INTERNET OF THINGS CYBER SECURITY ASSESSMENT MODEL AND METRICS

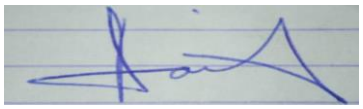
Matovu Davis

A thesis submitted in partial fulfilment for the requirements of the Degree of Doctor of Philosophy in Information Technology of Masinde Muliro University of Science and Technology

September, 2021

DECLARATION

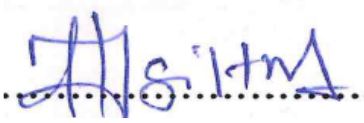
This thesis is my original work and has not been presented for a degree or any award in any other institution of learning.

Signature  Date 10th September, 2021

Davis Matovu, Reg. No. SIT/H/02/14

CERTIFICATION

The undersigned certify that we have read and hereby recommend for acceptance of Masinde Muliro University of Science and Technology the Thesis entitled "Internet of Things Cyber Security Assessment Model and Metrics".

Signature __  _. Date: 12th October 2021

Dr. Gilbert B. Mugeni, Ph.D

Innovation, Research & Development Division

Communications Authority of Kenya

Signature  Date 14th October 2021

Prof. Simon Maina Karume, Ph.D

Department of Mathematics & Computer Science

Laikipia University

Signature _  Date 14th October 2021

Dr. Stephen Makau Mutua, Ph.D

Department of Computer Science

Meru University of Science and Technology

COPYRIGHT

DEDICATION

This thesis is dedicated to my family, especially my wife for moral and financial support, my children, brothers and sisters during the whole process of the study.

ACKNOWLEDGEMENT

I wish to thank my supervisors, Dr. Gilbert B. Mugeni, Ph.D, Prof. Simon Maina Karume and Dr. Stephen Makau Mutua, Ph.D, for their guidance during my study. They have guided me through this academic work from the beginning till the end and their input and encouragement is highly appreciated.

My appreciation also goes to the Board of Postgraduate Studies for giving me an opportunity to undertake my education at this great academic institution. It is my belief and trust that my lecturers and supervisors guided me to reach this level and this assistance is highly appreciated with thanks.

I also wish to thank my classmates for their useful time, encouragement and discussion during my studies in the university.

Finally, I wish to thank my employer (Busitema University) for the financial support and for giving me an ample time during my coursework and support during the study. Without this understanding and cooperation, this entire process of studying would not have been successful. I have highly appreciated their understanding.

I thank God for the blessings of success during my studies.

ABSTRACT

In Uganda, there is a general lack of a specific model and appropriate metrics for evaluating IoT cyber security. To provide an informed basis for decision-making by policymakers, industry participants, and the public, a model and metrics in the domains of IoT cyber security readiness, intensity, and adoption are necessary. Previous cyber security research efforts have concentrated the general computer security. However, in the recent past, mobile devices and IoT based devises and networks are on the rise, giving rise to the emerging problem of IoT cyber security. In the recent years, the use of mobile devices and IoT-based devices and networks has increased, resulting in the emergence of the IoT cyber security problem. However, establishing IoT cyber security is difficult due to IoTs' intelligence, connectivity, sensing, and energy characteristics, which must be carefully analyzed if IoT cyber security is to be maintained. This thesis, which is based on a combination of qualitative and quantitative research, addresses the IoT cyber security metrics challenge in Uganda by establishing a model and metrics to assess the level of IoT cyber security in the domains of readiness, intensity, and acceptance. The research was based on the Technology Acceptance Model (TAM) and the Diffusion of Innovations (DOI) theory with the Socio-Technical Systems Theory (STS) providing the underpinning theoretical underpinning.The researcher utilised methodology triangulation involving a questionnaire in each of the research domains and structured interviews. In order to address the research objectives, and answer the research question the researcher firstly identified metrics that lead to increased IoT cyber security readiness, intensity, and adoption in Uganda. The thesis then presented a model, and an IoT cyber security metric, the IoT cyber security Assessment Index (ICSAM) that can be used to assess the state of IoT cyber security in Uganda, and other developing countries based on three sub-indices namely, IoT cyber security readiness (ICSR), IoT cyber security intensity (ICSI), and IoT cyber security adoption (ICSA), respectively across nine (9) constructs. These constructs were found to significantly explain the variation of the respective sub-indices in studies related to each of the research objectives. This thesis proposes an IoT cyber security specific model, and composite IoT cyber security assessment metric across the three domains of the IoT cyber security eco-system, namely readiness, intensity, and adoption designed for assessing IoT cyber security in Uganda, and other developing countries. Currently, general cyber security models and metrics are used to estimate the state of IoT cyber security. Using the delphi method of

validation using subject matter experts. The results appropriately validated the ICSAM model. The ICSAM computation algorithm can be easily automated, and the sub-index and construct weights varied to reflect the priorities of a particular decision modeler to suit a given developing country's special requirements. The major limitation of the study was that the findings and the implication of the study were based on the information received from the respondents in Kampala and Wakiso Districts due to the constraints of finance and time. However, because IoT technology users are dispersed across the country, this left a lot of information untapped. The study recommends further studies focused on developing a model for the implementation of IoT technologies in Uganda.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS & ACRONYMS

ABI-Allied Business Intelligence

CERT-Computer Emergency Response Team

CI-Cyber security Indicator

CPI-Cyber Power Index

CRI-Cyber security Readiness Index

CSIRT-Computer

GCI-Global Cyber security Indicator

GCA-Global Cyber Security Agency

ICT-Information Communication and Technology

IoT-Internet of Things

ITU-International Telecommunication Union

MMUST-Masinde Muliro University of Science and Technology

NCST- National Council of Science and Technology

NITA-U-National Information Technology Authority Uganda

SIRT-Security Incident Response Team

UCU- Uganda Christians University

WTDC-World Telecommunication Development Conference

CHAPTER ONE
INTRODUCTION

1.1 Background to the study

Advances in Information and communications technologies (ICTs) have resulted in disruptive technologies that enable instantaneous electronic transactions globally. One of the most disruptive of the emerging technologies is the Internet of Things (IoT) phenomenon [1]. According to [1], the Internet of Things (IoT) is a network of sentient devices with the ability to self-organize, share data, process data, react, and execute in response to their physical and logical surroundings. According to [2,] the Internet of Things (IoT) is a global network architecture that connects physical and virtual things via data and communication capabilities, necessitating a high level of autonomous data collection, event transmission, network connectivity, and interoperability.

The IoT idea was first introduced in the early 1980s and became widely popular in the late 1990s [1] . Wireless sensor networks and micro-electro-mechanical systems (MEMS) were among the first IoT applications [2]. At the moment, IoT applications can be found in practically every industry. A growing number of industries are relying on these devices for anything from health care to energy grids to environmental monitoring [3].

[4] notes that Smart gadgets connected to a network can help enterprises, governments, and the public-private sector address a wide range of challenges and issues.

Connecting people and things to each other at any time and from any location over any network and any service is the goal of the IoT [5].

There are numerous applications and domains for which the IoT has been hailed as one of the most disruptive technologies in the world, from smart cities to military and healthcare to agriculture and intelligent commerce systems [6]. There are several other IoT applications that may be used to monitor bridges, such as sensors and video security

cameras that can link to bridges, identify abnormal behaviour, and transmit alerts through text message. Video processing analysis can also be used to keep tabs on traffic flow[8].

With the IoT, "things" actively participate in business, information, and social processes, interacting with people and the environment, communicating, and exchanging environmentally friendly data and information. One is capable of responding autonomously. In the continuing process of providing services, events in the physical environment prompt actions and effects, with or without direct human involvement [9]. Smart things can be interacted with using a service-style interface, which allows for queries and changes in information about the devices' status, as well as consideration of privacy concerns [9][10].

IoT devices will outweigh the world's population of around 7 billion by 2018, according to the Federal Trade Commission (FTC) of the United States. [12] Predicts that by 2022, there will be more than 30 billion IoT devices online. Scalability, name, resource restrictions, mobility, interoperability, security, and privacy are just some of the issues that have developed as a result of this expanding trend of extending the Internet's boundaries to include non-traditional computing devices through the Internet of Things. Cybersecurity is the most serious of these new IoT problems [12]. Bain & Company consulting's 2018 [13] research shows that companies are willing to adopt additional IoT devices if their concerns about cybersecurity risks are addressed. Increasing IoT solution deployment might be greatly facilitated by enhancing IoT security, according to the report. On a worldwide scale, new legislation like the EU General Data Protection Regulation (GDPR), which set severe data protection obligations and fines for security failures, including data breaches, may be increasing pressure on security concerns. There is a data commissioner's office in Kenya, where the data protection act of 2019 was enacted and implemented to ensure the safety of personal data processed by individuals and organisations.

According to recent research [18], IoT-based threats will grow more pervasive and impactful, and organisations need to pay greater attention to IoT-related risks while establishing their organization's cyber risk management plan.

Intelligent platforms and digital, cyberphysical, and social systems all work together to make the IoT beneficial to society. It's possible to adjust the density, time, and automation of systems by integrating these systems together in an efficient and effective manner. The IoT's security and trust management challenges stem from the fact that it was built before current risk assessment procedures were in place [18].

However, these methods cannot justify the complexity and proliferation of these automated systems [19]. In addition, IoT security relies on the protection of all systems, entities, and levels involved (e.g devices, clouds, back-end systems, communications, operations, personnel, etc.) [20].

Research conducted on IoT cybersecurity threats [9] posited that with the rapid increase

In addition, [8] forecasts that by 2020, more over 25% of enterprise-identified assaults would be directed at IoT devices or systems, despite IoT accounting for less than 10% of IT security budgets. Therefore, there is an increasing need for researchers to take advantage of new computing and network security models and incorporate security into this fast-growing phenomenon of the IoT [8].

IoT Cybersecurity Threat Survey [9] found that with the rapid growth of the IoT, cybersecurity and privacy risks have significantly increased, creating a major dilemma for businesses and public institutions[10]. A study conducted in 2019 entitled IoT Cybersecurity Models concludes that there is still a significant amount of work to be done on country-specific IoT Cybersecurity models and cites the example of the lack of such country-specific IoT model for Kuwait.

Furthermore, [12] posits that current cyber security assessment models and models may not lend themselves to direct application for IoT Cybersecurity modelling, citing three distinct characteristics of the IoT devices. Because the majority of IoT devices operate unattended by humans, it is relatively easy for an attacker to physically gain access to them; they communicate over wireless networks, where an attacker could eavesdrop on confidential information; and finally, because many traditional complex security schemes cannot be applied to secure IoT systems due to their intrinsic capability limitations, such

as low power and computing resource capabilities, many traditional complex security schemes cannot be applied to secure IoT systems, opening a door for attack.

The rapid expansion of IoT networks and services, despite promising socioeconomic benefits, means that the security concerns associated with IoT are also rapidly increasing, as can be observed from the preceding. In addition, the widespread use of IoTs in today's vital systems means that the cyber risk associated with an IoT deployment could have a significant influence on the safety of life. Many businesses, organisations, and individuals would be impacted if a smart electrical grid or smart city's services were disrupted. IoT-based healthcare or air transportation, for example, could be targeted by a cyber-attack and result in the loss of life.

Additionally, [20], in a post-graduate thesis submitted to Florida Atlantic University's College of Engineering and Computer Science, advises additional study to construct new IoT-specific trust models that can be used in a variety of scenarios and would enable the creation of appropriate IoT remediation procedures [11,20].

According to [14] the unique legislation, technical aspects and literacy levels in other countries are also worth considering. Therefore, nature of cybercrime and its models cannot be used to evaluate the IoT cyber security. Hence, this has increased the need for information technology research regarding developing a specific IoT Cyber security assessment model under the domains of Intensity, readiness and adoption of cyber security strategies in a country.

Cyberspace or the entire Internet is increasingly being used as a tool and medium for cross-border crime. [21] found that cybercrime prevention and security are being challenged in a variety of ways, including power and regulatory independence. Existing global assessment models are based on security and privacy legislation, Return on Investment, threat types, and compliance with threat models. While these are good aspects or parameters to consider, it is also true that factors such as data protection, threat intelligence, and threat management changes are of paramount importance to the Internet of Things phenomenon [13].

The Operational Threat Assessment (OTA) methodology presents intensity as a domain to be used by the general threat matrix while assessing security of cyber threats. At the same time, it is an indicator of how far a threat is willingly prepared to go to achieve its objective [19]. As a result of their ferocity, high-intensity threats are deemed more hazardous [19].

1.2 Statement of the problem

In the race to develop and release the next generation of IoT domain killer applications, cyber security vulnerabilities are being disregarded, according to [19]. There are also concerns about data ownership, data privacy, and the long-term viability of digital assets that are brought on by IoT's incorporation into communication networks [13]. With the continued growth of the risk landscape IoT devices and applications, there is a need for the development of suitable security assessment tools [12]. Malware infection, denial-of-service attacks, and other risks to the network infrastructure and the business itself are just a few examples of the constantly expanding IoT threat landscape [38].
The user end of the Internet of Things (IoT) is expanded to include Thing to Thing (T2T), Human to Thing (H2T), and Human-to-Human (H2H) (H2T). Intruders can readily deploy security vulnerabilities thanks to the widely dispersed and ubiquitous access method. Identity theft, denial of service, and even system failure are all serious concerns for IoT because of the many complex security threats it faces [11].

Attacks against IoT systems, which are becoming increasingly common, have had a tremendous impact on people's reputation, compliance, and financial resources [12]. IoT cyber-attacks have risen dramatically as a result of the rapid growth of IoT devices in fields such as smart grids, environmental monitoring, patient monitoring systems, smart manufacturing, and logistics [19].

Due to this evolving IoT landscape [4], new strategies, models and metrics need to be developed to address the evolving IoT security challenges. However, recent research [11] reveals that current cyber security assessment models may not be directly applicable to the assessment of IoT cyber security due to the unique underlying characteristics of IoT

networks, specifically given the IoTs lending themselves to the use in isolated locations, ability to seamlessly and wirelessly interconnect with various devices and networks with inherently minimum inbuilt security protocols [10] [11] [12].

IoT also exhibits the characteristics of intelligence, connectivity, sensing, and energy which need to be carefully assessed if IoT cyber security is to be maintained [4][5].

Conventional cybersecurity models may address many not sufficiently address IoT related due to the unique aspects of IoT security that necessitate the development of specific models and metrics for the IoT cybersecurity assessment. This research sought to address the critical need for a specific Internet of Things Cybersecurity Assessment model, and criteria that can be used to determine a country's IoT cybersecurity status.

Because of the rapid evolution in the Internet of Things, the existing assessment models and models may not be effectively used for evaluating IoT cybersecurity [11] [12]. A recent study by [13] argues that IoT technologies products, services and applications are not yet fully standardized, with IoT ecosystems largely unstructured, making it too difficult to tell who the actual participants in the eco-system are and which roles they play [14].

Furthermore, the deployment of IoTs in present-day critical systems means that cyber risk in an IoT deployment might extend to many entities and impact the safety of life.

A unique approach and criteria for IoT Cyber security evaluation are therefore urgently needed to assess the IoT cyber security status in a country in terms of its readiness, intensity and acceptance, with a special focus on Uganda.

1.3 Main Objective

The main objective of this research was to develop an Internet of Things Cyber security assessment model and metrics that can assess the IoT cyber security status of a Country in the domains of Intensity, Readiness and Adoption respectively.

1. 4 Specific Objectives

Basing on the identified research gap and research purpose, this research sought to achieve the following specific objectives.

1. To identify the metrics for the assessment of IoT cyber security in the readiness domain.
2. To identify the metrics for the assessment of IoT cyber security in the intensity domain.
3. To identify the metrics for the assessment of IoT cyber security in the adoption domain.
4. To develop a model for the assessment of IoT cyber security based on the readiness, intensity, and adoption metrics above with the case study of Uganda

1.5 Research questions

Review of studies on IoT cyber security assessment revealed lack of a suitable model, and metrics for the assessment of the state of IoT cyber security for developing countries. This led to the formulation of the following general research question.

"How can a model, and metrics be specified for the assessment of IoT cyber security for a developing country, with the case study of Uganda?"

In order to achieve the above stated specific objectives, the general research question was decomposed into following research questions.

1. Which metrics can be used for the assessment of IoT cyber security in the readiness domain?
2. Which metrics can be used for the assessment of IoT cyber security in the intensity domain?

3. Which metrics can be used for the assessment of IoT cyber security in the adoption domain?
4. How can a model be developed for the assessment of IoT cyber security based on the readiness, intensity, and adoption metrics above with the case study of Uganda?

1.6 Justification

This research sought to address the critical need for a model and metrics for the assessment of the status of IoT cyber security when it comes to emerging countries' readiness, intensity, and adoption, with special reference to Uganda. The model developed, and metrics are useful for assessing the state of IoT cyber security, and for good decision making targeting the evaluation of public policies that affect IoT deployments and applications. Measurements of IoT deployment and policy plans are critical to the formulation of strategies for new technologies in underdeveloped nations. [39] [40] [41] This research also makes a significant contribution to the body of knowledge in the area of IoT cyber security.

1.7 Theoretical Underpinning

Selecting a sound theoretical framework is essential for a study since it helps to form and define the research process and its outcomes [114]. Information Systems, Information technology and cyber security related studies are considered practical since the events are studied either through qualitative, quantitative or mixed methods in their natural settings [88] [92]. Recent research in IT, IS, and Cyber security has employed socio-technical systems [STS] theories to guide their studies [108] [109]. The usage of such theories to underpin research in qualitative research is mainly due to the association between technical and social spheres of Information systems.

This study therefore was underpinned by the socio-technical systems theory (STS) coined by Bostromand & Heinen in 1977. This theory is based on an approach that better explains the complex organizational systems that exist. This theory asserts that organizational systems are composed of social and technical components that are

independent and interactive. The social system component is concerned with the people, people attributes, and the interactions between people in any setting. The technical system component of this theory is concerned with the processes and tasks within the organization and the required technology that transforms the inputs into outputs [111].

The proposed assessment model and metrics aimed to give a standard technique for measuring an organization's or setting's IoT cybersecurity capabilities in order to handle the threats. The IoT Cybersecurity Assessment model incorporates the technical and social dimensions of security [112]. The term "socio-technical gap" refers to the mismatch between the social and technological aspects of a system. Social and technological aspects of a system should be as closely aligned as possible in order for the socio-technical systems theory (STS) to be effective [113]. [113] further said that STS is made up of people implementing technological solutions to carry out work tasks within a social framework (organisation) in order to achieve certain objectives. However, even in smaller groups of people, the social dimension is just as or even more intricate [111]. Using the STS theory, [113] investigated the software supply chain security issue from a systemic perspective. As part of the project, researchers came up with an approach to analysing threats and responses in the global software supply chain by modelling the target system.

[109] used the socio-technical systems theory in his research to understand and define training scenarios so as to give indications on both social and technical challenges from real life cases.

[113] used the socio-technical systems theory to examine the subject of cyber security incident response. Because cyber security threats are becoming more complex and difficult to respond to, this study was prompted by the need to bridge the gap between knowledge and practise in order to better protect organisations from these threats. Developing concepts and methods for improving socio-technical security controls, as a result of holistic modelling of the incident response process for cyber security, was essential.

Furthermore, [111] applied this theory in their research and particularly investigated on the area of internet of things (IoT) development from a socio-technical system standpoint. They argued that the development of IoT is a socio-technical ensemble that requires analysis with a simultaneous focus on technical and non-technical issues. They identified the key socio-technical issues in IoT development as the four components of STS and these are classified under technology, tasks, structure and actors.

As stated by [108], a socio-technical approach to cyber security states, when designing, building, maintaining, operating, and maintaining systems and infrastructure for the purpose of safeguarding data or other vital infrastructure components, it is necessary to take into account the interplay between various types of people, organisations, economies, and technologies.

Using STS theory as a foundation for this study, the researcher argues that cyber security for IoT deployments and applications can be approached from a complex socio-technical systems perspective, enabling the development of a model and metrics for assessing a country's IoT cyber security cyber security status in terms of intensity, readiness, and adoption, with a particular emphasis on Uganda.

