAL DATA PROTECTION.* Retrieved from https://www.au.int/web/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf

Bairwa, S., Mewara, B., & Gajrani, J. (2014, March). *Vulnerability Scanners-A Proactive Approach To Assess Web Application Security*. Retrieved February 17, 2020, from Research Gate: https://www.researchgate.net/publication/261182006_Vulnerability_Scanners-A_Proactive_Approach_To_Assess_Web_Application_Security

Bloomfield, R. E., Popov, P., Salako, K., Stankovic, V., & Wright, D. (2017). Preliminary interdependency analysis: An approach to support critical-infrastructure risk-assessment. *Reliability Engineering & System Safety*, 198-217.

Busuttil, T., & Warren, M. (2006). *Information Security Management, Education and Privacy: IFIP 18th World Computer Congress TC11 19th International Information Security Workshops 22–27 August 2004 Toulouse, France* (Vol. 148 of IFIP Advances in Information and Communication Technology). New York: Springer.

Cavelty, M. D. (2007). Critical information infrastructure: vulnerabilities, threats and responses. *Disarmament Forum*, 15-22.

Communications Authority of Kenya. (2018, December 1). Retrieved from Communications Authority of Kenya: https://ca.go.ke/wp-content/uploads/2018/12/Sector-Statistics-Report-Q1-2018-2019.pdf

Department of Homeland Security. (2016, June 27). *About the National Infrastructure Simulation and Analysis Center*. Retrieved from Homeland Security: https://www.dhs.gov/about-national-infrastructure-simulation-and-analysis-center

European Union Agency for Network and Information Security. (2015, February 23). *Methodologies for the identification of Critical Information Infrastructure assets and services: Guidelines for charting electronic data communication.* Retrieved from European Union Agency for Network and Information Security: https://www.enisa.europa.eu/publications/methodologies-for-the-identification-of-ciis

Gheorghe, A., Masera, M., Weijnen, M., & Vries, D. L. (2006). *Critical Infrastructures at Risk: Securing the European Electric Power System.*

GmbH, G. N. (2010, March 19). *OpenVAS - Open Vulnerability Assessment Scanner*. Retrieved from openvas.org: https://www.openvas.org/

Hashim, M. S. (2009, September 24). *MALAYSIA'S NATIONAL CYBER SECURITY POLICY: Towards an Integrated Approach for Cyber Security and Critical Information Infrastructure Protection (CIIP).* Retrieved from International Telecommunications Union: https://www.itu.int/ITU-D/cyb/events/2009/hyderabad/docs/hashim-national-policy-malaysia-sept-09.pdf

Henckel, T., & McKibbin, W. J. (2017). The economics of infrastructure in a globalized world: Issues, lessons and future challenges. *1Journal of Infrastructure, Policy and Development* , 1-18.

International Telecommunication Union. (2012, February 8). *Critical Infrastructure.* Retrieved from International Telecommunication Union: https://www.itu.int/dms_pub/itu-t/oth/06/5B/T065B0000100043PPTE.ppt

ITU. (2014). *Malaysia ranks third in Global Cybersecurity Index*. Retrieved from ITU: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/MALAYSIA-RANKS-THIRD-IN-GLOBAL-CYBERSECURITY-INDEX.aspx

Kim, D., & Solomon, M. G. (2014). *Fundamentals of Information Systems Security.* Burlington MA: Jones & Bartlett .

Krass, A. S. (1991). The People, the Debt and Mikhail. In *Bulletin of the Atomic Scientists.* Educational Foundation for Nuclear Science, Inc.

Kritikos, K., Magoutis, K., Papoutsakis, M., & Ioannidis, S. (2019, October 15). A survey on vulnerability assessment tools and databases for cloud-based web applications. *Array, 3-4*.

Kundishora, S. M. (2013). *The Role of Information and Communication Technology ICT) in Enhancing Local Economic Development and Poverty Reduction.* World Bank.

Martin Maguire, & Nigel Bevan. (2002). User Requirements Analysis. *IFIP World Computer Congress, TC 13*, 133-148.

Mell, P., Scarfone, K., & Romanosky, S. (2006, Nov-Dec). Common Vulnerability Scoring System. *IEEE Security & Privacy, 4*, 85-89. doi:10.1109/MSP.2006.145

Ministry of Information, Communications and Technology. (2014). *National Cybersecurity Strategy.* Retrieved from Ministry of Information, Communications and Technology: http://icta.go.ke/pdf/NATIONAL%20CYBERSECURITY%20STRATEGY.pdf

Moteff, J. D. (2015). *Critical Infrastructures: Background, Policy, and Implementation.* Washington DC: Congressional Research Service .

Moteff, J. D. (2015). *Critical Infrastructures: Background, Policy, and Implementation* . Congressional Research Service .