1.8 Contributions of the research

This study has contributed to the existing body of knowledge in two fields namely, Cyber security and Internet of Things. The practical contribution of the study is through the development an Internet of Things cyber security assessment model under the domains of intensity, adoption and readiness (IoTCSAM). The developed model and metrics will be this beneficial to IoT eco-system developers, implementers, and policy makers in informed decision making.

Additionally, the study contributes to the body of knowledge on the adoption of new technology, using the example of IoT cyber security in a developing country context, with the case of Uganda.

The model encapsulates the critical parts of the process of assessing the cyber security of IoT devices. It can be used as a blueprint for processes or to assess the compliance of current systems with IoT cyber security criteria.

The research will provide new data on IoT cyber security metrics that significantly affect the readiness, intensity, and adoption of IoT cyber security with special focus on a developing country.

Furthermore, the developed model is generic and can therefore be applied to other entities and organizations to assist in the decision-making process by providing mitigating measures with regard to IoT cyber security

1.9 Research Scope

The purpose of this research was to construct an Internet of Things Cybersecurity Assessment Model capable of assessing a country's IoT cyber security status across domains of Intensity, Readiness, and Adoption of cyber security, with a particular emphasis on Uganda as a case study.

1.10 Research Assumptions

The primary assumption in this research was that the research instruments would yield sufficient data to enable derivation of the Model and metrics that can be used to assess the IoT cyber Cyber security of a country in terms of Intensity, Readiness and Adoption with focus on the case of Uganda.

1.11 Limitations of the research

The major limitation encountered during the research was that specific primary data was proprietary, and the owners were unwilling to disclose it. This, however, was addressed through methodological triangulation, where the self-administered questionnaire was first issued. Then a follow-up interview was carried out on respondents' to gauge the

consistency of the responses. In addition, due to the limitation of similar existing models developed to assess IoT Cybersecurity, especially about developing countries, validation of the developed model was performed via expert groups.

1.12 Definition of Terms

Cybersecurity: Cybersecurity is a term that encompasses both the technical and human capacity to guard or defend against cyberattacks [12].

Risk: The term "risk" refers to the degree to which an entity is at risk from a potential event or condition [13].

Risk mitigation: Risk mitigation is the process of prioritising, analysing, and implementing risk-reduction controls/countermeasures recommended by an organisation or individual's risk management strategy [14].

Internet of Things (IoT): The Internet of Things (IoT) is defined as a network of smart objects that possess the property of auto-organizing, data sharing, data processing, reacting, and performing under prevailing physical and logical environment [18].

1.13 Layout of the thesis

This thesis comprises Six Chapters arranged in three groupings: research setting (Chapters 1 and 2), methodology (Chapter 3), and research results, conclusions, and recommendations (Chapters 4,5 and 6).

Chapter One provides the context for the thesis, highlights the research gap, identifies the thesis purpose and objectives, presents the research questions, and explains the research theoretical context and research process.

Chapter Two critically reviews the literature on existing cybersecurity assessment models, models and metrics. The unique characteristics of IoT networks are reviewed,

and the adequacy of the existing models, models and metrics for application to the IoT eco-system are determined, validation of IoT cybersecurity models, and the research gaps are outlined.

Chapter Three presents the methodology that was adopted by the study to answer the research questions and achieve the research objectives. The research philosophy, design, approach, and the research instruments used and, the procedure that was followed, the location where the research was conducted, and the targeted subjects are also presented in this chapter.

Chapter Four presents the data analysis and presentation for the constructs used in the study to design the model for assessing the cyber security of Internet of Things.

Chapter Five details the model design, the derivation of the requirements, the model implementation, and validation.

Chapter Six presents the research conclusions and recommendations, and future work.

1.14 Summary

This chapter discussed the background information and motivation leading to the research. The problem statement, research gap, research objectives and research questions were communicated. The research scope, the justification, the research contribution, assumptions and limitations were presented. Lastly, the chapter enumerates the thesis layout. In the next chapter, the discussion is on the literature review followed in this study.

CHAPTER TWO
LITERATURE REVIEW

2.0 Introduction

This chapter presents the literature review concerning the IoT cyber security threat landscape. Further, the researcher investigates current cyber security assessment models to determine their adequacy to address unique cyber security risks associated with the Internet of Things phenomenon. Lastly, the recent related studies are reviewed and the existing cyber security assessment models therein are characterized to identify the research gaps that inform the need for the current study. The literature review in this chapter contributes to providing answers to the research question of this study.

2.1 IoT Cyber Security Landscape

The IoT is enabling new applications in a variety of fields. It raises several new security challenges due to its heterogeneous and large-scale nature. The ambiguity of the internet, the growing global IoT cyber security connectivity, increased network capacity due to the emergency of technologies such as 5G, and the exponential growth in the supply and adoption of smart devices has supported an evolving technology landscape, with the three key beneficiaries being IoT, Artificial Intelligence and Big Data respectively [5]. IoT has impacted almost all sectors of the economy, including energy, manufacturing, healthcare, finance, agriculture and transport.

However, this growing potential of the IoT also means extending the cyber threat security landscape in the areas where it is applied [55] and recognizing its possible consequences. For example, in the home setting, IoT is often employed in the control of home devices, heating and cooling, and the general security of the home. This can translate into multiple IoT devices installed in the home. The same is true for the enterprise where IoT devices would often be employed to support operational technology and office support, respectively [56]. The IoT systems' data gathering and monitoring capabilities allow IoT devices to interface with important systems in the Office, such as intranet and database servers. For example, in health care, IoT may be employed in critical systems for life support and support remote telemedicine [48]. This certainly increases the possibility of

threats in spaces that had never posed cyber security risks before. As a result, even threats that involve IoT deployment in non-critical areas such as smart toilets, laundry, and hospitality deployments can significantly impact the environment they are set up in.

Data transmission and authentication must be secure in order for IoT devices to be considered safe. IoT data security and the ability of authorised users to access data securely [50]. IoT devices face a variety of security difficulties, including technological, ethical and privacy concerns [51]. In order to function properly, the Internet of Things demands architectural solutions that can handle heterogeneous states. There are three layers to the IoT architecture: (a) the perception layer (b) the network layer (c) and the application layer [54].

Due to the fact that each layer of the IoT architecture has its own security problems and connects with the others, security measures must be addressed for the entire architecture [43]. A complete and integrative picture of IoT cyber security is offered through a review of the literature on cybersecurity breakthroughs viewed through the lens of IoT architecture. According to Lee's five-layer business IoT design, the focus should be on cyber security concerns and solutions at the layer level [54]. The five layers covered here include cybersecurity at the network layer, cybersecurity at the processor layer, cybersecurity at the application layer, cybersecurity at the service management layer, and cybersecurity at the perception layer.

The network layer plays an important role in the overall security performance of the IoTs. In order for devices, processing stations, and the IoT system to function properly, secure data transfer is required. Attacks are detected, countermeasures are taken, and packets are monitored using an intrusion detection system (IDS) [39].

At the Processing Level: Cybersecurity Fog computing and cloud computing are now mainstream processing technologies for storing and analysing big-size data streams generated by a large number of IoT devices at the same time. Fog computing makes use of network devices to process data in real time while taking into account the impact of delay. It is also possible to detect intrusions using the IDS on a fog node.

Application Layer Cybersecurity: Different techniques are required for different application domains, such as Smart Homes and Transportation and Smart Health and Smart Grids. Because many IoT apps are owned by third-party service providers, cyber-attacks on these applications are possible and may have an impact on the security of other interconnected applications.. Monitoring and control, big data and business analytics, and knowledge exchange and collaboration are some of the enterprise IoT applications [55].

At the Service Management Layer: Cybersecurity Unlike previous layers, the service management layer focuses on the human and organisational components of cybersecurity rather than the technological dangers. These concerns are important to IoT service management because they affect IoT services [56].

Because of their small size and low power consumption, many IoT devices collect a large amount of data from their surroundings in real time, necessitating the employment of energy-saving strategies. Accurate inferences can be drawn from the data generated by machine learning techniques. Although IoT devices are so small and light, it is still difficult to include computation-intensive security and privacy protections into these devices [81]. Figure 2.1, adapted from [82], depicts the IoT Security Landscape.

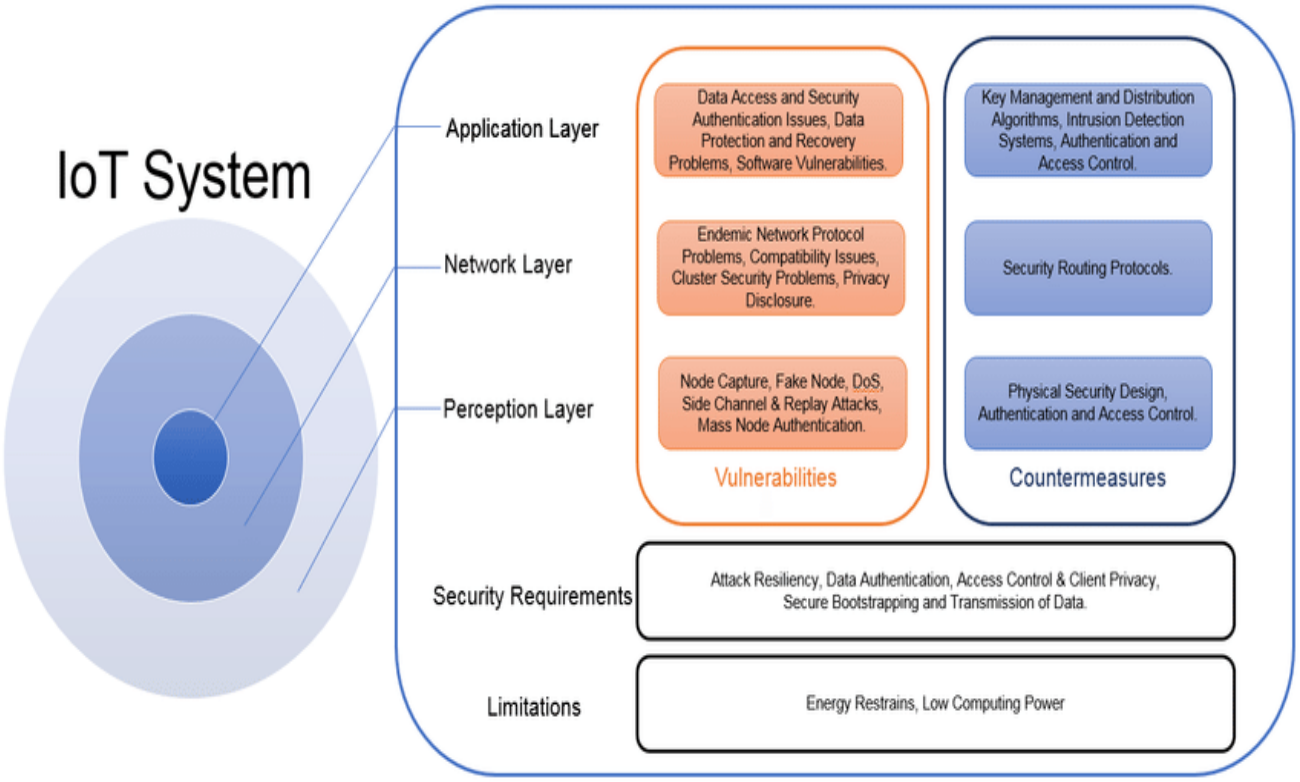


Figure 2.1 The IoT Security Landscape. Adopted from [82]

2.1.1 Unique IoT Characteristics with regard to Cyber Security

Specific characteristics make IoT environments highly susceptible to cyber-attacks [55] [69]. These characteristics include:

i) Unattended Operation

Because most IoT devices are left unattended, an intruder can more easily obtain physical access to them.

ii) Wireless Operation

The IoT devices communicate over wireless networks and this makes it easier an attacker to possibly obtain confidential information by eavesdropping and lastly,

iii) Resource capability

Majority of the IoT devices have inherently low computing resource capabilities and low power. As a result, many typical complicated security strategies cannot be applied to secure IoT devices, which frequently expose IoT services and the wider Internet to attacks and exploitation.

iv) Interaction with Large and Complex Data sets

The IoT sensors and devices gather greatly detailed and complex data from their virtual and physical environments as well as users. This data is vital for the IoT environments to function correctly. However, this data could mean a lot of cascading adverse effects if not secured or if stolen or otherwise compromised.

2.1.2 Anatomy of Internet of Things

According to [73] the IoT is a connection of physical objects that are accessed over the Internet, use embedded technology to interrelate with internal states or external conditions and can identify themselves to additional devices. Figure 2.1 below shows the Anatomy of Internet of Things. IoT avails a platform where objects can embody themselves then later turn out to be greater through connections to nearby objects and the wide-ranging data surrounding it.

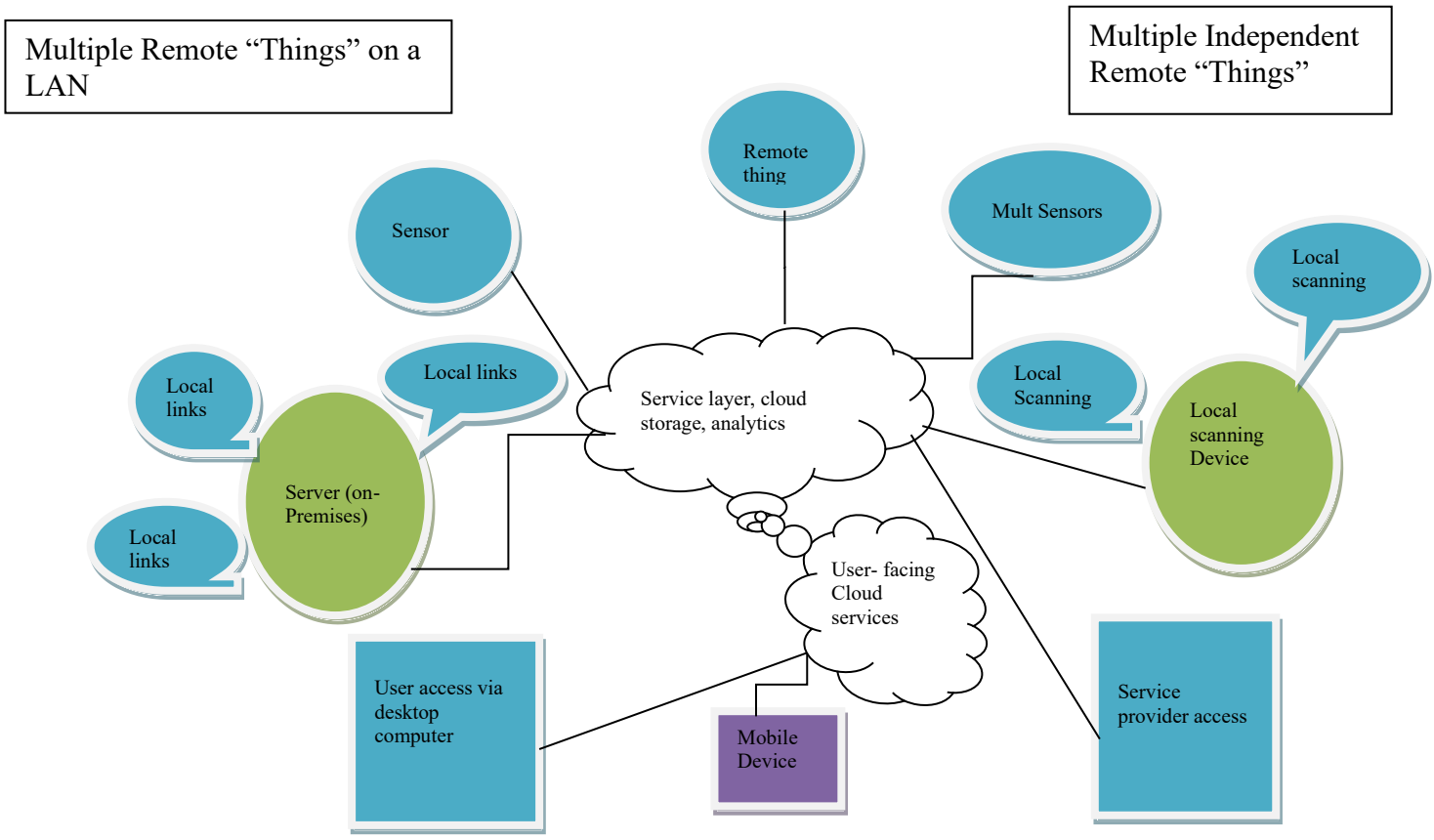


Figure 2.2: The anatomy of internet of things. Adopted from [97]

IoT describes a world that has the possibility for anything to be linked and communicate in a smart mode through integration of simple data to yield usable intelligence. Because of IoT, the physical world is transforming into one large information system whose vital goal is improving quality of life and enhancing new business models. However, this implies that extra business data and personal information will exist in the cloud and be passed back via thousands of devices that may have weaknesses copied from web. Any weak link in the security sequence might provide hackers with unlimited doorways that could potentially be unlocked and lead them to data access.

According to [93] the IoT is the next advancement in Internet technology that creates an improved interactive and unified entity, which connects the virtual and physical worlds in highly cohesive and progressive valuable ways. This information that IoT avails on real-

world objects, will turn the world into a more highly connected status thus enabling human-to-human, human-to-thing, and thing-to-thing (machine-to-machine) interactions. With [74] asserting that the IoT is a worldwide network that facilitates communication between people, things, and things-to-things, which is everything in the world by providing a unique identity to every object, this is a good fit. The IoT is a constantly expanding idea in the IT world, and it is widely considered to be the newest and most touted technology. A global network of networked physical items, allowing timely connectivity for anything, has been repeatedly presented as a vision of the IoT time and again

2.2 IoT Attack surfaces

[42] defines an attack surface as the total number of feasible entry points into a system or network from which an attacker can retrieve data. In Section 2.1 above, we saw that the IoT attack surface is quite big, which raises the risk exposure. Because of this, it is possible to take advantage of all the primary components of IoT systems. As a result, ensuring the safety of IoT systems should be a top focus during their development and maintenance. It doesn't matter how big or small an IoT system is or what type of environment it is built into; security must be considered in all phases of system development beginning with the design phase. According to [44], threats and vulnerabilities can be found in the following areas of IoT systems and applications:

2.2.1 Devices.

One of the most common ways an attack can be launched is using a device. The memory, firmware, physical interface, web interface, and network services of a device are all potential points of vulnerability. Default settings, out-of-date components, and unprotected update systems can all be exploited by attackers.

2.2.2 Communication channels.

Cyberattacks are also originating through the interconnected networks and channels of IoT devices and systems. Network assaults such as denial of service (DoS) and spoofing can also affect IoT systems.

2.2.3 Applications and software.

Security flaws in web apps and related technologies plague the IoT. Applications can be used to collect user passwords or push malicious firmware updates.

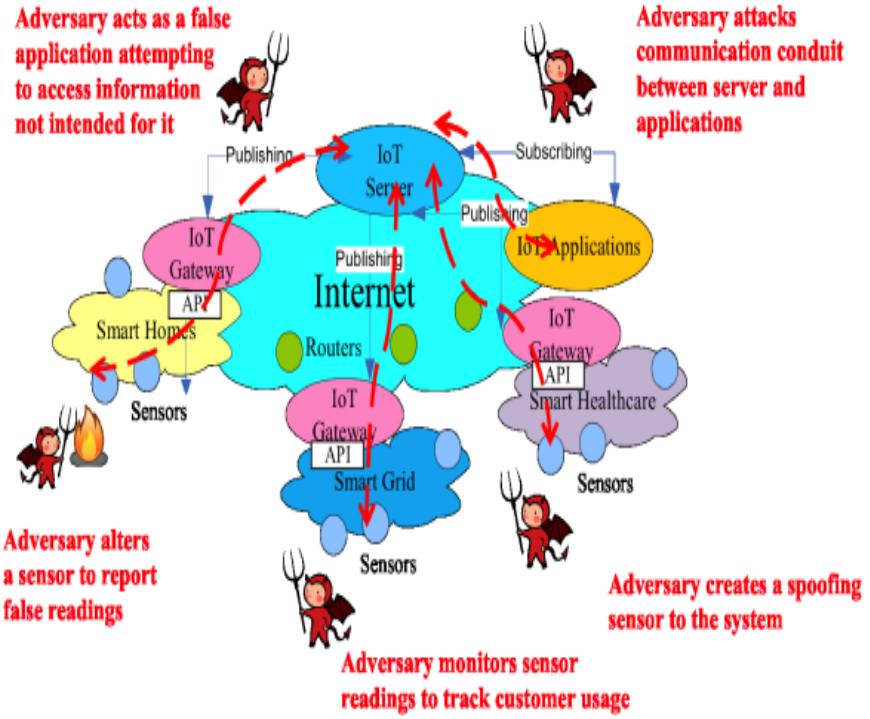


Figure 2.3 Potential Threats for the IoT system. Adopted from [14]

2.3 Cyber threats that impact internet of things

IoT cyber security is now recognized as a critical national policy issue [14] by many Countries.

It is important that we understand how operators of modern cyber-physical systems commonly approach monitoring, controlling, and managing infrastructures in order to classify security threats to these systems It is also said that security risks come from four different avenues of attack. Cyber-physical systems are vulnerable to associated software defects and hardware malfunctions because they inherit vulnerabilities from commercial off-the-shelf ICT equipment that are embedded in the systems. Cyber-physical systems can also be targeted by hostile attackers who are able to exploit protocol and network weaknesses. Open Internet protocols and shared networks are being supplanted by proprietary protocols and private networks.

Third, the CPS data is generated, used, and modified by a number of other parties as well.. As a result, key parties like system operators, ICT providers, and end users will face new access control and authorization difficulties.

Finally, a large number of remote field devices are used in cyber-physical systems, and these devices can be accessed via short-range communications. As a result, cyber-physical systems are open to both distant and local attack [75].

According to [43], IoT cyber-attacks are becoming more prevalent and sophisticated. For example, in September 2016, the Mirai malware conducted a DDoS attack (the Mirai Distributed Denial of Service (DDoS) botnet attack) against the website of a well-known security expert. A major attack on the internet in October 2016 is thought to have been caused by a code that was quickly copied by other cyber criminals. [6] Malware called Mirai infects smart gadgets and turns them into zombies or robots that can be controlled from afar [9]. Known as a botnet, these machines are regularly employed in DDoS attacks. An all-encompassing phrase used to describe a wide range of malicious software, malware comprises everything from trojan horses to spyware to rootkits to computer worms.

[7]. IoT cyberattacks of the future are expected to be significantly more severe than those that have been detected thus far.

Table 2.1 summarises the different standard classes of cyber threats and their impact [15]

Classes and impacts of cybersecurity threats		
Threat	Description	Impact
Compromise: remote	It is granting Concession of the device and its data, entirely or slightly, over a network.	Breach of External security radius.
Compromise: local	It is granting Concession of the device or its data, entirely or slightly through local hardware or software.	Breach of External security radius.
Privilege escalation	Surge in access, either locally or remotely, breaking a security boundary.	Humiliation or collapse of a security radius directing to an increased level of access either on a short-term or everlasting basis.
Imitation	Imitation of a trusted entity.	Humiliation or collapse of a security radius directing to an increased level of access either on a short-term or everlasting basis.
Perseverance	Persevering access is acquired post-compromise through configuration modification or hardware/software exploitation.	The honesty of the policy or the external security radius implementation is no longer productive.
Confutation of service	Service is lost, slightly or entirely. This can be for some time or good.	Humiliation in attainability or applicability.
Interference or alteration of Traffic	Network traffic of any type can be interrupted or altered.	Essential trust in the integrity and privacy of data transmission over the network can no longer be guaranteed.

Stored data access or alteration	Persistent data is read or altered.	Underlying trust in the integrity and confidentiality of the persisted data can no longer be assured.

(Source: [15])

2.4 Internet of things cyber security risks

Various of cyber security Risks exist in the Internet of Things Phenomenon as discussed in the following sections [18]

2.4.1 Illegal Access

Any unauthorised entry into a computer system is considered illegal access. This is sometimes referred to as hacking, cracking, or computer trespassing[18]. Computer systems and data can be damaged or compromised as a result of unauthorised access for instance, bypassing a password or other security measure to gain unauthorised access to a system or data.

2.4.2 Data Espionage

Data espionage involves individuals gaining information that is considered secret or confidential without the permission of the owner [19]. Sensitive information is often stored in networked computer systems. Offenders continuously try to access this information remotely.

2.4.3 Illegal interception

The term "illegal interception" refers to the intercepting of computer data transfers within a computer system, as well as electromagnetic emissions from a computer system [20]. An increase in the use of email and unprotected or unencrypted wireless Internet connection presents an opportunity for illicit interception.

2.5.5 Data Interference

Intentional or irresponsible tampering with computer data or electronic documents without permission is called data interference. A virus can be introduced or transferred as

part of this process [20]. Interfering with data, for example, entails introducing malicious code, such as viruses or worms, in an attempt to destroy or alter the data. Malicious actors can utilise data manipulation techniques to create backdoors that allow unauthorised users to gain access to systems, as well as malware and key loggers that record and transmit the keystrokes of computer users.

2.4.6 System interference

System interference is an act that modifies a signal in a disruptive manner, as it travels along a channel's source and receiver [18]. Computer systems can be interfered through insertion of malware that can tremble the functioning of a computer system. Such attacks can be committed through powerful distributed botnets.

2.4.7 Fraud and computer-related fraud

[19] describes computer-related fraud as the act of interfering with a computer system's normal operation in order to deprive another person of their property by entering, altering, deleting, or suppressing data. This is frequently done with the intention of obtaining an economic profit for oneself or another in a dishonest or fraudulent manner. Internet marketing and retail scams are among the many examples of credit card or advance-fee fraud.

2.4.8 Illegal Content:

Illegal content is exceptionally an offensive material that is employed online and includes acts like Child pornography or child abuse, content that promotes terrorism or encourages terrorist [20]. Criminals engage in illicit material distribution through a variety of means, including the distribution of child pornography, hate speech, and the operation of illegal gambling websites.

2.4.9 Spam

spam refers to the sending of large numbers of unsolicited emails. [13] E-mail providers estimate that between 85 and 90 percent of all e-mails are spam.

2.4.10 Copyright violations:

Copyright infringement is the act of violating, pirating, or stealing the exclusive rights of a copyright holder by the unauthorised use of a copyrighted material or work [14]. Internet-based copyright infringements have transitioned to sharing systems such as peer-to-peer networks, which allow users to communicate directly with one another.

2.4.11 Identity-related crimes

Using someone else's identity to achieve an advantage that you are not entitled to is a form of identity theft. Using another person's identity to commit a crime hides the offender's identity and further confuses law enforcement officers into believing that the victim is in reality the criminal [66]. As more data, services, and transactions move to global networks, crimes like these become more concerning.

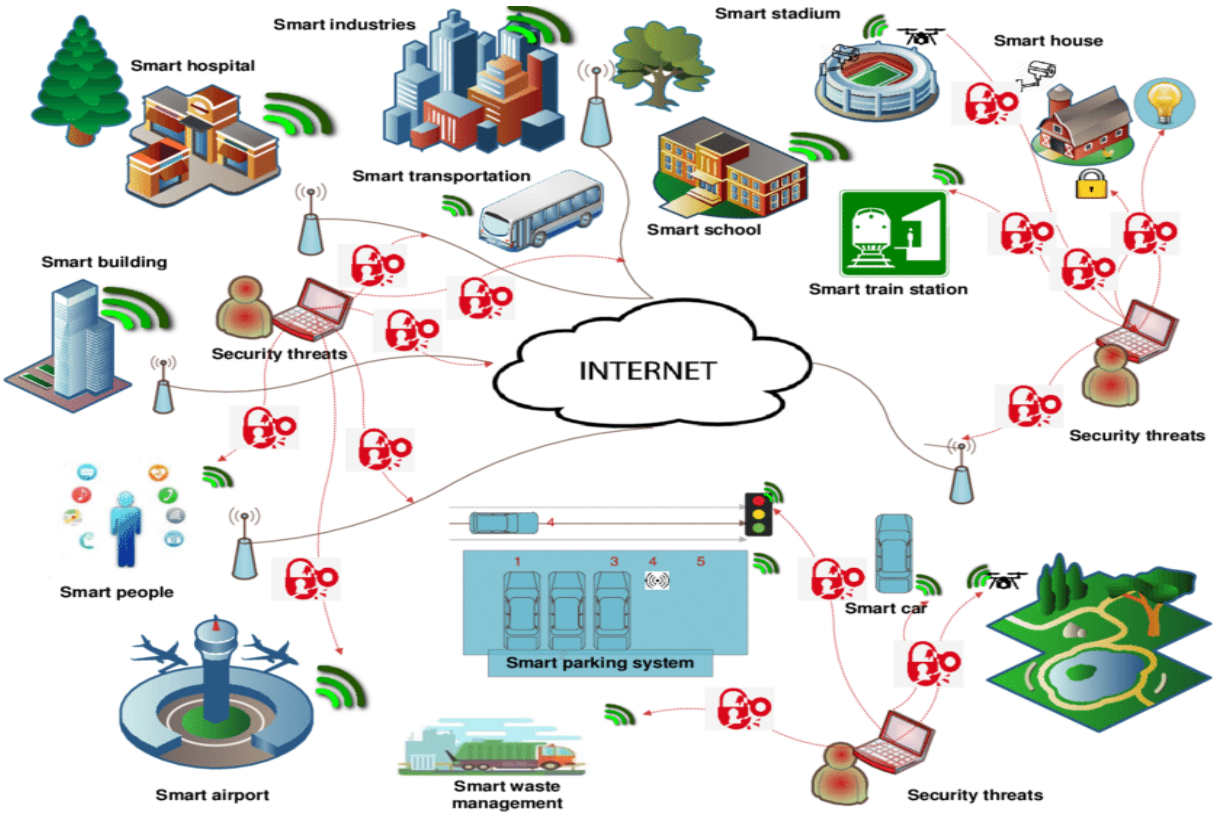


Figure.2.4 An illustration of Security Concerns in an Internet of Things Environment. Adopted from [119]

2.5 Cyber security assessment metrics and domains

The term "metric" refers to a unit of measurement. It is described as a standard of measurement in the current guide to security metrics [118]. Attributes and behaviours of interest can be measured through metrics. Consistent metrics help us better comprehend, control, and, in the event of a threat, protect against a given phenomenon In the words of James Harrington, a performance engineer, measurement is the first step toward control and improvement [119]. Clarity and unambiguity are among the most common criteria of quality metrics. Additionally, it facilitates decision-making and prevents subjective interpretation [119]. A solid threat metric aids in decision-making since it is concise and easy to understand [119].

The Allied Business Intelligence (ABI) research presented a cyber-security index [13] in 2014 that proposed metrics such as Legal Measures, Technical Measures, Organizational Measures, Capacity Building and cooperation to facilitate the measurement of cyber security. This study therefore will analyse each of these measures in addition to Threat Intelligence, Threat change management and Data protection to specify an Internet of Things cyber security assessment model.

Additionally, the Global Cyber security Agenda (GCA) that was launched by [16] for world-wide multi-stakeholder collaboration towards a safer and more secure information society presented five work areas as cyber security metrics. They are: legal measures, technical measures, organisational measures, capacity building, and cooperation, amongst other things. A country's intensity, preparedness and adoption in cyber security must be linked with these five parameters that constitute the basis of indicators for the cyber security assessment model, according to [16]. Similar arguments have been made [118] that measurements alone are insufficient to convey the threat level of an organisation. A more robust security posture can be achieved through the use of metrics and an organised approach to identifying and reducing threats [117].

Because of the nature and dynamics of the IoT, this study uses Intensity, Adoption and Readiness as domains for aligning the metrics to guide the development of an Internet of

Things Cyber security Assessment Model. Intensity is borrowed from the Generic threat matrix in section 2.5.1.6 of this study, Adoption is borrowed from the Security Diffusion Model in section 2.5.1.7 of this study, and Readiness is borrowed from the holistic digital forensic readiness (DFR) model in section 2.5.1.5 of this study.

2.5.1 Intensity as a domain an assessment model

According to [38], "intensity" describes the diligence and perseverance with which a danger pursues its purpose. When it comes to threat intensity, it's important to know how far and what risks a threat is willing to take to achieve its objectives. Intense threats are considered more harmful since they have a strong desire to achieve a goal. There should also be a focus on securing individual, organisational, and system layers of IoT cyber security [44].

Security systems and networks use protection intensity to determine the degree of protection they can provide to a moving object [18]. As stated by [18], the intensity of Internet of Things cyber security should be in terms of cyber security at the levels of the Individual, Organization and the state legal system. Therefore, as the researcher develops the model the following factors that show extent of the intensity of Internet of Things cyber security will be paramount. Secure and dependable information infrastructures (assured accessibility, availability, reliability, and service continuity); Policies to build confidence; The correct legal framework; Justice and law enforcement officials familiar with IoT and related cyber security issues. Management tools for securing information E - commerce, e-finance, health and government services and procedures to preserve human rights (such as privacy) all benefit from the use of security implementation tools. The escalating intensity of cyber-attacks on the IoT devices and networks is a key factor driving the need towards providing security to hyper-connected technologies [39].

2.5.2 Readiness as a domain in assessment model

Assessment is the act of evaluating someone or something [39]. Readiness is the state of being entirely prepared for something [39]. Thus, the readiness evaluation is an official measurement of the preparedness for a big shift or a new project of an enterprise/industry

as an individual component or as a community. Assessment of an industrial company's preparedness is important since it helps to adapt its processes and information architecture so that it can take use of the most up-to-date and accurate information accessible in the enterprise today [126].

Forensic digital preparedness is defined by ISO/IEC 27001 [96] as the act of preparing for a digital inquiry in advance of an incident taking place. If a cyber-attack were successful, the repercussions of not adding cyber security and forensic capability into IoT may be dire. Because of this, it is necessary to build digital forensic readiness and cyber security evaluation in tandem [81].

Decision-makers may also feel justified in ignoring the security readiness of IoT technology in their firms, according to [81]. A solid and well-considered IoT security plan, however, is still necessary. Due to IoT devices' role in numerous security incidents, including actual attacks, the vast majority of companies have already encountered at least one security problem.

2.5.3 Adoption as a domain in assessment model

Adopter characteristics is used as adoption and it is a metric to guide the development of an Internet of Things Cyber security Assessment Model. In this research, adoption is measured as the individual traits that influence IoT technology user’s intention with respect to security measures. Understanding the motivations of end-users to embrace IoT technology is critical to a project's success, as well as providing their perspectives and experiences of using IoT [81].

IoT vulnerabilities like the Mirai botnet and Stuxnet have resulted in major financial losses and disruptions to operations [81]. However, it is stated that security is an enabler and boosts the adoption of IoT in the company. Adoption of the Internet of Things necessitates a close examination. Since the Internet of Things (IoT) presents a wide range of cyber risk challenges, businesses that use IoT need to plan ahead to address these issues and keep up with ever-increasing regulatory obligations.

2.6 Cyber security Assessment Models

In the words of [18], a cyber security model is a predetermined set of policies and processes that enhance cyber security strategy in an environment. In addition to providing theoretical and practical guidance, it is documented for future reference. Using an assessment model, a country's existing level of cyber security capabilities, practises, procedures, and methodologies, as well as defined goals and priorities, can be evaluated against a benchmark. A model such as this can be developed in order to reduce the undiscovered vulnerabilities and misconfigurations that exist inside a specific environment, such as a country, industry, or sector [19]. As a result of the models described in Section 2.6.1 through 2.6.3, it was possible for the researcher to isolate the adoption, intensity, and preparedness dimensions for use in developing the IoT cyber security assessment model.

2.6.1 The holistic digital forensic readiness (DFR) model.

The ISO/IEC 27001 international standard is used as the basis for a comprehensive digital forensic readiness (DFR) model. It is possible to use this approach for a variety of digital investigations and evidence. ISO/IEC 27043 defines the readiness process as a set of planning, implementation, assessment, and concurrent process groups to be followed. By replacing DFR with organisational readiness and IoT security processes, a proposed proactive-based IoT-FR Model addresses this issue.

Organizational procedures handle DFR requirements that affect the entire business. Readiness processes guarantee that important data and prospective digital forensic data (DF) are recognised, collected, processed, and stored in accordance with the specifications outlined in the organisational processes. This includes the identification of essential data sources inside a business, as well as the implementation and monitoring of disaster recovery (DR) tools. To assure data integrity and confidentiality, both in transit and at rest, a layered security approach to the Internet of Things (IoT) is necessary. When creating a DFR, IoT security is essential to meet legal, regulatory, and organisational requirements.

The researchers conducted an investigation into cyber vulnerabilities in healthcare critical infrastructures over the last 15 years based on real-world projects [18]. The authors assert that the data complies with the European Commission's Directive on Critical Infrastructures. Probabilistic and quantitative methodologies were used by the writers. Access control and authentication as well as data integrity and loss are all potential threats to eHealth systems, according to the study's conclusions.

The principles for using computational intelligence in IoT security are presented in an overview of security challenges in IoT enabled cyber physical systems [50]. It looks at how evolutionary computation and other forms of computational intelligence are utilized to defend IoT systems in particular. [55] investigates the interdependencies of many key infrastructures. These dependencies, according to the authors, may pose a security concern. Because of the linkages, a failure in one infrastructure can result in breakdowns in its dependent infrastructures. For finding dependencies and analysing consequences, the study takes a holistic, dynamic, and quantitative approach.

The authors of [38] examine critical infrastructure protection measures and conclude that, in addition to standard security procedures, intelligent mechanisms are required. [38] introduces a paradigm for developing resilient distributed intrusion detection systems for critical infrastructures. This model works in a distributed environment. To identify and rank key communication flows, the model employs a risk assessment technique by enforcing a shortest-path routing algorithm, the goal is to reduce the number of deployed detection devices and reduce communications latency.

[46] presented a model and methodology for modelling and assessing security of the IoTs. The model aided in the creation of graphical security models for the Internet of Things. [44] created a graphical security model for the IoT in the model and demonstrated the model’s benefits by demonstrating IoT networks based on a wireless body area network (WBAN) and a wireless sensor network (WSN). In general, the methodology included five processes for identifying attack scenarios, analysing IoT security using well-defined security metrics and evaluating the efficacy of defense tactics. A study of two examples of the IoT networks was used to demonstrate the model’s

benefits. The findings demonstrated the capabilities of the proposed model on minimizing the effects of prospective assaults and evaluating the security of large-scale networks using the analytical results. In the research, a five-step paradigm for modelling and analysing security for the Internet of Things was provided, which included (a) pre-processing, (b) security model creation, (c) visualization and storage, (d) security analysis and changes and updates. An IoT Generator was developed comprising of a Security Model Generator and a Security Evaluator as part of the model.

For the IoT networks, [38] presented an automated security evaluation approach. To predict vulnerability metrics, the methodology first used machine learning and natural language processing to examine vulnerability descriptions. The predicted metrics are then fed into a two-layered graphical security model, which includes an attack graph on the top layer to show network connectivity and an attack tree on the bottom layer to provide vulnerability information for each node in the network. By collecting probable attack pathways, our security model automatically analyzed the security of the IoT network. A proof-of-concept smart building system model with a range of real-world IoT devices and possible vulnerabilities used to assess the practicality of the method. The suggested methodology was found to be effective in terms of automatically predicting the vulnerability metrics of new vulnerabilities with an average accuracy of more than 90% and finding the most vulnerable attack paths within an IoT network. However, the studies by [38] were outside Africa, whose context may not be as close to the Ugandan context and therefore incompatibility and direct application may be a challenge.

According to [109], a high-level target state for organisations that integrate IoT devices and/or services was identified using several cyber risk assessment approaches. Using the organization's current state as a starting point, a high-level transformation roadmap was developed to show how the company can get to their desired state. A goal-oriented strategy and the Internet of Things Micro Mart model were utilised to tailor the transformation roadmap for IoT risk impact assessments. Standardizing IoT risk impact assessments was one of the research's primary contributions, as were design imperatives for transformation, which outlined how IoT firms may achieve their ideal state by

applying a Goal-Oriented methodology based on their current situation. A single cyber risk assessment model has been established through an epistemological investigation. Calculating the economic impact of cyber risk and developing an international strategy for risk assessment are all possible with these tools, as is preparing for cyber attacks in advance through the purchase of insurance, for example. New approaches to IoT risk analysis include functional dependency, network-based linear dependency modelling, IoT risk effect assessment using a goal-oriented strategy, and a connection between the Goal-Oriented Approach and the IoT MM model.