Moteff, J., & Parfomak, P. (2004). *Critical Infrastructure and Key Assets: Definition and Identification.* Congressional Research Service: The Library of Congress.

Moteff, J., Copeland, C., & Fischer, J. (2003). *Critical Infrastructures: What Makes an Infrastructure Critical?* Congressional Research Service: The Library of Congress.

National Academy of Sciences. (2003). *Critical Information Infrastructure Protection and the Law: An Overview of Key Issues.* Washington DC: National Academies Press.

National Institute of Standards and Technology. (2018, April 16). *National Institute of Standards and Technology.* Retrieved from https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

Naughton, J. (2016). The evolution of the Internet: from military experiment to General Purpose Technology. *Journal of Cyber Policy*, 5-28.

Newbery, D. M. (2000). *Privatization, Restructuring, and Regulation of Network Utilities.* Massachusetts: The MIT Press.

Nosworthy, J. D. (2000). Implementing Information Security In The 21st Century - Do You Have the Balancing Factors? *Computers and Security*, 337-347.

Pfleeger, C. P. (1997). *Security in Computing.* New Jersey: Prentice Hall PTR.

President's Commission on Critical Infrastructure Protection. (1997). *Critical Foundations Protecting America's Infrastructures.* Washington DC: The White House.

Republic of Estonia: Information System Authority. (2018, September 10). *Cyber Security*. Retrieved from Estonian Information System Authority: https://www.ria.ee/en/cyber-security/critical-information-infrastructure-protection-ciip.html

Republic of South Africa. (2015). *CIP Bill for Publication.* Retrieved from Police Secretariat: http://www.policesecretariat.gov.za/downloads/bills/CIP_Bill_for_Publication.pdf

Revnivykh, A. V., & Fedotov, A. M. (2016). Main Reasons of Information Systems Vulnerability. *Global Journal of Pure and Applied Mathematics*, 2133-2142.

Riedman, D. (2016). Questioning the Criticality of Critical Infrastructure: A Case Study Analysis. *The Journal of the NPS Center for Homeland Defense and Security*.

Rinaldi, S. M., Peerenboom, J. P., & Terrence, K. K. (2001). Complex Networks: Identifying, Understanding and Analyzing Critical Infratructure Interdependencies. *IEEE Control Systems Magazine*, 14-21.

SATRC Working Group on Policy and Regulations. (2012). *CRITICAL INFORMATION INFRASTRUCTURE PROTECTION AND CYBERSECURITY.* Kathmandu: SATRC.

Shostack, A. (2014). *Threat Modeling: Designing for Security.* Indianapolis, Indiana: John Wiley & Sons, Inc.

Sullivant, J. (2007). *Strategies for Protecting National Critical Infrastructure Assets: A Focus on Problem-solving.* New Jersey: John Wiley and Sons.

Theoharidou, M., Kotzanikolaou, P., & Gritzalis, D. (2009). Risk-Based Criticality Analysis. *International Conference on Critical Infrastructure Protection* (pp. 35-49). Berlin, Heidelberg: Springer.

Tikk-Ringas, E. (2015). Legal Framework of Cyber Security. In M. Lehto, & P. Neittaanmäki, *Cyber Security: Analytics, Technology and Automation. Intelligent Systems, Control and Automation: Science and Engineering.* Springer, Cham.

Tøndel, I. A., Foros, J., Kilskar, S. S., Hokstad, P., & Jaatun, M. G. (2018). Interdependencies and reliability in the combined ICT and power system: An overview of current research. *Applied Computing and Informatics*, 17-27.

Torrisi, G. (2009, January). Public infrastructure: definition, classification and measurement issues . Germany: University Library of Munich.

U.S. White House. (1998, May 22). *Critical Infrastructure Protection.* Retrieved from Presidential Decision Directive/ NSC - 63: https://fas.org/irp/offdocs/pdd/pdd-63.htm

United States General Accounting Office. (2004). *CRITICAL INFRASTRUCTURE PROTECTION: Challenges and Efforts to Secure Control Systems.* Washington D.C: GAO.

Velasquez, L. C. (2016). A Comprehensive Instrument for Identifying Critical Information Infrastructure Services. *A Comprehensive Instrument for Identifying Critical Information Infrastructure Services*. Tartu, Estonia: University of Tartu.

Whitman, M. E., & Mattord, H. J. (2012). *Principles of Information Security* (4th ed.). Boston: Course Technology Press.

Wigert, I., & Dunn, M. (2003). Critical Information Infrastructure Protection (CIIP) Policies in Selected Countries: Findings of the CIIP Handbook., (pp. 79-83).