Businesses must be digital forensically prepared for incidents involving the compromise of Internet of Things devices as well. Digital forensic readiness (DFR) can be improved by forensic-by-design. Forensic readiness (DFR) capabilities are the ability of an organization's investigators to maximise the use of digital artefacts while minimising the cost of conducting an investigation [113]. [114]. Using DFR, firms can better prepare for cyberattacks by assessing, planning, and preparing ahead of time [114].

An worldwide standard, like as ISO/IEC 27001, shows that applying DFR processes has various advantages for organisations. The digital investigative process necessitates making the ready process class essential [74]. Preparation allows companies to make the most of potential uses for digital evidence by ensuring that relevant and useful forensic data is captured and stored in an appropriate format that minimises interruptions to business operations during a real incident investigation by making sure that the technology, people and processes required to conduct an investigation are clearly identified then put into place and optimised across the organisation.

2.6.2 Generic threat matrix

There is a model for arranging a group of linked indicators into a generic threat matrix. This approach was created to aid in the risk and vulnerability assessment process during the OTA stage. Risk and vulnerability assessments begin with an Operational Threat Assessment (OTA), which is designed to give an accurate picture of the level of danger facing a certain organisation. For defining hostile cyber threats, the generic threat matrix

provides consistent and unambiguous threat measurements and models [107]. The matrix was created by Sandia to identify and categorise threats to specific targets. It is also possible to determine possible attack paths that could be supported by the asserted capability and to identify proper mitigation procedures to stop attacks by using the generic threat matrix. Further, [108] emphasises the importance of accurate threat assessment in risk management.

The matrix identifies characteristics that aid the analyst in classifying threats according to their overall capabilities. This categorization enables the representation of the whole spectrum of threat without tagging a specific threat with a name (and its associated preconceived beliefs). The model examines two groups of threat qualities: commitment attributes (Intensity, Time, and Stealth), which represent the threat's willingness to act, and resource attributes (Technical people, Knowledge, and Access), which reflect the threat's capability [106].

According to this view, each characteristic is defined by a distinct measure. Some measures are quantitative (for example, the number of technical individuals), while others are qualitative (for example, the number of technical personnel) (the level of cyber knowledge). This study takes the intensity metric from this model and applies it to the development of an IoT Cybersecurity Assessment Model.

2.6.3 Security Diffusion Model

[105] created a model to study how people use computer security in their homes. For this model, there are five main components: (Adopter Characteristics, Characteristics of Innovation, communications channels, social consequences of adoption, and the adopter decision process). According to the model, the user's risk tolerance, risk awareness, and perceived self-efficacy of implementing security measures were all taken into consideration, as well as the user's general computer self-efficacy perception. The concept asserts that, in order for an innovation to be adopted, its perceived features must be taken into account. This was tested by the construct of perceived suitability of the

proposed security solution, the perceived effectiveness of the security solution, and the perceived complexity of executing the recommended security solution.

2.7 Generalized Cyber Security Assessment Models

Other models for cyber security assessment are briefly discussed below:

2.7.1 ISO IEC 27001

In the context of an organisation, ISO/IEC 27001:2013 provides the requirements for creating, implementing, maintaining, and upgrading an information security management system. It also specifies requirements for assessing and addressing the organization's specific information security concerns. It doesn't matter what type, size, or nature of organisation you are; the requirements in ISO/IEC 27001:2013 are generic.

A cybersecurity model based on international standards that specify requirements for administering information security management systems (ISMS) is known as the ISO 27001 cybersecurity model [18]. In order to meet the requirements of ISO 27001, enterprises must put in place procedures to detect security threats that affect their IT systems. Several controls are recommended by ISO 27001 standards to combat the highlighted dangers. In order to avoid being hacked, a company must have appropriate security controls to reduce security risks. Over the course of 14 categories, the ISO 27001 standard proposes 114 controls. Two controls are included in information security policies; seven controls outline the duties for various tasks; and six controls help employees understand their role in preserving information security in the category of human resource security.

2.7.2 NIST Cybersecurity Model

The architecture of the NIST Cybersecurity model was focused on protecting critical facilities [102]. Private organisations, on the other hand, use it to beef up their online security measures. Managing the dangers to data and information security can be accomplished through the NIST's five functions: identification, protection, detection,

response, and recovery. The NIST guidelines, on the other hand, are geared toward federal agencies and must be adapted for use by businesses in general and the Internet of Things in particular [117]. The NIST model requires a complete current cyber profile and maturity level, but no model is provided for these processes [102].

2.7.3 COBIT

IT security, governance and management are all integrated into the COBIT model, which is the Control Objectives for Information and Related Technologies (COBIT). The model was created and is being maintained by ISACA [40], the Information Systems Audit and Control Association. Using the COBIT cybersecurity model can help companies improve product quality while adhering to more stringent security standards. Stakeholder expectations, end-to-end procedural controls for organisations and the development of a single yet integrated security model were the driving forces for the design of the model [119].

2.7.4 COSO

Organizations use COSO (Committee of Sponsoring Organizations) to identify and manage cyber security threats [115]. Monitoring, auditing, reporting, and regulating are just a few of the key components that went into the creation of this model. A total of 17 needs are included in the model, which can be broken down into five groups. Control environments, risk assessments, control activities, information and communication, and monitoring and control are all included in this category. In order to build sound methods for recognising and managing risks, all of the model's components collaborate. As a result of using the model, the organisation is able to identify and assess security threats at all levels of the organisation. It also recommends communication strategies for conveying information risks and security objectives up or down in an organisation [116]. Security events may be monitored in real time, allowing for timely reactions.

2.7.5 General Specifications of a Cyber Security Model

[5] Defines the main cyber security model’s main processes as Identity, Protect, Detect, Respond, and Recover. [5] Further attempts to define each of these processes as follows:

Identify: The identification process helps the entity or individual identify the existing cybersecurity critical elements within the environment. These could include IT assets, resources, information, and other types of information.

Protect: This phase is a proactive stage and ensures steps are taken for access control, data security, and maintenance, among others.

Detect: Using this technique, the entity is able to discover potential breaches by monitoring logs and implementing intrusion detection procedures at the device, system, and network levels.

Respond: The respond phase starts once a breach is detected. In this phase, the entity will have protocols to review and understand the breach, fix the vulnerability, and prepare for the recovery phase.

Recover: During this phase, Recovery procedures, like disaster recovery and backup plans, will be invoked. These processes are summarised in Figure 2.2 Below.

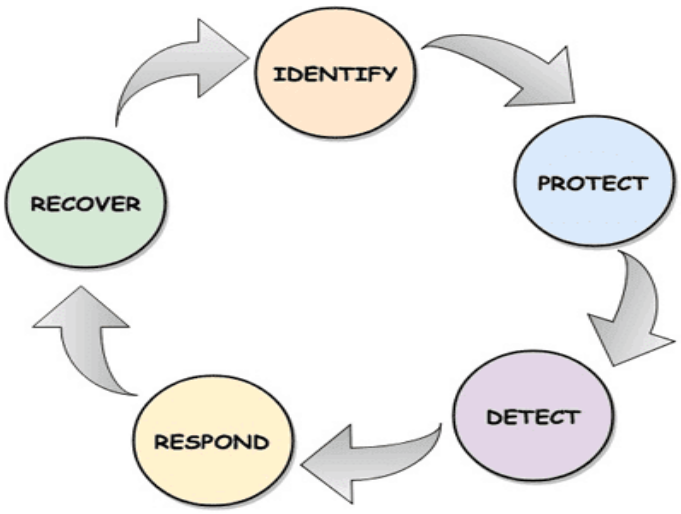


Figure 2.5 General cybersecurity processes. Source [5]

2.8 Methods of Validation of a Cyber Security Assessment Model

According to [58], the Delphi technique or Delphi method is one of the methods that can be employed in validating a designed cybersecurity model. According to [76], the Delphi technique searches for consensus opinions of a group of experts about future events.

According to [59], the Delphi method is a group communication method used to get expert agreement and viewpoints on a certain topic. The Delphi method is a consensus-building approach that enables decision-making by drawing on the knowledge and experience of relevant experts [91]. In addition to helping with consensus formation, it can also be utilised to help reach a decision. As an iterative procedure, the Delphi method utilises the same group of experts in successive rounds of surveying them. The results of previous rounds are used to inform the current round. With regards to how many rounds a Delphi process can have, the majority of processes have three or four rounds. It has been widely utilised to predict the future of science management, as well as computer science and cyber security. The Delphi technique's usage of experts is also notable because experts' opinions are the product of this method. In [60], he stated that the Delphi method needed seven or more experts.

An additional recommendation is to use the Software product Quality Requirements and Evaluation (SQuARE) standards to validate a cyber security model. [83] According to the SQuaRE standards for ontologies, these properties include structural, functional adequacy, adaptability; dependability; transferability; maintainability; and operability. This helps to discover the model's faults as well as strengths.

2.9 Reviewed cybersecurity assessment models and gaps identified.

Table 2.3 Analysis of the cybersecurity assessment models and gaps. Source :(Researcher)

Title	Author (S)	Key Focus Areas	Gaps/Recommendations
NIST Cybersecurity Model [14]	NIST, 2014	The NIST model aims to secure critical infrastructures and describe five functions: identifying, protecting, detecting, responding, and recovering, that manage the	The NIST model is created for Federal Agencies and requires changes to apply to businesses in general and the IoT.

		risks to data and information security.	The model less focuses on the adoption aspect of security management in IoT organisations.
COSO (Committee of Sponsoring Organizations) model	Al-Moshaigeh, A., Dickins, D., & Higgs, J. L. (2019).	The model aims at identifying and managing cybersecurity risks in organizations through monitoring, auditing, reporting, controlling, among others. It also allows collaboration of model components.	Model only focuses on cyber security risk management in organizations. It focuses less on the adoption and readiness aspects of security management of the IoT phenomenon.
COBIT- Control Objectives for Information and Related Technologies model	Almuhammadi, S., & Alsaleh, M. (2017).	The approach blends the best features of a company's operations into its information technology security, governance, and management. The model helps companies improve product quality while adhering to enhanced security practices.	Stakeholder cybersecurity expectations are only met by end-to-end procedural controls for firms, according to the model, which emphasises solely that. But puts less focus on other dimensions such as intensity and adoption that contribute to sound cybersecurity and secure IoT technologies.
IoT Cybersecurity	Ali, A. (2019).	The study focused on current cybersecurity models for	The models does not cover the organisational

Models [10]		protection and privacy issues related to cyber security. It also reviewed these models concerning cyber security in IoT.	view of readiness and adoption of security on for IoT applications. .
ISO/IEC 27001/ISO 27002	Radanliev, P., De Roure, C.D., Nurse, .R.C., Nicolescu, R., Huth, M., Cannady, C., Montalvo, R.M., Cannady, S., (2018).	Using the concept, firms are required to put in place mechanisms for detecting security threats that could affect their information systems.	The model focuses on putting in place controls that impact information systems in organizations. It less focuses on the readiness and adoption security dimensions beyond the organizational boundaries and IoT cyber security.
The holistic digital forensic readiness (DFR) model.	Kebande, V. R., Mudau, P. P., Ikuesan, R. A., Venter, H. S., & Choo, K. K. R. (2020).	The holistic digital forensic readiness (DFR) enables organizations to assess, plan, and prepare for cyber incidents in order to minimize the impacts. This model consist of a) Organisational processes, b) Readiness processes and c) IoT security layer processes.	Although the model does cover the organizational readiness, and security. It does not touch the aspect of Intensity.
The generic threat matrix	Mateski, M., Trevino, C. M., Veitch, C. K., Michalski, J., Harris, J. M., Maruoka, S., &	The generic threat matrix characterizes and differentiates threats against targets of interest.	The model is not based on the international standard. The model less focuses on the readiness

	Frye, J. (2012).	Additionally, the generic threat matrix allows analysts to (1) identify potential attack paths that could be supported by the asserted capability and (2) identify proper mitigation steps to thwart attacks.	and adoption security dimensions beyond the organizational boundaries and IoT cyber security.
Security Diffusion Model	Conklin, W. A. (2006).	Using the Security Diffusion Model, researchers examine how people use computer security at home. Essentially there are five different parts to the model (Adopter Characteristics, Characteristics of Innovation, communications channels, social consequences of adoption, and the adopter decision process).	The model less focuses on the intensity security dimensions beyond the organizational boundaries and IoT cyber security.

2.10 Conceptual model

This study postulated that the Dependable Variable (DV), IoT Cyber Security Assessment Index (IoT CSAI) independent variables (IV) that can be divided into three basic categories, namely Readiness, Intensity and adoption factor variables. These variables were adopted from the gaps in existing Cyber security Assessment Models. The Secondary data sources from literature review and primary data sources from interviews

and questionnaires helped to understand and analyse the factors that contribute to the Internet of Things cyber security Intensity, Readiness and Adoption, which the researcher uses as parameters for the Cyber security Assessment Model that is specific to Internet of Things.

Figure 2.4. Conceptual Model, IoT Cyber Security Assessment Model (Source-

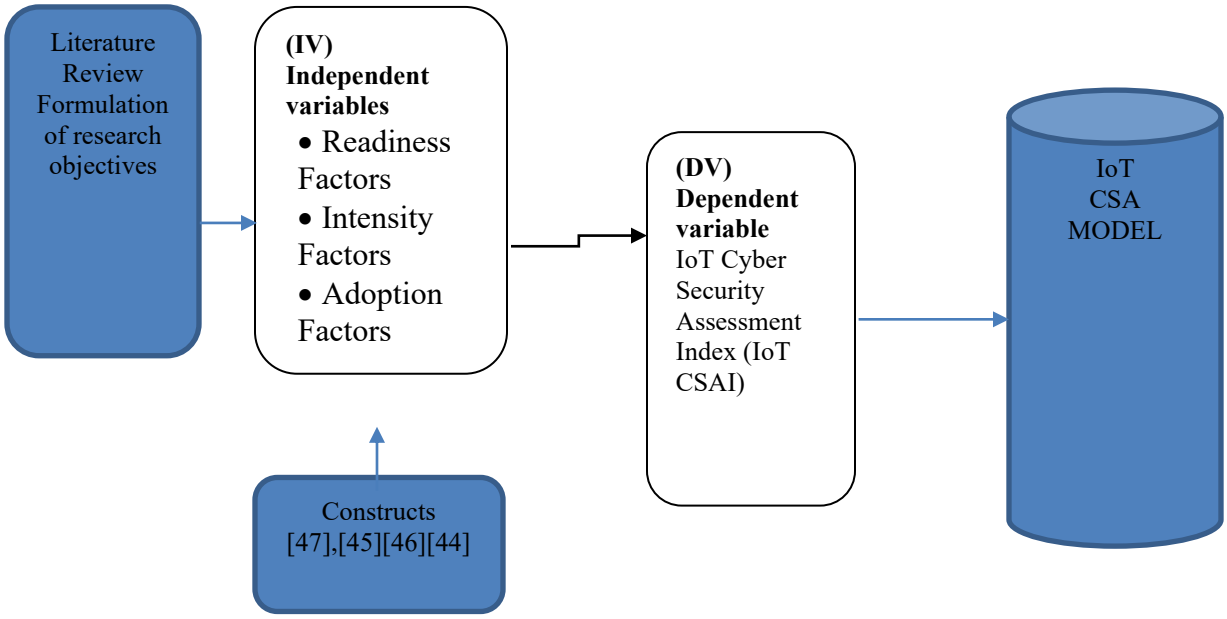


Figure 2.6: Conceptual Model (Source: Researcher).

2.11 Conclusion

The Chapter discussed and summarized the investigation into the related works specifically on the IoT cyber security threat landscape, especially about unique IoT Characteristics that make IoTs susceptible to Cyber attacks and relevant methodologies applicable to this research. Analyzing IoT cyber security factors is challenging because security factors are a subjective matter demanding socio-technical systems theory.

This chapter helped achieve Research Objective one and answer research question one, namely, to review literature on the current cyber security landscape, cyber security assessment models and determine their adequacy to address unique cyber security risks associated with the Internet of Things phenomenon. Literature on validation of cyber security models is also presented. Lastly, the reviewed cyber security assessment models therein are characterized to identify the research gaps that inform the need for the current study. The Chapter concludes by specifying a conceptual model and identifying the independent and dependent variables. In the subsequent chapter, we'll explain the research approach used in this project. The research approach used in this study will be discussed in detail in the following chapter.

CHAPTER THREE
METHODOLOGY

3.0 Introduction

In order to address the research problem and achieve the research goals outlined in Chapter One, this chapter describes the methodology used. Research philosophy or epistemology that is relevant to the knowledge claim must be described before the optimal research approach can be chosen. As a result, the research strategies and tools used in the study are described in detail in the next section. The research setting, target population, and sampling techniques are next discussed. Finally, data collection methods are discussed, and the approaches used for ensuring data reliability and validation presented, as well as the ethical observations during the research. The overall research design is summarised in Figure 3.1 below

3.1 Research Design

[85] defines research design as a method of critical or scientific investigation. [82] suggest that design is a logical depiction of the steps or tasks, from issue formulation through the creation of conclusions or theory, which are required in planning or conducting a study. The research design is often summarised a research onion concept, as illustrated in Figure 3.1

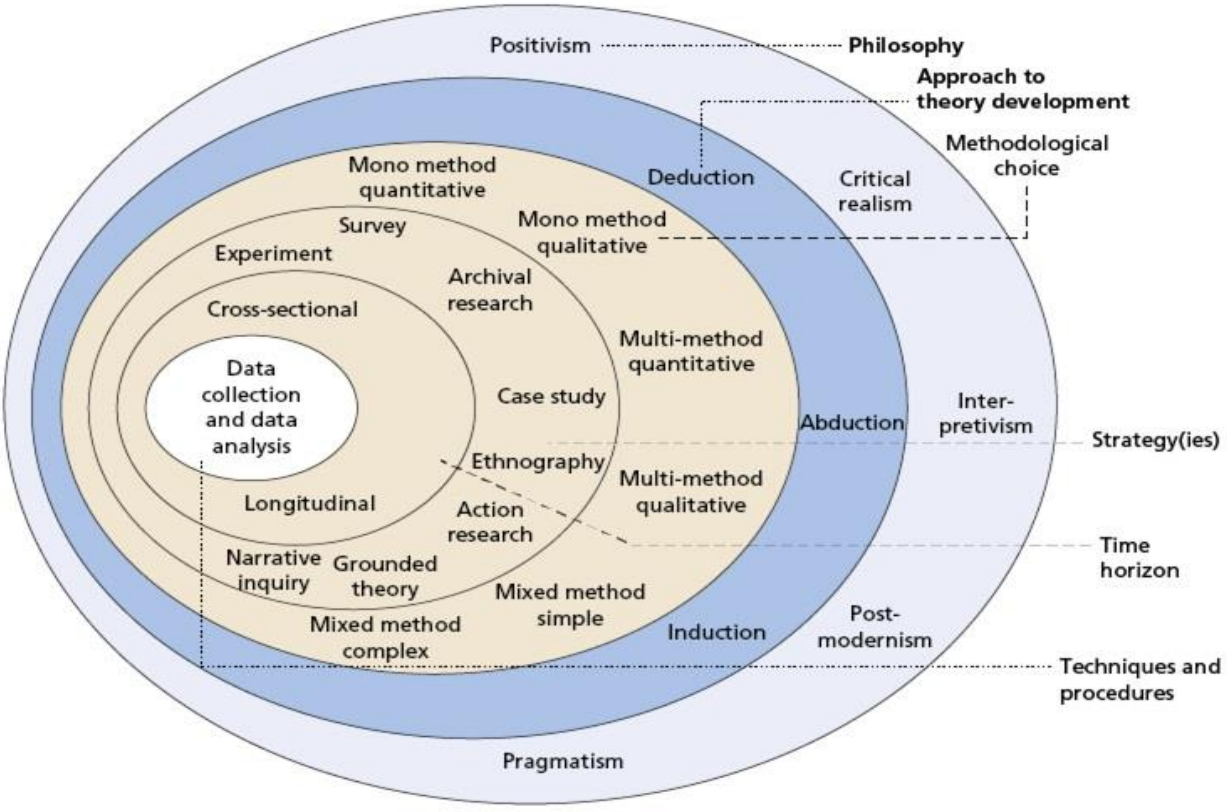
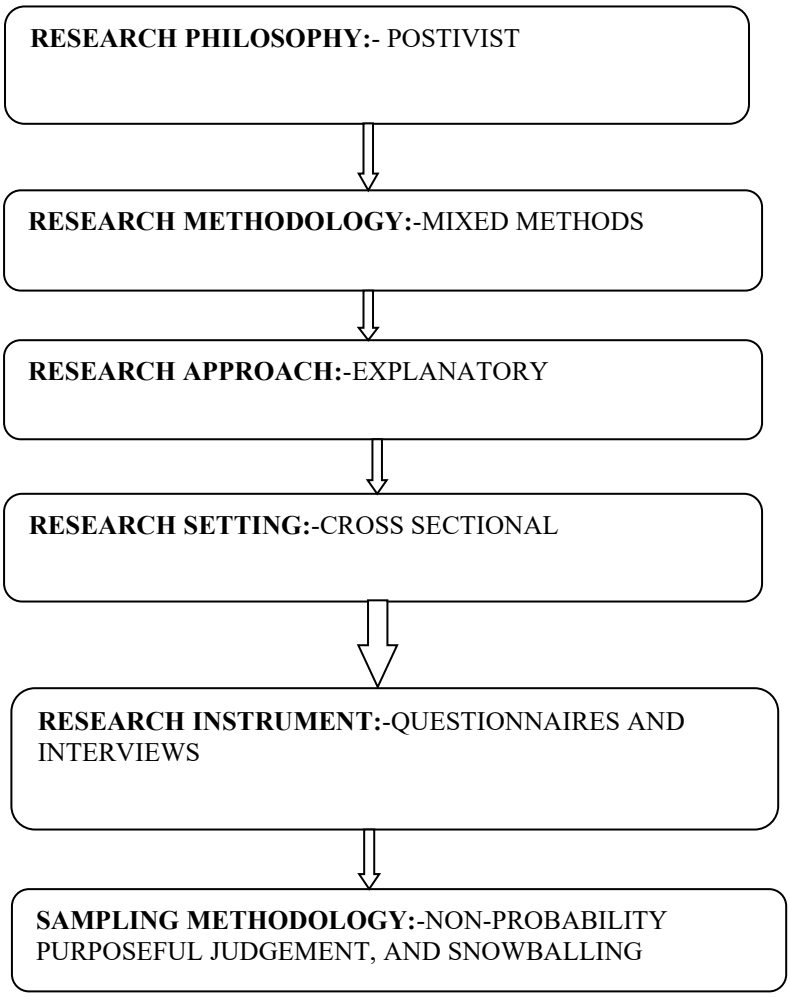


Figure 3.1: The research onion adopted from [21].

According to [21], a "research onion" is a framework for guiding the organisation of a research approach. The research onion concept provides a solid foundation for a logical and substantiated research design [22].

It is common for researchers to begin with the outermost layer of a study design, which is the philosophy layer, before working their way down to the methodologies and procedures layer. In each layer of the onion, researchers have a variety of possibilities from which to choose based on their own study goals, hypotheses, and questions. Critical review of the problem statement, research objectives, and the attendant research questions presented by the researcher in Chapter 1, and consequently the mapping of these to the “research onion”, resulted in the specific overall design schematic for the research as presented in Figure 3.2 below



Key

⇩ Research process flow

Figure 3.2 Schematic for research design

Source: Researcher

The detailed discussions on the choice of specific design options are as detailed below:-

3.2 Research Philosophy

[22] defines philosophy as the reasoned and critical pursuit of truth in a certain field. A more specific definition of philosophy is "the study of ideas with the goal of uncovering the truth" [24]. Questions regarding the world, our understanding of it, and what we can do about it are raised by philosophers. [25] Metaphysics, epistemology, and ethics are three branches of philosophy that can be used to answer philosophical questions. The philosophy of mind, language, and science are all part of metaphysics. Epistemology is the other half of these philosophies, which investigates the world's cognitive background [24]. The Greek word epistêmê, which means "theory of knowledge," is the root of the English word "epistemology" [22]. Philosophies of law, social justice, and aesthetics all fall within ethics. [29][30]

In [22], research philosophy is the philosophy of knowledge and is critical to determining the research paradigm. Thomas Kuhn who is known for the term ‘paradigm’, characterizes a paradigm as “An integrated cluster of substantive concepts, variables and problems attached with corresponding methodological approaches and tools…” [22].

[22] identifies three major research paradigms that support theoretical propositions:

(i) **Positivist.** The positivist research ideology systematises knowledge generation through quantification, primarily to improve the precision with which parameters are described and correlations between them are discerned [26], thinking that reality is objectively provided and can be articulated quantitatively [27]. It is primarily concerned with quantitative measures of variables and is linked to research methods such as surveys, experimental, and quasi-experimental approaches [28].

(ii) **Anti-Positivist:** Anti-positivist philosophy emphasises that individuals observe and interpret social reality in accordance with their ideological perspectives, and that knowledge is obtained via experience rather than from the outside [28]. Interpretivism is another name for this type of research philosophy. According to the interpretivism school of thought, researchers are free to offer their own interpretations of the data they collect.

As a result, interpretivism incorporates human interest into the study of the human condition [28]. The goal of interpretive research, according to [30], is to produce new and more detailed interpretations of social environments and settings. In order to address the study questions, an interpretivist researcher must also acknowledge the complexity by gathering meaningful data from the participants [31].

(iii) **Critical Theory:** Critical theory, according to [32], relies on ideological critique and action research to investigate the existing phenomena, and that reality is constantly being shaped by individuals who have limited ability to change their social and economic status owing to numerous restrictions, and that critical theory is mainly focused on analysing these conditions or constraints [34].

It was determined that the positivist paradigm was the most appropriate approach in terms of its consistency with the research procedure outlined in Chapter One because the major objective was to evaluate links between various constructions and IoT cyber security readiness, intensity, and adoption. As a result, positivism was selected as the guiding concept for this study.

3.3 Approach to theory development

The three major processes of theory development are induction, deduction, and abduction, and they are collectively referred to as types of logical reasoning [25].The deductive strategy comprises testing a theory or hypothesis by a researcher and derives from it one or additional observational forecasts, which lends themselves to a straight experimental check [26]. Starting with the broad strokes and ending with the specific, deductive inquiry begins with a general theory and finishes with a specific one [25]. It is through hypothesis testing that the theory is either verified or rejected, or it may be adjusted [26].]

Understanding and seeing following singularities as asserted belongings to their speculative description associated to primary causal processes is the foundation of the abductive research technique [27]. In order to expand the nature of the underlying mechanisms in question, plausible models of the mechanisms must be created after

favourable results of their original plausibility have been obtained [27]. As the name suggests, abductive research aims to conduct a comprehensive analysis of the available information in order to discover new ideas.

There is no need for further observational testing as a result of the inductive technique, which involves simultaneously developing and justifying concepts. An important aspect of this technique is working from the bottom up, drawing on participants' perspectives in order to generate larger themes and develop a theory that connects the topics [18, 19]. To this, [20] adds that in the inductive technique, the investigator begins with specific explanations and measures and then detects the patterns and designs in the statistics. This method relies on data collection and analysis to identify patterns that suggest a connection between variables, and it is from these observations that generalisations, linkages, and hypotheses are developed [21].

Accordingly, an inductive approach was used in this study, as evidenced by an evaluation of various research methods. The model for IoT Cyber Security Assessment was developed with the use of induction, which was used to identify requirements from the acquired data. A basic theoretical model for IoT Cyber Security Assessment was developed based on the literature. The basic theoretical model was expanded based on information gathered from a survey.

3.4 Research strategy

There are a number of factors to consider when deciding what kind of technique to use in a certain research project [21]. There are six common study designs used by qualitative researchers [24]. a) Narrative research: the researcher studies a participant's life and asks questions to learn more about the tale of their life. b) Qualitative research: the researcher gathers data by interviewing participants and observing them.
B) Phenomenology: This type of research uses participants' data to characterise a phenomenon.

Grounded theory: the researcher draws a theory from the information collected from the participants themselves.

d) Ethnography: the researcher observes a cultural group of people in a natural context over a period of time.

e) Case study: the researcher conducts an in-depth examination of a particular case, which may be a programme, event, activity, process, or one or more individuals.

f) Survey research: the researcher gathers data to describe, compare, or explain participants' knowledge, attitudes, and behaviours.

The researcher employed a survey research approach in this investigation. Survey research is a process that uses questionnaires to collect data in order to develop conclusions about the attitudes, beliefs, views, and behaviours of those who participate [26].

Qualitative research makes heavy use of surveys [26]. As a result, a survey's value is in its ability to gather information of a wide variety from participants' knowledge that is not concerned with statistical data such as frequency and standard deviation, but rather with users' views and perceptions. Experience, understanding, and perception questions lend themselves well to qualitative surveys [28].

Self-administered or interviewer-administered survey research instruments are both options. A combination of both online and physical delivery options may also be used based on the interviewer's and respondent's availability, convenience, or personal preferences. While interviewer-administered surveys require the interviewer to be present, self-administered surveys require respondents to complete the questionnaires on their own, without any guidance or assistance. It is up to the interviewer to ensure that the questionnaire is administered correctly during an interviewer-administered survey.

The questionnaires in this study were printed on paper and given to the participants by the interviewer. Before commencing the questionnaire administration, the researcher explained to participants why they needed to answer the open-ended questions for qualitative analysis and how they could minimise interviewer bias by completing the questions. Only when a participant requested the researcher to explain a question that

they didn't understand was an individual consultation between the researcher and a participant. Rather than providing examples of possible responses, the researcher explained the situation to the participant.

3.5 Research Design

The study design is the overall strategy for addressing and answering the research questions [35]. A study's methodology can be influenced by the research philosophy it employs. Methodology includes the research plan, the study's time horizon needs, and the data gathering and data analysis methods examined and employed [37].

In a similar vein, [38] argues that a research design is based on the objectives for the research, specification of where the data is going to be collected from, how it is intended to be collected and analyzed, and consideration of possible challenges and ethical issues [44]. In the following sections, the researcher describes and elaborates on four components of the research design namely, the *research purpose, research method,* and *time horizon.*

3.5.1 Questionnaires

Questionnaires are a collection of questions that are distributed to study participants via paper or electronic means [83]. Questionnaires are a low-cost data gathering tool that may be distributed to a large number of people at once [84]. Depending on the research, questionnaires might include both open-ended and closed-ended questions. For qualitative research projects, open-ended questions are desirable, and researchers should ensure that the instructions are clear to avoid confusion and nonresponse from the participants [85].

A total of two surveys were utilised in this research (see Appendix I and II). Open-ended and closed-ended questions were included in the questionnaires for participants to

complete. Questionnaires are a collection of questions that are distributed to study participants via paper or electronic means [83]. Questionnaires are a low-cost data gathering tool that may be distributed to a large number of people at once [84]. Depending on the research, questionnaires might include both open-ended and closed-ended questions. For qualitative research projects, open-ended questions are desirable, and researchers should ensure that the instructions are clear to avoid confusion and nonresponse from the participants [85].

A total of two surveys were utilised in this research (see Appendix I and II). Open-ended and closed-ended questions were included in the questionnaires for participants to complete.

3.5.2 Interviews

Qualitative research employs in-depth one-on-one interviews with a small number of participants to gain a better understanding of their views on a certain idea, programme, or issue [88].

Structured, semi-structured, and unstructured interviews are all forms of interviewing. These are as follows:

Structured interviews: consist of a set of pre-determined questions that are answered in the same order by all interviews.

Unstructured interviews: are often the least dependable in terms of research because no questions are planned in advance and data gathering is done in an informal manner.. [more] A substantial amount of prejudice is associated with unstructured interviews.. Because of the wide range in question wording, it can be difficult to compare the responses of various respondents.

Semi-structured interviews: include both scheduled and unstructured interview elements Interviewers in semi-structured interviews prepare a series of questions for all interviewees to answer. It's possible that during interviews, extra questions will be asked in order to get to the bottom of some situations and provide more context.

Semi-structured interviews were used in this investigation. This is due to the researcher's desire to delve deeply into participants' personal and, at times, sensitive, thoughts, feelings, and beliefs regarding a specific IoT security phenomenon.

3.5 The study population and sampling

Population is described by [86] as a study entity that encompasses individuals, groups, organisations and the circumstances they are exposed to. This study population included adult individuals occupying positions such as Security Analysts, Information Technology specialists, PC Technicians, Information systems managers and heads, IT experts, administrators, IT security administrators and managers, and Information systems end-users. This study considered all these people as “all technical staff of the Cyber Security Unit and Emerging Technologies." The study was conducted in the Wakiso and Kampala districts, which form part of the urban districts of Uganda. It is also observed that internet connectivity is available mainly up to primary headquarters, which are always located in urban. It does cover only up to around 50 districts and not all the districts in Uganda [89]. Secondly, access to basic ICT information of internet services, IoT equipment, and stable telecommunication network and ICT facilities in these districts [89]. These are some of the requirements for cyber technologies and IoT.

3.6.1 Sampling and Sample Size

As a general rule, sampling is used to choose a sufficient number of participants from a vast population of potential participants. It includes everyone the researcher cares about in the study [89].

3.6.1.1 Purposive sampling

Purposive sampling, according to [89], is favoured when selecting individuals in positions that enable them to be more knowledgeable about respective fields. In that regard, the researcher employed purposive sampling to identify key interviewees with expertise in cybersecurity in Uganda. The researchers purposively choose 26 potential

participants from which the researcher could document an accurate representation of IoT cybersecurity practices to conduct the validation of the model.

3.6.1.2 Sample Size

According to the records officers of the various organisations that the study used as a unit of analysis, the total population emerged as 198 from both Wakiso and Kampala districts of Uganda. To simplify the process of determining the sample size for a finite population, Krejcie & Morgan (1970) [33] came up with a table using a sample size formula for a finite population. This formula helps the researcher determine the sample size without making an independent study on each of the samples. Krejcie & Morgan
state that for a population of between 190 to 200 persons, the researcher needs to get feedback from 127 persons. Therefore this study used a sample of 127 respondents from 7 firms (Ministry of ICT, National Information Technology Authority (NITA), Uganda Communications Commission (UCC), Uganda Police, Makerere University, Nkumba University, and Uganda People's Defence Forces (UPDF).

As a result of their accessibility and willingness to engage in the study, these companies were readily chosen for inclusion. The term "opportunity sampling" refers to convenience sampling. Using this strategy, researchers can pick volunteers based on their availability, accessibility, and desire to participate in a study [35].

All of the Cyber Security Unit and Emerging Technologies employees at each of these companies were selected using a purposive sampling approach because it was necessary to select respondents who already knew the necessary information. It is possible to select participants for a study through the use of a sampling technique called "purposeful sampling" [34]. This staff category was chosen because they are Key players in strategy implementation and management for the Cyber Security Unit and Emerging Technologies in the organizations.

Table 3.1 below shows a sample of 7 firms from which the study participants were chosen across the two districts of Kampala and wakiso.

Table 3. 1: Sample Breakdown.

District	Firm	No of Participants	Sampling Method
Kampala District	Ministry of ICT	40	Simple Random
Kampala District	NITA	15	Simple Random
Kampala District	UCC	16	Simple Random
Wakiso District	Uganda Police	15	Purposive
Kampala District	Makerere University	22	Simple Random
Wakiso District	Nkumba University	10	Purposive
Wakiso District	UPDF	9	Purposive
TOTAL	7	127	
Sampling for Model Validation			
Wakiso District	Nkumba University	4	Purposive
Kampala District	Ministry of ICT	3	Purposive
Kampala District	Makerere University	5	Purposive
Wakiso District	Uganda Police	3	Purposive
Kampala District	UCC	4	Purposive
Wakiso District	UPDF	3	Purposive
Kampala District	NITA	4	Purposive
TOTAL	7	26	

3.7 Data Analysis

Data were analyzed using both quantitative and qualitative techniques as follows;

a) Quantitative Analysis

Analyzing quantitative data means looking at data that can be expressed numerically rather than vocally, or data that can be numerically represented without losing any of its original significance. For example, category-based variables such as gender, ethnicity, or native language could be translated into integers without losing their meaning [28].
Quantitative data analysis is often used to quantify differences between groups, such as the popularity of various clothing colours, establish correlations between variables, and evaluate scientifically sound hypotheses [27].
There are two main branches of statistical methods/techniques used in quantitative data analysis: descriptive statistics and inferential statistics [28].

The SPSS statistical package was used for quantitative data analysis to analyze data, and thereafter-descriptive statistics and inferential statistics were generated. Results are presented and discussed in this Chapter Four.

b) Qualitative Analysis

Qualitative data were subjected to thematic analysis. Using a procedure known as thematic data analysis, researchers code data and then use the codes to create groups and themes. Analysis, organising, description and reporting of data themes are all possible using the thematic analysis [26]. It is crucial to read and re-read the data as many times as possible in order to find themes [27]. Thematic analysis helped to discover recurring themes in the data, which supplied the basis for the Internet of Things cybersecurity assessment model's model requirements.. According to [27], the six steps of theme analysis are as follows:

1. Familiarisation with the data
2. Coding
3. Theme development
4. Reviewing themes
5. Defining and naming themes
6. Writing up and producing the report

These steps were closely and carefully followed throughout the process of qualitative data analysis. This is expanded as follows;

Phase 1: Familiarization with the data

The goal of the familiarisation phase is for the researcher to become intimately acquainted with their own study data. In order to make sense of all the information, the researcher has to go through and reread everything. Listening and transcribing audio recordings is an example of how researchers might gain a general understanding of what participants are saying.

The answers to the study's questions were written by hand, and the researcher first read them all to gain a general sense of what the participants were saying and to underline interesting terms and idioms. The replies from the surveys were then typed into an Excel spreadsheet by the study's author. Afterward, the SPSS software was used to analyse the data entered in the Excel spreadsheet.

3.8 Reliability and validity of the instruments

Reliability refers to the degree to which a test, survey, surveillance, or other determining tool can be relied upon in similar circumstances across time [29]. Validity is a term that refers to the study findings' integrity and dependability [30].

Because of this, it is important to guarantee that data collection and research instruments are free of bias. In this study, different research participants were surveyed at different times and their answers exhibited consistency. All of the respondents were selected from a sample population based on predetermined selection criteria. For those who couldn't be contacted, an online version of the survey was made available. In addition, the sample criteria were used to choose participants for online surveys.

3.8.1 Validity

According to [25], Validity refers to the degree to which the result obtained from data analysis represents the phenomenon under study. It further measures how much the

measured values agree with the true values. [28] deliberate two categories of validity; contented rationality and criterion-related validity that is extrapolative and simultaneous Validity. Validity is classified into two categories: internal and external. Both internal and external validity are important in determining the validity of a research study's findings, but they are not interchangeable. It is imperative that a study's suitability, importance, and usefulness be assessed using both forms of evaluations [29].

For the study's internal validity, questions were included that helped describe an acceptable model for Internet of Things cybersecurity evaluation. It was through the survey's questions that the Internet of Things cybersecurity assessment model could be evaluated and improved by the survey's selected cybersecurity experts. The survey was given to the supervisor, professionals in the field of IoT and cybersecurity from Makerere University, and some questions were rephrased to increase their clarity and relevance. Closing-ended questions were altered to include more appropriate response possibilities to accommodate data examination [30]. Once all of the experts' input had been taken into account, the final instrument could be created.

The study's external validity was accomplished since it was taken into account from the beginning. To ensure that the results could be generalised, a representative sample selection method was used. The study's conclusions can be applied to a larger population than the sample size. The people who were asked to participate in the study did so willingly, and they answered all of the survey questions. This means that the findings of the study are of an externally valid nature.

Table 3.2: Cronbach's alpha coefficients for the study variables

Variable	*Number of items*	*Cronbach's Alpha value*
IoT threats exposure	9	.934
Risk determination of IoT	27	.968

Source: Primary Data

As shown in Table 3.2, all variables in the study a Cronbach alpha reliability coefficient above the acceptable minimum of 0.50 [30]. This indicates that the instrument used to collect data in this study was adequate.