Wolfpack Information Risk. (2016). *Critical Information Infrastructure Protection Report.* Wolfpack.

Xynos, K., Sutherland, I., Read, H., Everit, E., & Blyth, A. J. (2010). Penetration Testing and Vulnerability Assessments:A Professional Approach. *Internantional Cyber Resilience Conference* (pp. 125-132). Perth Western Australia: Edith Cowan University.

APPENDICES

APPENDIX I: LETTER OF INTRODUCTION

Strathmore University

P.O. Box 59857-00200

Nairobi, Kenya

April, 2020

Dear Respondent;

RE: REQUEST TO COLLECT RESEARCH DATA.

I am a student at Strathmore University pursuing a Master's of Science Degree in Information Technology. I am currently doing a research study on A **model for identifying vulnerabilities on critical infrastructures: case of cyber threats in Kenya which** is also the main purpose of this study. The specific objectives of this study are to identify common characteristics and profiles of CII threats and vulnerabilities, determine the measure of vulnerabilities against assets of critical information infrastructure and to design and develop a cyber-threat analysis model for identifying vulnerabilities on CII. Data from the participants will be collected through a tool that will be implemented on selected organizational systems that are considered critical in various socio-economic sectors.

The research study is in partial fulfilment of the award of Master's Degree. I humbly request your organization to participate in this study which will surely make this research a success. I would like to assure you that the information collected will be treated with strict confidentiality. Your voluntary involvement and cooperation in this study will be extremely appreciated.

Thank you in advance

Yours Sincerely,

Simon Kuria Maina

Student admission number: 050692

VT OMNES
VNVM SINT

APPENDIX II: LIST OF PARTICIPANTS

Sector	Count
Agriculture	
Ministry of Agriculture	43
Ministry of Agriculture Mail Servers	47
N.A.F.I.S	30
Banking	
ABC Bank	26
CO-OP Bank	13
CO-OP Bank	7
CO-OP Bank Bulk Payments	1
Equity Bank	103
Equity Bank Insurance	1
Family Bank	1
Jamii Bora Bank	14
Jamii Bora Bank App Server	4
Jamii Bora Bank Mail Servers	3
Spire Bank	26
Commercial_Services	
apps.batakenya.com	8
autodiscover.tuskys.com	1
blog.batakenya.com	6
mail.batakenya.com	7
mail.masoko.com	72
mail.tuskys.com	21
news.masoko.com	13
saritcentre.com	1
staff.masoko.com	76
www.mail.masoko.com	72
www.masoko.com	1
www.nakumattglobal.com	247
www.staff.masoko.com	77
www.tuskys.com	8
Construction	
Arm Cement	3
Bamburi Cement	6
East African Cables	277
East African Cables Mail Servers	87
East African Portland	33
Education	
Egerton University	283
J.K.U.A.T	113
K.N.E.C	32
K.N.E.C Mail Servers	12
Maseno University	1115
Masinde Muliro University	335
Ministry of Education	23
Ministry of Education Mail Servers	26
Moi University	828
Moi University	2
Moi University Mail Servers	15
Technical University of Mombasa	49
University of Nairobi	151
University of Nairobi Mail Servers	17
Energy	
K.P.L.C Mail Servers	7
KENGEN	200
KENGEN Mail Servers	7
Kenya Power	34
Kenya Power Web Mail	7
Ministry of Energy	4
Government_Services	
ECITIZEN ACCOUNTS	10
ECITIZEN BRS	1
ECITIZEN DATAFLOW	6
ECITIZEN LANDS	3
ECITIZEN NTSA	1
ECITIZEN PESAFLOW	1
I.E.B.C	4
I.E.B.C cpanel	2
I.E.B.C FORMS	3

I.E.B.C IMS	10
I.E.B.C Mail Servers	11
K.R.A	13
K.R.A	7
K.R.A SYSMAIL	4
Ministry of Health	29
Ministry of Health	3
Ministry of Health Mail Servers	21
N.S.S.F	2
Healthcare	
agakhanhospitals.org	1
bestpractice.mariestopes.org	3
brandlibrary.mariestopes.org	3
clictime.mariestopes.org	31
dev.orion.mariestopes.org	2
fs.mariestopes.org	6
gateway.mariestopes.org	4
global-impact-report.mariestopes.org	3
internship.medicalboard.co.ke	17
kondukta-auth.mariestopes.org	4
kondukta-web.mariestopes.org	5
mail.mpshahhosp.org	64
mpshahhosp.org	15
msibiwebservices.mariestopes.org	5
mwai.medicalboard.co.ke	17
online.knh.or.ke	6
orion.mariestopes.org	1
osp.medicalboard.co.ke	17
portal.medicalboard.co.ke	17
rdweb.mariestopes.org	5
remote.mariestopes.org	5
sandbox.medicalboard.co.ke	17
sandbox.orion.mariestopes.org	2
screenmedia.mariestopes.org	1
servicecentre.mariestopes.org	5
test.orion.mariestopes.org	2