3.9 Ethical Considerations

Ethics is concerned with valuing human behaviour. Participants in a study should feel valued and meaningful, and their human dignity should not be violated[78]. Masinde Muliro University of Science and Technology authorised the researcher to utilise their students as subjects in the study by obtaining a letter of approval. A participant information sheet was distributed to study participants, outlining the study's objectives, the participants' voluntary participation, and their ability to withdraw at any time. Additionally, participants signed a consent form prior to completing the surveys and conversing with the interviewers.

To guarantee that this study was conducted ethically, the following human rights were observed: free choice, anonymity, confidentiality, and informed consent. Throughout the study, anonymity and secrecy were maintained. According to [29], anonymity indicates that the data collected does not contain any personally identifiable information about the participants, such as their name, address, or email address, and hence cannot be linked to the participants' identities through their responses.

3.10 Summary

This Chapter presents the research philosophy, research design, and study population, sampling methods, data collection methods that the study adopted. In section 3.1, the researcher presents the research philosophy, where we describe and elaborate on the

research method, research strategy, and time horizon. Section 3.4 and 3.5 offer the research design and methods of data collection, respectively. In section 3.6, the researcher presents the study population, section 3.7 data analysis, 3.8 presents the reliability and validity of research instruments. Finally, section 3.9 emphasizes the ethical principles and that the research followed.

CHAPTER 4

DATA ANALYSIS AND PRESENTATION

4.1 INTRODUCTION

In the IoT Cyber Security readiness (ICSR) domain, a total of 80 responses were obtained from the 127 questionnaires sent out within the specified time. Thus a response rate of 63 per cent was achieved. Similarly, in the IoT Cyber Security intensity (ICSI), and IoT Cyber Security adoption (ICSA) domains, a total of 80 responses were obtained from the 127 questionnaires sent out within the specified duration, achieving a response rate of 63 per cent. [60] argues that response rates above 40 per cent are acceptable in survey based qualitative research on emerging technologies. Further, the response rates obtained in this research are comparable to response rates in recent studies on IoT Cyber Security adoption conducted in developing countries in Malaysia (49.14%), and India (48%) respectively [61]. The sample size of 127 is notably compatible to other recent studies utilizing snowballing sampling techniques [38][36][35].

4.1.1 Testing for non-response bias

According to [26], non-response bias refers to a situation in a survey in which non-respondents have opinions that are systematically different from those of the respondents.

Data from the respondents would be non-representative if non-response bias existed; this would compromise external validity of research findings [26]. According to [25], non-response bias testing often entails comparing the characteristics of respondents who returned completed surveys and those who did not. Among alternative methods for detecting non-response bias, a difference in means test, a t-test for independent samples, or a chi-square goodness of fit test can be utilised [36].

[66] suggests three methods of handling non-response bias namely:-

(i). A comparison of early and late responders is presented. The underlying premise is that participants who react late are statistically identical to non-respondents.

(ii). “Days to respond” method. The "days to respond" variable is coded as a continuous variable in this method, and it is used as an independent variable in the regression analysis.

(iii). Non-respondents are compared to those who responded. By following up with the original set of non-responders in order to obtain a specified number of responses, and then comparing their responses to those of the real respondents.

In this research, the “Days to respond” technique was used to test for non-response bias. The “days to respond” variable (CODED) produced non-significant results in the regression in terms of non-response bias, suggesting that it is less likely that the findings of this study were affected due to non-response bias [36]

4.1.2 Interview Data Analysis

Interview data analysis consisted of data reduction techniques as well as thematic analysis involving data categorization and coding [35][36]. The process started with raw data consisting of a section or the entire answer to one question [37]. This was then split into entities which in turn were ordered into categories [38]. Interview data from each respondent was first anaylsed independently, and then cross-case analysis applied to the corresponding questionnaire responses for the entire group of respondents [24] [25]

4.1.3 Questionnaire Data Analysis

The analysis of questionnaire data for each of the three research domains began with a classification of the responses and the assignment of a unique identification number to each response. The survey data was analysed using descriptive statistics generated by Version 26 of the Statistical programme and reliability tests and correlation analyses [30][31]. Least squares regression analysis was also employed to fit a linear probability model in order to investigate the influence of the independent variables on each of the dependable variables in the IoT Cyber Security readiness (ICSR), IoT Cyber Security Intensity (ICSI), and IoT Cyber Security Adoption (ICSA) domains, respectively[26][27][24][25].

4.2 Constructs and Individual Items for Measuring IoT Cyber Security Readiness (ICSR)

According to the ITU Model for assessment of cyber security [14], IoT Cyber Security Metrics of readiness focus on the technical, commercial, and physical infrastructures required to support IoT Cyber Security. Thus a country's IoT Cyber Security readiness is a key determinant of it's global cyber security preparedness , robustness, competitiveness, and a measure of the degree in which it's qualified to participate in the digital economy with enhanced IoT Cyber Security [16][94]

As discussed in Chapter 3, The Conceptual Model For IoT Cyber Security Readiness (ICSR) It was hypothesised that various independent variables influenced the dependent variable 'IoT Cyber Security Readiness,' including the broad categories of policy, regulatory, digital literacy, and technology.
These constructs and the individual items utilised to measure them are now enumerated.

4.2.1 Policy (POL) Construct

In this construct, the researcher sought to determine the effectiveness of the National CIRT (CERT.UG/CC) in managing cyber incidents in Uganda, the Availability and effectiveness of the Cyber law (Act), and the view of IoT Cyber Security as an eco-system on the variation of IoT Cyber Security readiness (ICSR) in the context of a developing country.

4.2.1.1 Items used to measure IoT Cyber Security policy (POL) construct

The details of the three items used to measure this construct follow:

(i). Effectiveness of the National CIRT (CERT.UG/CC) in managing cyber incidents in Uganda (BSD)

Uganda's official National Computer Security Incident Response Team is the Computer Emergency Response Team/Coordination Center (CERT.UG/CC). It was founded to assist in ensuring the protection of important information infrastructures and in developing the country's overall strategy for dealing with cyber security challenges. It acts as a focal point for advocating for the development and implementation of a national cyber security culture [18].

National CERT is a joint effort by the Ministry of Information and Communications Technology and the National Information Technology Authority-Uganda (NITA-U) that promotes communication between local and international professionals to aid in the resolution of security events.

In this study, the effectiveness of the CERT-UG/CC was evaluated against the objectives of the CERT namely to:

- Effectively manage cyber security incidents
- Improve information security awareness
- Provide analytical support, analysis & advice on cyber security in Ugan

(ii). IoT Cyber Security view as an ecosystem (BES). [14] proposes that IoT Cyber Security be defined beyond the traditional notion of computer security. Rather, it proposes that IoT Cyber Security be viewed as an ecosystem that includes networks, the personnel, the devices, the applications they deliver, and services offered on the networks. This eco-system view of IoT Cyber Security is being increasingly embraced the world over [14] and there was need access the applicability of this notion to increased IoT Cyber Security readiness in Uganda.

(iii). The Availability and effectiveness of the Cyber Crimes Act in Uganda development of a National IoT Cyber Security Strategy (NBS). A number of countries have developed national IoT Cyber Security strategies and policies with a view to the realisation of an all inclusive information security for socio-economic benefits associated with IoT Cyber Security [94].

For example, In Uganda, the Computer Misuse Act, 2011 makes provision for the safety and security of electronic transactions and information systems to prevent unlawful access, abuse or misuse of information systems including computers and mobile devices

as well as ensuring security of electronic transactions. It also establishes different categories of computer misuse offences and proposes mechanisms for investigation and prosecution of the cyber related offences.

4.2.1.2 Descriptive statistics for Policy construct items.

The means and standard deviations of aggregated measures for the three items used to measure the policy (POL) construct are illustrated in Table 4.1 and Figure 4.1 below

Table 4.1 Descriptive statistics for policy (POL) construct items.

Item	Mean	Std. Dev	Rank
Scale-POL	**4.304**	**1.282**	
BSD	4.445	1.449	2
BES	3.800	0.915	3
NBS	4.665	0.953	1

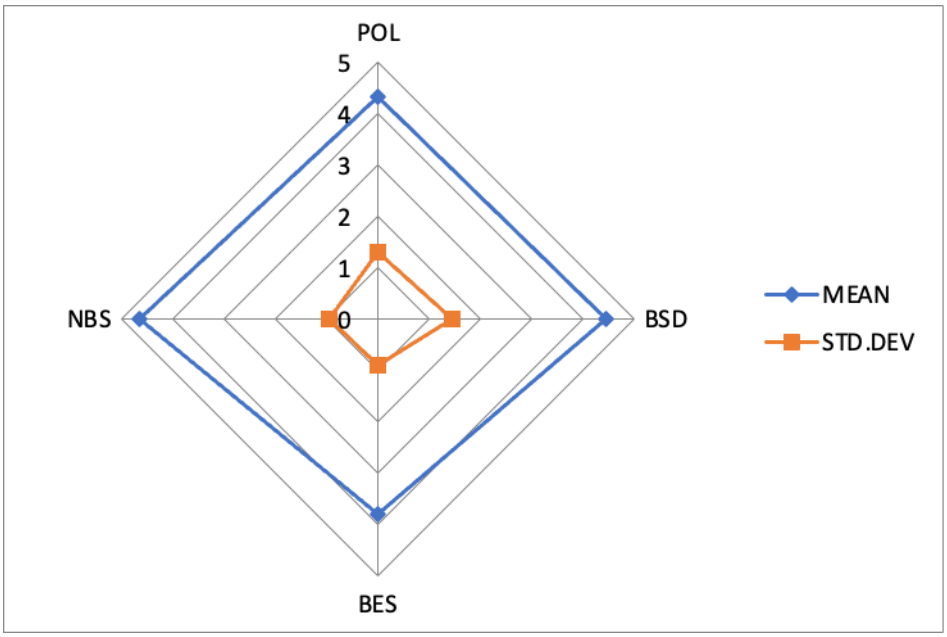


Figure 4.1 Radar plot for policy construct items

With reference to Table 4.1, and Fig. 4.1 respectively, a strong agreement was made for the policy (POL) construct with the average score of aggregate measure POL (M = 4.304, SD = 1.282) with the item on the development of the National IoT Cyber Security Strategy being the most agreed upon, NBS (M = 4.665, SD = 0.953), followed by the effectiveness of the National CERT System BSD (M = 4.445, SD = 1.449), and the view of IoT Cyber Security as an eco-system BES (M = 3.800, SD = 0.915) being the least agreed upon item in this category.

Table 4.2 shows the inter-item correlation for the items used to measure the policy (POL) construct.

With reference to Table 4.2, the three items had acceptable inter-item correlation (r>=0.2), with a strong relationship (r=0.617) between the effectiveness of the National CERT system (BSD) , and the eco-system view of IoT Cyber Security (BES).

Table 4.2 Inter-item correlation for policy (POL) construct items.

Item	BSD	BES	NBS
BSD	1.000	.617	.307
BES	.617	1.000	.313
NBS	.307	.313	1.000

It can consequently, be concluded that the items selected for measuring the policy construct (POL) were appropriate for the measure [30][31]

4.2.2 Regulatory (REG) construct

Recent research [30][31] shows an emerging trend towards developing specific cyber security regulations to ensure security generally for on-line presence and for personal data in particular in order to protect users, systems and networks from cyber exploitation. Governments have therefore sought to improve national cyber risk management systems

in the wider economy through its implementation international (such the General Data Protection Regulation (GDPR)) and national regulations.

Thus the regulatory (REG) construct was used to determine the effect of various regulatory items on IoT Cyber Security readiness in the context of a developing Country.

4.2.2.1 Items used to measure regulatory (HO) construct

The details of the three items used to measure this construct follow:

a. **Development of regulations to operationalize the Cyber security Act**
b. **Establishment of a specific entity to Manage the National cyber security**
c. **Development of a National IoT Cyber Security Strategy (NBS)**

i. **Development of regulations to operationalize the Cyber security Act (HOS)**

A number of Countries have developed specialized regulations to operationalize their national cyber security laws. For example in Kenya, following the enactment of the Data Protection Act No. 24 of 2019 (the "**DPA**"), The DPA gives the Office of the Data Commissioner the power to impose administrative fines for failure to comply with the DPA. The Data Commissioner was consequently formally appointed on 16 November 2020. Following the Data Commissioner's appointment, a Task Force was convened in January 2021 to develop the Data Protection Regulations under the DPA.

ii. **Establishment of a specific entity to operationalize the the cyber security law (HON)**

To further improve security generally for on-line presence and for personal data in particular in order to protect users, systems and networks from cyber exploitation, Governments around the world have established specific agencies to operationalize the cyber security law. For example in Kenya, the office of the Data Commissioner

has been established to operationalize the Data Protection Act. This is an important construct to gauge the effectiveness of enforcement of the Data protection law.

iii. Development of a National IoT Cyber Security Strategy (HOO)

A number of countries have developed national IoT Cyber Security strategies which layout the short term and long term strategy towards the realisation of an all inclusive information security for socio-economic benefits associated with IoT Cyber Security [18]. The development of the National IoT Cyber security strategy is therefore an important measure for the IoT cyber security readiness of a Country.

4.2.2.2 Descriptive statistics for regulatory (HO) construct items.

The means and standard deviations of aggregated measures for the three items used to measure the regulatory construct (HO) are illustrated in Table 4.3

Table 4.3 Descriptive statistics for the regulatory (HO) construct items

Item	**Mean**	**Std. Dev**	**Rank**
Scale-HO	**2.907**	**0.694**	
HOS	3.370	0.870	**1**
HON	3.130	0.947	**2**
HOO	2.200	0.805	**3**

With reference to Table 4.3, a fair agreement was made for the regulatory (HO) construct with the average score of aggregate measure HO (M = 2.907, SD = 0.694). The item on the development of regulations to operationalize the Cyber security Act was more strongly agreed upon HOS (M =3.370, SD = 0.870), followed by the item on the establishment of a specific entity to operationalize the the cyber security law HON (M =3.130, SD = 0.947) and the item on the development of a National IoT Cyber Security Strategy being less agreed upon in this category HOO (M =2.200, SD = 0.805) respectively.

Table 4.4 shows the inter-item correlation for the items used to measure the regulatory (HO) construct. With reference to Table 4.4, the three items had acceptable inter-item correlation (r>=0.2), we can therefore conclude that the three items selected for measuring the regulatory (HO) construct were appropriate for the measure [11]

Table 4.4 Inter-item correlation for regulatory (HO) construct items.

Item	HOS	HON	HOO
HOS	1.000	.462	.344
HON	.462	1.000	.577
HOO	.344	.577	1.000

4.2.3 Human Resource (MBAD) construct

The Human Resource (MBAD) construct was assessed using a total of four items. Human resources for IoT cyber security were ranked according to respondents' perceptions of their availability in the firm. For the ranking, a five-point likert scale was used to measure agreement or disagreement with a neutral option that was intended to represent the usage item under research. The results were then tallied up. Questionnaires using Likert scales were developed from [32].

Due to the lack of existing research on this construct in Uganda, the items used to measure the Human Resource (MBAD) construct were constructed based on a critical examination of previous studies conducted elsewhere on the human resource capacity for IoT Cyber Security in developed nations. [33]

4.2.3.1 Items used to measure the Human Resource (MBAD) construct

The individual items which were included for measuring the human resource advantages construct (MBAD) are listed below:

(i). **Effectiveness of security Department/Division dedicated to overseeing cyber security management in the organisation (MICSR).** Respondents were asked to rate their perceived effectiveness of the cyber Security Department/Division dedicated to overseeing cyber security management in there my organisation. Because of targeted sampling (purposeful), in this case, it was assumed that the absence of such a dedicated department/division to overseeing cyber security management would correspond to a strongly disagree choice in the responses.

(ii). Effectiveness of the Cyber security policy or information security policy for the organisation (MBS). Respondents were asked to rate their perceived effectiveness of the cyber security policy or information security policy for the organisation. Because of targeted sampling (purposeful), in this case, it was assumed that the absence of such a dedicated security or information policy would correspond to a strongly disagree choice in the responses.

(iii). Effectiveness of security certification i.e ISMS ISO 9001:2013 or a similar standard (MBE).

Respondents were asked to rate their perceived effectiveness of the security certification i.e ISMS ISO 9001:2013 or a similar standard (MBE). Because of targeted sampling (purposeful), in this case, it was assumed that the absence of such a certification would correspond to a strongly disagree choice in the responses.

It has been asserted that a successful ISO 27001 information security management system (ISMS) provides a management model of policies and procedures for ensuring the Confidentiality, Integrity, and Availability (CIA) of information, regardless of its format.

Therefore achieving ISO 27001 or similar certification would show commitment on the part of the organization to:

- Protect organizational and stakeholder information from unauthorized access

- Ensure such information is accurate and accessable only by authorised users
- Assess and mitigate the risks pertaining to the organisation's information resources
- To adhere to the international security standard based on industry best practices [][][][]

(iv). Sufficient personnel qualified in Information security, and with corresponding certifications (MBC). Respondents were asked to rate their perceived view that sufficient personnel qualified in Information security, and with corresponding certifications existed in their organisations. Because of targeted sampling (purposeful), in this case, it was assumed that the absence of such personnel would correspond to a strongly disagree choice in the responses.

4.2.3.2 Descriptive statistics for the Human Resource (MBAD) construct items.

Table 4.5 and Figure 4.2 show the mean and standard deviation of aggregated measures for the four elements that make up the Human Resource (MBAD) construct.

Table 4.5 Descriptive statistics for Human Resource (MBAD) construct items.

Item	Mean	Std. Dev	Rank
Scale-MBAD	**3.969**	**0.635**	
MICSR	3.850	0.893	**4**
MBS	3.930	0.982	**2**
MBE	4.090	0.703	**1**
MBC	3.910	0.847	**3**

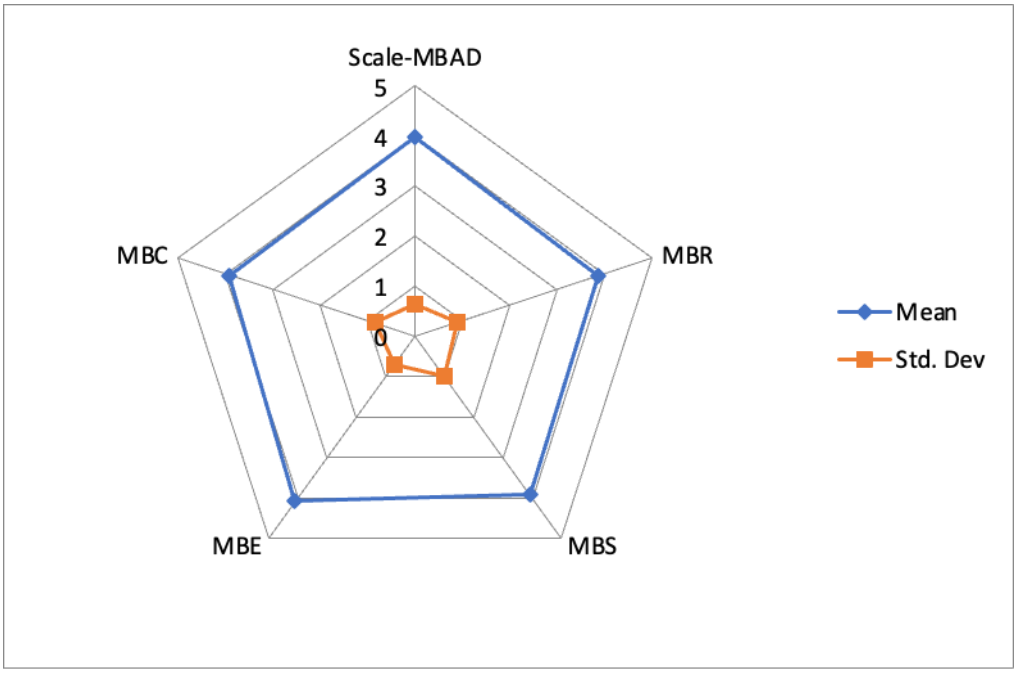


Figure 4.2 Radar plot for Human Resource construct items

With reference to Table 4.5, and Fig. 4.2 respectively, a stronger agreement was made for the Human Resource (MBAD) construct the average score of aggregate measure MBAD (M = 3.969, SD = 0.635) with the item on the perceived effectiveness of security certification i.e ISMS ISO 9001:2013 or a similar standard being the most agreed upon i.e MBE (M =4.200, SD = 0.850), followed in second position by the item on the effectiveness of the Cyber security policy or information security policy for the organisation MBS (M =3.930, SD = 0.982), and the item on sufficient personnel qualified in Information security, and with corresponding certifications MBC(M =3.910, SD = 0.847), and finally the effectiveness of security Department/Division dedicated to overseeing cyber security management in the organisation MICSR (M =3.850, SD = 0.893) in fourth position respectively.