time.mariestopes.org	4
training.medicalboard.co.ke	17
vms.mariestopes.org	11
www.internship.medicalboard.co.ke	19
www.knh.or.ke	9
www.mariestopes.org	1
www.mwai.medicalboard.co.ke	19
www.osp.medicalboard.co.ke	17
www.portal.medicalboard.co.ke	17
www.sandbox.medicalboard.co.ke	17
www.training.medicalboard.co.ke	19
Insurance	
assessment.jubileeinsurance.com	8
assessments.jubileeinsurance.com	8
autodiscover.assessments.jubileeinsurance.com	11
autodiscover.intraafrica.co.ke	12
autodiscover.mpesa.jubileeinsurance.com	11
autodiscover.online.jubileeinsurance.com	11
autodiscover.salvage.jubileeinsurance.com	11
bima.ira.go.ke	5
certificates.jubileeinsurance.com	10
cpanel.assessments.jubileeinsurance.com	11
cpanel.jubileeinsurance.com	8
cpanel.korient.co.ke	28
firstassurance.co.ke	50
ira.go.ke	3
iraersportal.ira.go.ke	13
jubicare.jubileeinsurance.com	2
korient.co.ke	5
mail.firstassurance.co.ke	4
mail.gakenya.com	2

mail.intraafrica.co.ke	13
mail.korient.co.ke	48
marine.korient.co.ke	6
motor.jubileeinsurance.com	2
motorclaims.jubileeinsurance.com	2
motortanzania.jubileeinsurance.com	2
ns1.jubileeinsurance.com	14
occidental-ins.com	27
omb.korient.co.ke	10
online.ira.go.ke	1
online.jubileeinsurance.com	8
parts.korient.co.ke	1
payments.intraafrica.co.ke	2
sale.firstassurance.co.ke	18
sales.firstassurance.co.ke	18
salvage.jubileeinsurance.com	8
statements.jubileeinsurance.com	14
uat.assessments.jubileeinsurance.com	8
uat-assessment.jubileeinsurance.com	8
valuation.jubileeinsurance.com	10
webdisk.assessments.jubileeinsurance.com	11
webdisk.intraafrica.co.ke	13
www.certificates.jubileeinsurance.com	2
www.gakenya.com	9
www.jubicare.jubileeinsurance.com	2
www.motor.jubileeinsurance.com	2
www.motorclaims.jubileeinsurance.com	2
www.motortanzania.jubileeinsurance.com	2
www.sale.firstassurance.co.ke	19
www.statements.jubileeinsurance.com	14
www.uat-assessment.jubileeinsurance.com	8
www.valuation.jubileeinsurance.com	2

Investment	
Centum	229
centum.co.ke	15
conference.nse.co.ke	5
cpanel.transcentury.co.ke	18
eregulations.invest.go.ke	9
Home Africa	203
invest.go.ke	4
Kenya Investments Authority	116
Kurwitu Ventures	20
kurwituventures.com	3
mailman.nse.co.ke	5
Nairobi Stock Exchange	333
Nairobi Stock Exchange Mail Servers	238
nse.co.ke	6
nsemail.nse.co.ke	3
nsemailman.nse.co.ke	6
ochl.co.ke	54
Olympia Capital Holdings	214
onlinetrading.nse.co.ke	1
smtpgate.nse.co.ke	3
tradetest.nse.co.ke	6
tradetest2.nse.co.ke	6
Transcentury	266
Transcentury	262
Transcentury Webmail	261
webdisk.transcentury.co.ke	15
webmail.transcentury.co.ke	15
www.eregulations.invest.go.ke	6
www.homeafrika.com	29
Tourism	
bonfireadventures.com	11
mail.tourism.go.ke	38
mail.tourismauthority.go.ke	15
tourismauthority.go.ke	1
ww.tourism.go.ke	12

Transport	
barua.bluebirdaviation.com	7
bulksms.kcaa.or.ke	6
change.jambojet.com	2
cpanel.kenyaairports.co.ke	8
demo1.silverstoneair.com	18
demo2.silverstoneair.com	16
dna.amlea.info	7
dna2.amlea.info	7
fids.kaa.go.ke	39
internet.kenyaairports.co.ke	9
jambojet.com	1
kaa.go.ke	14
mail.bluebirdaviation.com	18
mail.flysafarilink.com	18
mail.kaa.go.ke	6
www.kenyaairports.co.ke	8
www.krc.co.ke	38
www.mail.kenyaairports.co.ke	9
Grand Total	**8312**