Table 4.6 shows the inter-item correlation for the four items used to measure the Human Resource (MBAD) construct.

Table 4.6 Inter-item correlation Human Resource (MBAD) construct items.

Item	MICSR	MBS	MBE	MBC

MICSR	1.000	.455	.348	.523
MBS	.455	1.000	.307	.440
MBE	.348	.307	1.000	.265
MBC	.523	.440	.265	1.000

With reference to Table 4.6, all the four items had acceptable inter-item correlation (r>=0.2), with the highest inter-correlation being between the perceived availability of sufficient security personnel (MBC) and the effectiveness of a dedicated cyber security department/division at the organization (MICSR) with inter-item correlation (r=0.523).

It can therefore concluded that the four items selected for measuring the Human Resource (MBAD) construct were appropriate for the measure [26][28]

4.2.4 Digital Literacy (DL) construct

Recent research contends that there is no universal definition for "digital literacy" [][][]. However, the term is frequently associated with ICT related skills []. Thus generally speaking, the measure of digital literacy may be made at two levels, namely the general digital literacy of the masses, and that of ICT experts [][]. It has been argued that improvement in digital literacy in developing countries is key to the success of IoT cyber security readiness [38][53][54]

4.2.4.1 Items used to measure the digital literacy (DL) construct

The details of the two items used to measure this construct follow:

(i). Availability of technical IoT Cyber security expertise (ATE). Availability of technical expertise is the driving force behind innovation, research and development in IoT Cyber security related areas. Furthermore, availability of technical experts will enable more efficient installation and maintenance of IoT based networks thus increasing the overall IoT Cyber Security readiness of a given country [38][54]

It was therefore necessary to test the effectiveness of this item in influencing IoT Cyber Security readiness in developing countries.

(ii). Digital literacy of the masses (DLM). Digital literacy of the masses is a term closely related to the general literacy rates of the population [38][53] . Digital literacy of the masses is also closely linked to the Perceived Knowledge, Self Efficacy, and Perceived Ease of Use constructs in relation to ICTs as used in the IoT Cyber Security adoption domain [][][][][]. It was therefore necessary to test the effectiveness of this item in influencing IoT Cyber Security readiness in Uganda, as a developing country.

4.2.6.2 Descriptive statistics for the digital literacy (DL) construct items.

The means and standard deviations of aggregated measures for the two items used to measure the digital literacy (DL) construct are illustrated in Table 4.7

Table 4.7 Descriptive statistics for the digital literacy (DL) construct items.

Item	**Mean**	**Std. Dev**	**Rank**
Scale-DL	**4.756**	**1.111**	
ATE	4.800	0.915	**1**
DLM	4.710	1.177	**2**

Two items used to measure digital literacy (DL) are shown in Table 4.12. The mean and standard deviation of aggregated measures for these two items are shown. According to Table 4.7, the average score of aggregate measure DL (M = 4.756, SD = 1.111) had a greater agreement with the digital literacy (DL) concept than any of the other constructs used to assess IoT Cyber Security readiness.

The item on the availability of technical expertise ATE (M = 4.800, SD = 0.915) was the most agreed upon followed by the digital literacy of the masses item DLM (M = 4.710, SD = 1.177) respectively.

Table 4.8 shows the inter-item correlation for the items used to measure the digital literacy (DL) construct.

Table 4.8 Inter-item correlation for digital literacy (DL) construct items.

Item	ATE	DLM
ATE	1.000	.709
DLM	.709	1.000

With reference to Table 4.8 the two items had acceptable inter-item correlation (r>=0.2), and, as expected, a strong relationship for the two items i.e. availability of technical expertise (ATE), and digital literacy of the masses (DLM) with inter-item correlation (r=0.709).

We can accordingly, conclude that the two items selected for measuring the digital literacy construct (DL) were appropriate for the measure [27][30]

4.2.7 Linear Regression Analysis: IoT Cyber Security Readiness (ICSR)

According to [], linear regression is a statistical technique for simulating the linear connection between a dependent variable and one or more independent variables. Some people refer to the dependent variable as the "predictand," while others refer to it as "predictors." There is a minimum sum-of-squares difference between the observed and predicted values in linear regression, which is based on least squares.

Many assumptions are made in the linear regression model. As long as the assumptions are met, the regression estimators are the best since they are fair, effective, and consistent [30]. The estimator's predicted value is equal to the true value of the parameter. As a rule of thumb, an efficient estimator has a lower variance than any other estimate. A consistent estimator has a zero bias and zero variance as the sample size increases. [34] provides a list of the regression model's six most basic assumptions.

1. **Linearity**: Predictor and predictors are assumed to have a linear relationship. As an exploratory step in regression, scatter plots should be evaluated to identify probable deviations from linearity.

2. **Non-stochastic**: That there is no correlation between the errors and the specific predictors. The residuals analysis checks this assumption by plotting the residuals against each individual predictor on a scatterplot. If the assumption is violated, it could imply that the predictors have undergone a change.

3. **Zero mean:** The residuals should have a value of zero. The least squares approach of calculating regression equations ensures that the mean is zero.

4. **Constant variance:** There is no systematic change in the error variance with increasing predicted value size because of the constant variance of the residuals. Error variances should not be bigger when the predictand is large than when the predictand is small.

5. **Non-auto-regression:** There is no correlation between the residuals and time. When it comes to time series applications, this assumption is one that is most likely to be broken

6. **Normality:** The error term has a regularly distributed probability. If this condition is not met, standard testing of the significance of coefficients and other statistics in the regression equation will be invalid.

To figure out how to fit a linear probability model based on the above assumptions, ordinary Least Squares Regression was used (Table 4.11). IoT Cyber Security readiness (ICSR) was the dependent variable in a regression analysis. Four constructs were used as predictors: Policy (POL), Regulatory (HO), Human Resources (MBAD), and Digital literacy (DL).

The adjusted R square of the emerging model (Table 4.9) was 0.892 ($F(4,43)=61.418$, p <0.001). Two of the predictor variables included in the analysis were found to be very significant (Table 4.10). These are the Human Resource construct MBAD ($\beta = 0.379$, p =0.003) and Policy construct POL ($\beta = 0.259$, $p = 0.003$) respectively. These were closely

followed by the Digital Literacy construct DL (β = 0.205, p = 0.018), and the Regulatory construct HO (β = 0.127, p =0.042) respectively.

Table 4.9 Model Summary-IoT Cyber Security Readiness (ICSR)

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.952[a]	.907	.892	.518
a. Predictors: (Constant), MBAD, HO, POL, DL				

TABLE 4.10 ANALYSIS OF VARIANCE- IOT CYBER SECURITY READINESS (ICSR)

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	98.791	4	16.465	61.418	.000[a]
	Residual	10.187	38	.268		
	Total	108.978	44			
a. Predictors: (Constant), HO, MBAD, POL, DL						
b. Dependent Variable: ICSR						

Table 4.11 Regression analysis- IoT Cyber Security Readiness (ICSR)

Coefficients[a]						
Model		Unstd. Coef		Std.Coef	T	Sig.
		B	Std.Error	Beta		
1	(Constant)	-1.365	.647		-2.108	.042
	DL	.222	.090	.205	2.463	.018
	POL	.324	.103	.259	3.138	.003
	HO	.171	.081	.127	2.103	.042
	MBAD	.405	.125	.379	3.225	.003
a. Dependent Variable: ICSR						

4.3 Constructs and Individual Items for Measuring IoT Cyber Security Intensity (ICSI)

According [], the OECD posits that IoT Cyber Security intensity metrics are concerned with the state of IoT Cyber Security implementation and effectiveness respectively. This primarily means that IoT Cyber Security intensity metrics would give an indication of the use of IoT Cyber Security, and the demographics of the users, as well the effectiveness IoT Cyber Security deployments [35][38}

Thus a Country's IoT Cyber Security intensity status would inform both the IoT Cyber Security readiness, and IoT Cyber Security adoption strategies [34]

Because there has been no prior research into IoT Cyber Security intensity in Uganda, the constructs included in this study were developed based on a critical analysis of previous studies conducted elsewhere in the world, both developed and developing, on cyber security readiness and other ICT related studies. The constructs were developed based on a critical review of previous studies conducted elsewhere in the world, both developed and developing, on cyber security readiness and other ICT related studies. [53][54]

As seen in Chapter 3, the conceptual model, Figure 3.7, for the IoT Cyber Security intensity domain metrics assumed that the dependent variable 'IoT Cyber Security

intensity (ICSI)' was influenced by several independent variables categorized into two groups, namely.

(i) **Demographic factors**, which are the socio-economic characteristics expressed statistically including gender, age, marital status, education level, income level, occupation, and employment [38]

(ii) **Control factors,** which influence the state of IoT Cyber Security implementation and effectiveness []. These are constructs such as IoT deployments, IoT Cyber Security implementation, effectiveness, and IoT Cyber Security applications respectively.

These constructs and the individual items utilised to measure them are now described in detail.

4.3.1 DEMOGRAPHIC CONSTRUCTS

A number of characteristics associated with a person's behaviour and commonly referred to as demographics are key in investigating the variations in the intensities of emerging and new concepts such as IoT Cyber Security [38]. The research adopted two approaches to investigating IoT Cyber Security intensity in Uganda namely, the technology acceptance model (TAM) [47], and the diffusion of innovations theory (DOI) [38]

The technological acceptance model is based on an individual's construction of an intention to act despite of restrictions, but the diffusions of innovations hypothesis is based on the communication of a perceived novel concept through time among members of a social system who share specific traits.

The TAM and DOI theory models examine the characteristics of an individual that influence their use of technology, and are thus more appropriate for examining the IoT Cyber Security intensity in developing countries. Models for examining technology acceptance at the household level, such as the model for the adoption of technology in the home (MATH), which were previously employed in ICT adoption research, were determined to be insufficient for specific domains such as IoT cyber security.

The demographic characteristics of the 127 respondents in the IoT Cyber Security intensity domain is summarised in Table 4.12 The choice of the variables to be included in the measures for the demographics constructs was largely informed by previous studies for the determinants of IoT Cyber Security access in developed countries [38]

Table 4.12 Demographic characteristics of the respondents

Variable (N=127)	**Description**	**Frequency**	**Percent**
Gender	Male	74	58.3
	Female	53	41.7
Age	18-34yrs	40	31.5
	35-44yrs	42	33.1
	45-54yrs	32	25.2
	Above 55yrs	13	10.2
Education level	Diploma	19	15.0
	Degree	40	31.5
	Masters	68	53.5
Years of Experience (	<5yrs	39	30.7
	5-10 yrs	39	30.7
	10-15 yrs	30	23.6
	Above 15yrs	19	15.0

Source: Researcher

Regarding the background characteristics of the respondents, as depicted analysis of in table 4.12, indicates that majority of the study respondents were male with 74 out of the

127 respondents constituting a percentage of (58.3%) being males while 53 were females. This is consistent with the findings of other studies that showed a large percentage of individuals in Science & Technology in general, and in ICTs in particular, were males [38].

In terms of segregation by age, nearly three quarters of the respondents were below 45 years (40 or 31.5 per cent were aged between18-34 years while 42 or 33.1 per cent were aged between 35 and 44 years respectively). Thirty two (32) or a quarter (25.2 per cent) were aged between 45-54 years while 13 or 10.2 per cent were aged 55 years and above respectively.

In terms of level of education, over two thirds of the respondents (68.0%) had above at least a masters degree, followed by respondents with at least a first degree (40%), and with diploma holders constituting 15.0% of the respondents. The distribution of respondents by highest level of education services as an indication of the specialized knowledge required to implement IoT cyber security initiatives

With regard to level of experience in ICTs, Emerging technologies, IoTs or cyber security thematic areas, majority of respondents accounting for nearly two-thirds of the total respondents (61.4 per cent) had between at least 10 years of experience. Those with 10-15 years of experience accounted for 23.6 per cent of the respondents while with over 15 years of experience numbered 19 and constituted 15.0 per cent of the total respondents respectively.

4.3.2 Control constructs

A total of four control constructs were used to measure IoT Cyber Security intensity (ICSI), namely,

i. Total number of IoT deployments (TID),

ii. IoT Cyber Security implementation (ICS),
iii. Effectiveness of IoT cyber security (EIS)
iv. IoT Cyber Security applications (ICA) respectively.

The selection of these constructs was based on recent studies on IoT Cyber Security, which place emphasis considerations for the nomadic nature of IoT devices, the inherent smaller processing power of IoT devices. It was thus not only important to establish the extent of IoT Cyber Security infrastructure, but also who (demographic constructs) and how (control constructs) IoT Cyber Security is being implemented, with special emphasis on developing countries

4.3.2.1 Total number of IoT deployments (TID)

Respondents were asked to rank their perceived view that the total number of IoT deployments nationwide, in their specific sector, and in their organization was large enough to warrant a need to take steps to ensure cyber security of these deployments. The ranking was determined using a five-point likert scale ranging from strongly disagree to strongly agree, along with a neutral choice designed to capture the usage item under inquiry. The questions using the likert scale were borrowed from [47][48].

IoT deployments were reviewed across multimedia services, Government services, e-Commerce, e-Health, Education, Manufacturing, Supply chain and so on. Due to the lack of existing study on IoT in Uganda, the items used to measure the IoT deployment construct were constructed after a critical examination of previous studies conducted abroad on IoTs [1][2][3].

4.3.2.2 IoT Cyber Security Implementation (ICS)

Respondents were asked to rank their perceived view that Cyber Security was actually being implemented in IoT deployments. The ranking was determined using a five-point likert scale ranging from strongly disagree to strongly agree, along with a neutral choice designed to capture the usage item under inquiry. The questions using the likert scale were drawn from [38].

This was a question purely based on the respondent's experience in cyber security of IoT deployments across multimedia services, Government services, e-Commerce, e-Health, Education, Manufacturing, Supply chain and so on. Due to the lack of existing study on IoT in Uganda, the items used to measure the IoT deployment construct were constructed from a critical review of previous studies conducted abroad on IoTs. [44][43]

4.3.2.3 Effectiveness of IoT Cyber Security (EIS)

Respondents were asked to rank their perceived effectiveness of cyber security implementation in IoT deployments. The ranking was determined using a five-point likert scale ranging from strongly disagree to strongly agree, along with a neutral choice designed to capture the usage item under inquiry. The questions using the likert scale were borrowed from [][].

This question was also based on the respondent's experience in the effectiveness of cyber security of IoT deployments across multimedia services, Government services, e-Commerce, e-Health, Education, Manufacturing, Supply chain and so on. Due to the lack of existing study on IoT in Uganda, the items used to measure the IoT deployment construct were constructed from a critical review of previous studies conducted abroad on IoTs. [44][43]

4.3.3 Descriptive statistics for the IoT Cyber Security Intensity (ISCI)

Table 4.12 and Figure 4.3 exhibit the averages and standard deviations of aggregated values for the four categories used to calculate the IoT Cyber Security Intensity (ISCI).

Table 4.12 Descriptive statistics for IoT Cyber Security Intensity (ISCI) construct items.

Item	**Mean**	**Std. Dev**	**Rank**
Scale-ISCI	**3.969**	**0.635**	
TID	3.850	0.893	**4**

ICS	3.930	0.982	**2**
EIS	4.090	0.703	**1**
ICA	3.910	0.847	**3**

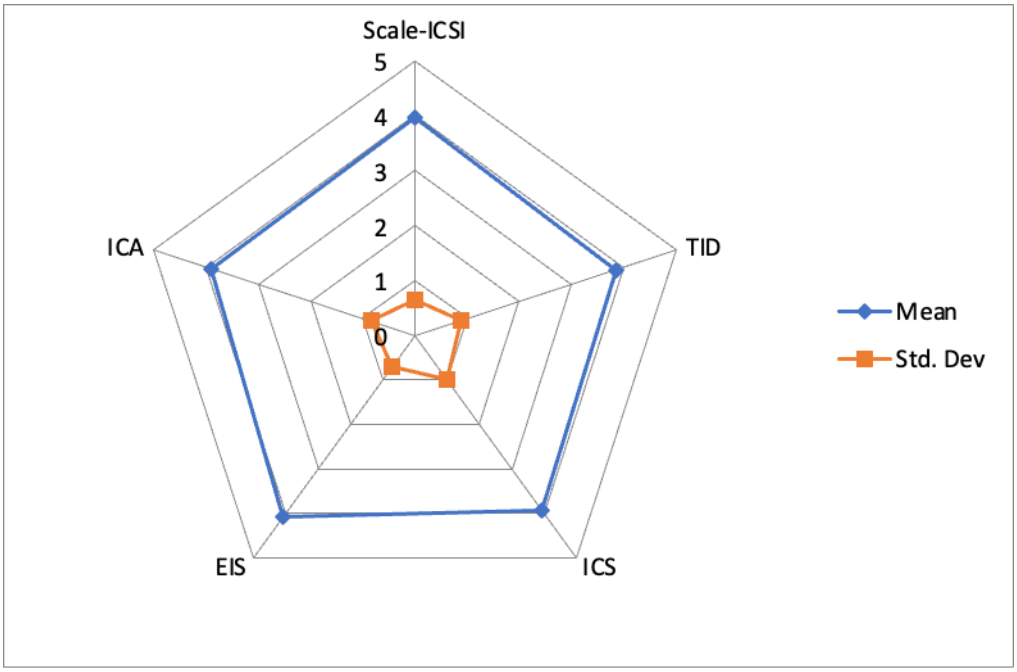


Figure 4.3 Radar plot for IoT Cyber Security Intensity (ISCI) items

With reference to Table 4.12, and Fig. 4.3 respectively, a strong agreement was made for the IoT Cyber Security Intensity (ISCI) with the average score of aggregate measure ISCI (M = 3.969, SD = 0.635) with the item on the perceived effectiveness of IoT cyber security being the most agreed upon i.e EIS (M =4.200, SD = 0.850), followed in second position by the item on the perceived implementation of IoT cyber security ICS (M =3.930, SD = 0.982), and the item on IoT cyber security applications ICA (M =3.910, SD = 0.847), in third place, and finally the total number of IoT deployments TID (M =3.850, SD = 0.893) respectively. Table 4.13 shows the inter-item correlation for the four items used to measure the IoT Cyber Security Intensity (ISCI) construct.

Table 4.13 Inter-item correlation for IoT Cyber Security Intensity (ISCI) construct items.

Item	TID	ICS	EIS	ICA

TID	1.000	.455	.348	.523
ICS	.455	1.000	.307	.440
EIS	.348	.307	1.000	.265
ICA	.523	.440	.265	1.000

With reference to Table 4.13, all the four items had acceptable inter-item correlation (r>=0.2), with the highest inter-correlation being between the IoT cyber security applications (ICA) and the total number of IoT deployments (TID) with inter-item correlation (r=0.523).

It can therefore concluded that the four items selected for measuring the IoT Cyber Security Intensity (ISCI) were appropriate for the measure [35][36]

4.3.4 Regression Analysis: IoT Cyber Security Intensity (ICSI)

The theoretical underpinnings of linear regression and the necessary assumptions thereof were already discussed in Section 4.2.7

Using ordinary least squares regression to fit a linear probability model [] in the domain of IoT Cyber Security Intensity [], it was discovered that the IoT Cyber Security Intensity domain has a high level of security (Table 4.14). With IoT Cyber Security Intensity (ICSI) as the dependent variable and a total of five constructs (including one for assessing non-responder bias, CODED, which represents the "Days to respond" variable) as the predictors, the regression analysis was conducted. These are, total number of IoT deployments (TID), IoT Cyber Security implementation (ICS), Effectiveness of IoT cyber security (EIS), and IoT Cyber Security applications (ICA) respectively,.

The adjusted R square of the emerging model (Table 4.14) was 0.780 ($F(5,161)=115.189$, $p<0.001$), which was significantly higher than the baseline model. Several predictor factors included in the research were found to be highly significant, with two of them being extremely significant (Table 4.16). These are, effectiveness of IoT cyber security EIS ($\beta = 0.728$, $p= 0.001$), and IoT cyber security implementation ICS ($\beta = 0.584$, $p<$

0.001). The IoT cyber security applications construct ICA (β = 0.267, p<0.001) was fairly significant while both total number of IoT deployments TID (β = -0.220, p =0.298), and "days to respond" CODED (β = -0.032, p =0.391) predictors were found to be insignificant, Table 4.16

Table 4.14 Model Summary- IoT Cyber Security Intensity (ICSI)

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.887[a]	.787	.780	.253
a. Predictors: (Constant), TID, ICS,EIS, ICA, CODED				

Table 4.15 Analysis of Variance- IoT Cyber Security Intensity (ICSI)

Model		Sum of Squares	Df	Mean Square	F	Sig.
1	Regression	36.892	4	7.388	115.189	.000[a]
	Residual	10.053	157	.064		
	Total	46.944	161			
a. Predictors: (Constant), TID, ICS,EIS, ICA, CODED						
b. Dependent Variable: ICSI						

Table 4.16 Regression Analysis: IoT Cyber Security Intensity (ICSI)

Coefficients[a]						
Model		Unstd. Coef		Std. Coef	T	Sig.
		B	Std. Error	Beta		
1	(Constant)	-.18	.229		-.08	.018
	TID	-.189	.181	-.220	-1.044	.298
	ICS	.276	.018	.584	15.296	.000
	ICA	.227	.033	.267	6.898	.000
	EIS	.713	.207	.728	3.443	.001
	CODED	-.012	.014	-.032	-.860	.391
a. Dependent Variable: ICSI						

4.4 Constructs and Individual Items for Measuring IoT Cyber Security Adoption (ICSA)

According to []IoT Cyber Security adoption metrics are concerned with the Attitudinal, Normative and Control factors that influence IoT Cyber Security intentions.

The definition of the different categories of the adoption constructs, and the descriptions of each of the three constructs used in the adoption domain were considered in Chapter three. We now briefly describe the individual items used to measure each of the constructs.

[] validated a survey instrument to investigate IoT cyber security adoption in the UK Household. The constructs and the individual items for this research instrument are shown in Annex 1. Although this research investigated IoT Cyber Security adoption most of the items validated by [9] are applicable to test their influence on the individual or organisation's intentions to adopt IoT Cyber Security [10]

4.4.1 Relative Advantage (RA) construct

Relative Advantage (RA) is defined as the extent to which a technology, service or product is better or more advanced than it's alternative or predecessor [38]. In terms of IoT cyber security, RA could be viewed as IoT cyber security would offer distinct advantages over unprotected IoT devices, networks or services [17][18] and is a key factor influencing the intention to adopt IoT Cyber Security.

4.4.1.1 Items for measuring the relative advantage (RA) construct

A total of three items were used to measure the IoT Cyber Security relative advantage construct. Respondents were asked to rank their perceived relative advantages of IoT Cyber Security connections over the predecessor unsecured IoT. Among the factors considered as potentially presenting the relative advantage of IoT cyber security the perceived user satisfaction and experience; Perceived better protection of data and networks; and assurance of privacy and security among others.

The individual items used to measure the relative advantage (RA) construct are as listed.

(i). **Perceived better protection of data and networks (PDN)**. i.e. This item was used to gauge the respondents' perception of IoT cyber security providing better protection for data and networks compared to unsecured IoT Cyber Security [38]

(ii). Perceived better user satisfaction and experience (USE). This item was used to gauge the respondents' perception of IoT cyber security leading to better user satisfaction and experience [38]

(iii). Perceived better user privacy and security (UPS). This item was used to gauge the respondents' perception of IoT cyber security leading to better privacy and security of devices, networks, and systems [38]

4.4.1.2 Descriptive statistics for relative advantage (RA) construct items

The means and standard deviations of aggregated measures for the three items used to measure the relative advantage (RA) construct are illustrated in Table 4.17 and Figure 4.4 respectively.

Table 4.17 Descriptive statistics for relative advantage (RA) construct Items.

Item	**Mean**	**Std. Dev**	**Rank**
Scale-RA	**4.080**	**0.784**	
PDN	4.040	0.965	**2**
USE	4.000	1.040	**3**
UPS	4.200	0.800	**1**

With reference to Table 4.17 and Fig. 4.4, respectively, a strong agreement was made for the relative advantage (RA) construct with the average score of aggregate measure RA (M = 4.080, SD = 0.784).

The item on the perceived better user privacy and security as a result of implementing IoT cyber security was the most agreed upon i.e UPS (M =4.200, SD = 0.800), followed in second position by the item on perceived better protection of data and networks PDN

(M =4.040, SD = 0.965), and finally, the item on better user satisfaction and experience USE (M =4.000, SD = 1.040) respectively

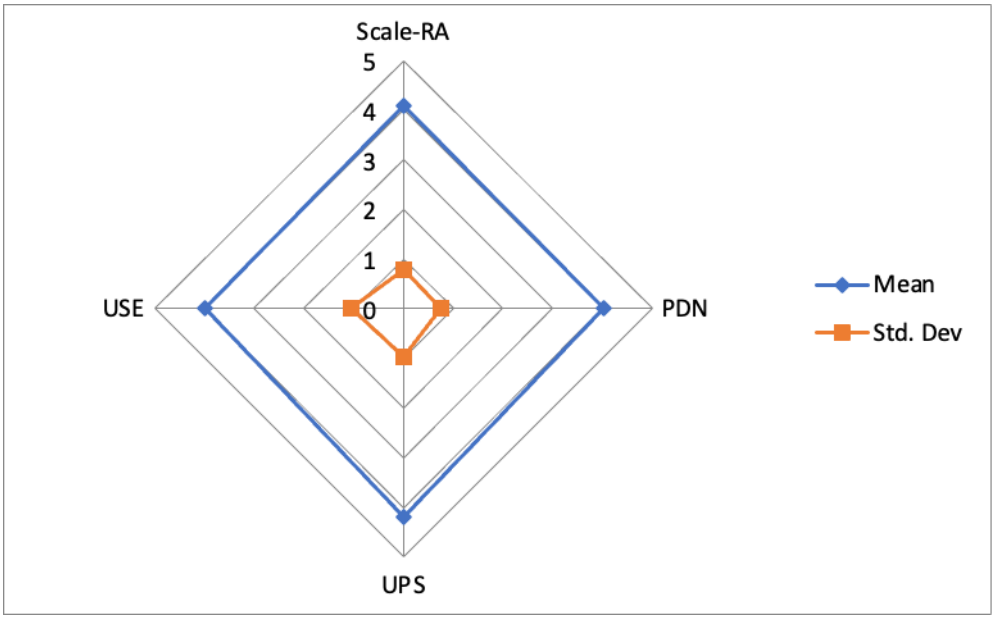


Figure 4.9 Radar plot for relative advantage construct items

Table 4.18 shows the inter-item correlation for the three items used to measure the relative advantage (RA) construct.

With reference to Table 4.18, all the three items had acceptable inter-item correlation (r>=0.2), with the highest inter-correlation being between protection of data and networks (PDN) and user privacy and security (UPS) (r=0.717), and between user privacy and security (UPS) and user satisfaction and experience (USE) with inter-item correlation (r=0.582) respectively.

Table 4.18 Inter-item correlation for relative advantage (RA) construct items.

Item	USE	PDN	UPS
USE	1.000	.557	.582
PDN	.557	1.000	.717
UPS	.582	.717	1.000

We can therefore conclude that the three items selected for measuring the relative advantage (RA) construct were appropriate for the measure [38]

4.4.2 Facilitating conditions (FC) construct

Facilitating conditions (FC) are defined as the perceived level of resources available to enable one to subscribe to a service such as IoT Cyber Security [38][

Researchers investigating the diffusion of technology have previously established facilitating conditions as a factor influencing technology adoption [4][38]. Hence it was necessary to investigate the effect of this construct on the intention to adopt IoT Cyber Security in a developing country context.

4.4.3 Items for measuring the facilitating conditions (FC) construct

The facilitating conditions (FC) construct was assessed using a total of six items. Respondents were asked to rank their perceived facilitating conditions for adopting IoT Cyber Security. The ranking was determined using a five-point Likert scale ranging from strongly disagree to strongly agree, along with a neutral choice designed to capture the usage item under research. The questions using the Likert scale were borrowed from [].

The 6 items used to measure the facilitating conditions (FC) construct are as follows.

(i). Perceived declining costs of IoT Cyber Security services (PDC) [38]
(ii). Availability of IoT Cyber security as a service (SSS) [38]
(iii). Availability of different IoT cyber security service providers (FCC) [38]
(iv). Perceived reliability of IoT Cyber Security offerings in ensuring CIA (PRS) [38]
(v). Perceived knowledge or expertise in IoT cyber security (PKC) [38]
(vi). Referent's influence in the adoption of IoT cyber security (SRI)[38]

4.4.5.2 Descriptive statistics for facilitating conditions (FC) construct

The means and standard deviations of aggregated measures for the six items used to measure the facilitating conditions (FC) construct are illustrated in Table 4.19 and Fig. 4.5 respectively.

With reference to Table 4.19 and Figure 4.5 respectively, a strong agreement was made for the facilitating conditions (FC) construct with the average score of aggregate measure FC (M = 4.115, SD = 0.581).

The two most agreed upon items for this measure were the perceived reliability of IoT cyber security (PRS) and Referents influence in adopting IoT cyber security (SRI) both with PRS,SRI (M=4.200, SD=0.581) followed by the availability of different IoT cyber security service providers FCC (M=4.150, SD=0.707). In fourth position was the perceived knowledge or expertise in IoT cyber security PKC (M=4.060, SD=0.782), followed by in fifth position by both the perceived declining costs of IoT Cyber Security services (PDC) and the availability of IoT Cyber security as a service (SSS)
PDC, SSS (M=4.040, SD=0.965) respectively

Table 4.19 Descriptive statistics for facilitating conditions (FC) construct items

Item	**Mean**	**Std. Dev**	**Rank**
Scale-FC	**4.115**	**0.581**	
SSS	4.040	0.965	**5**
SRI	4.200	0.850	**1**
PDC	4.040	0.965	**5**
PRS	4.200	0.850	**1**
PKC	4.060	0.782	**4**
FCC	4.150	0.707	**3**

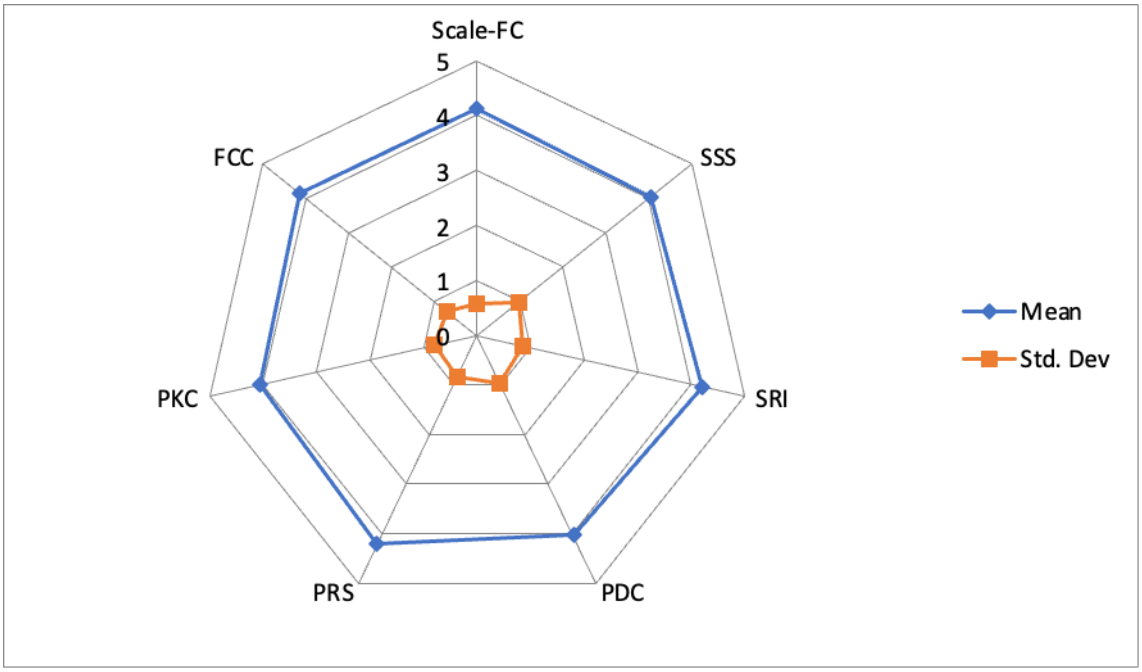


Figure 4.5 Radar plot for the facilitating conditions construct items

Table 4.20 Inter-item correlation for facilitating conditions (FC) construct items

Item	FCC	SRI	PRS	PKC	PDC	SSS
FCC	1.000	.180	.122	.222	.252	.039
SRI	.180	1.000	.521	.549	.016	.011
PRS	.122	.521	1.000	.702	.215	.064
PKC	.222	.549	.702	1.000	.016	.079
PDC	.252	.016	.215	.016	1.000	.167
SSS	.039	.011	.064	.079	.167	1.000

Table 4.20 shows the inter-item correlation for the six items used to measure the facilitating conditions (FC) construct items. With reference to Table 4.20, most of the items for measuring the facilitating conditions (FC) construct had acceptable inter-item correlation (r>=0.2), with some items registering high correlation [][]. For example the item on the perceived knowledge or expertise in IoT cyber security (PKC) and that on the perceived reliability of IoT Cyber Security offerings in ensuring CIA (PRS)) with a Pearson r value of r=0.702 followed by that of the item on the perceived knowledge or

expertise in IoT cyber security (PKC) and Referent's influence in the adoption of IoT cyber security (SRI) (r=0.549) with the third highest correlation being between perceived reliability of IoT Cyber Security offerings in ensuring CIA (PRS) and Referent's influence in the adoption of IoT cyber security (SRI) (r=0.521) respectively.

4.4.11 Regression Analysis: IoT Cyber Security Adoption (ICSA)

The theoretical underpinnings of linear regression and the necessary assumptions thereof were already discussed in Section 4.2.7

Ordinary least squares regression was used to develop a linear probability model in the area of IoT Cyber Security adoption based on the assumptions mentioned in Section 4.1.7 [85][86], Table 4.21.

IoT Cyber Security was designed with one question in mind: whether or not respondents planned to renew their subscriptions in the following year or purchase a new subscription (ICSII).

The regression analysis, Table 4.22, was performed with IoT Cyber Security intention (ICSII) as the dependent variable and a total of two constructs included for measuring IoT Cyber Security adoption i.e, Relative advantage (RA) and Facilitating conditions (FC) as the independent variables respectively.

The adjusted R square of the emerging model, Table 4.23 was 0.820 ($F(2,16)=7.4365$, p <0.001). Both of the predictor variables included in the analysis were found to be very significant, Table 4.24. These are the relative advantage RA ($\beta = 1.008$, $p< 0.001$) and facilitating conditions FC ($\beta = 1.012$, $p< 0.001$) respectively, Table 4.24

Table 4.21 Model Summary: IoT Cyber Security Adoption (ICSA)

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.912[a]	.831	.820	.236
a. Predictors: (Constant), RA, FC				

Table 4.22 Analysis of variance : IoT Cyber Security Adoption (ICSA)

Model		Sum of Squares	Df	Mean Square	F	Sig.
1	Regression	4.1376	2	4.138	7.4365	.000[a]
	Residual	.8402	15	.056		
	Total	4.9778	17			
a. Predictors: (Constant), FC, RA						
b. Dependent Variable: ICSA						

Table 4.23 Regression Analysis: IoT Cyber Security Adoption (ICSA)

Coefficients[a]						
		Unstd. Coef		Std.Coef		
Model		B	Std.Error	Beta	T	Sig.
1	(Constant)	.651	.273		2.385	.018
	FC	.619	.124	1.012	5.009	.000
	RA	.715	.112	1.008	5.850	.000
a. Dependent Variable: ISCA						

4.5 Summary

This chapter discussed the data analysis and presentation for the first three objectives of this research namely:-

1. To identify the metrics that contribute to increased IoT Cyber Security readiness of a developing country
2. To identify the metrics that contribute to increased IoT Cyber Security intensity in a developing country

3. To identify the metrics that contribute to increased IoT Cyber Security adoption in a developing country

The results of these objectives were to be used to accomplish the fourth objective, namely, to specify a model to asses the state of IoT Cyber Security for a developing country based on the readiness, intensity, and adoption metrics above.

The chapter has presented the research results of the first three chapters in three distinct steps: Firstly, the individual items that were included to measure each of the constructs of the domains of IoT Cyber Security readiness (ICSR), IoT Cyber Security intensity (ICSI), and IoT Cyber Security adoption (ICSA), their rationale thereof, and situational significance and relevance to the domain under investigation were outlined.

As a second step in this study, we looked at descriptive statistics, such as mean and standard deviation, for each item that was used to measure IoT Cyber Security readiness (ICSR), IoT Cyber Security intensity (ICSI), and adoption (ICSA) for each of these three domains in a developing country setting.

Thirdly, the results of Ordinary Least Squares Regression employed to fit a linear probability model in order to investigate the influence of the independent variables on each of the dependent variables in the IoT Cyber Security readiness (ICSR), IoT Cyber Security intensity (ICSI), and IoT Cyber Security adoption (ICSA) domains were reviewed.

With reference to results in Section 4.2.7, Section 4.3.4, and Section 4.4.4 respectively, a total of nine constructs were found significant for explaining the variation of the dependable variables in the three research domains is as enumerated below.

(i).IoT Cyber Security Readiness (ICSR) : Human Resource (MBAD), Policy (POL) and Regulatory (REG) constructs

(ii). IoT Cyber Security Intensity (ICSI) : Education (ED) and years of experience I (EX), Effectiveness of IoT cyber security (EIS), Perceived implementation of IoT cyber security (ICS)

(iii) IoT Cyber Security Adoption (ICSA): Relative Advantage (RA) and Facilitating Conditions (FC)

CHAPTER FIVE

IoT CYBER SECURITY ASSESSMENT MODEL (IoTCSAM) AND METRIC

5. 1 Introduction

The previous Chapter presented the research results of the metrics that determine increased IoT Cyber Security Readiness (ICSR), IoT Cyber Security Intensity (ICSI), and IoT Cyber Security Adoption (ICSA) respectively, in a developing country instance with focus on Uganda

Building on the work of the previous Chapters, and specifically on the eight constructs found significant for explaining the variation of the dependable variables in the three research domains in Chapter 4, this Chapter presents a model, the IoT Cyber Security Assessment Model (IoTCSAM) that scores the state of IoT Cyber Security of a country based on three sub -indices namely, IoT Cyber Security readiness (ICSR), IoT Cyber Security intensity (ICSI), and IoT Cyber Security adoption (ICSA), respectively, across the eight constructs.

5.2 Theoretical Basis

In Chapter two, it was noted that specific research relating to IoT Cyber Security models in the readiness, intensity and adoption domains are still at the infancy stage [][][] thus necessitating this research.

It is on this basis that this research went beyond the determination of the individual constructs responsible for increased IoT Cyber Security readiness (ICSR), IoT Cyber Security intensity (ICSI), and IoT Cyber Security adoption (ICSA) respectively, in a developing country instance, and developed a model, the IoT Cyber Security assessment model (IoTCSAM) for measuring the state of IoT Cyber Security for a developing country. The IoTCSAM model can also be used for benchmarking purposes.

5.3 The IoTCSAM Model

The IOTCSAM model seeks to establish a metric across the entire IoT Cyber Security ecosystem of readiness, intensity, and adoption to measure the state of IoT Cyber Security in developing countries. The IOTCSAM model is used to specify the IOTCSAM composite metric, and is composed of the following three sub-indices as defined in Literature Review in Chapter Two, namely:

• *IoT Cyber Security readiness sub-index (ICSR)*: Concerned with the policy, regulatory, technical, commercial and physical infrastructures necessary to support IoT Cyber Security

• *IoT Cyber Security intensity sub-index (ICSI)*: Concerned with the state of IoT Cyber Security implementation and effectiveness respectively

• *IoT Cyber Security adoption sub-index (ICSA)*: Concerned with the attitudinal, normative and control factors that influence intentions to adopt IoT Cyber Security.

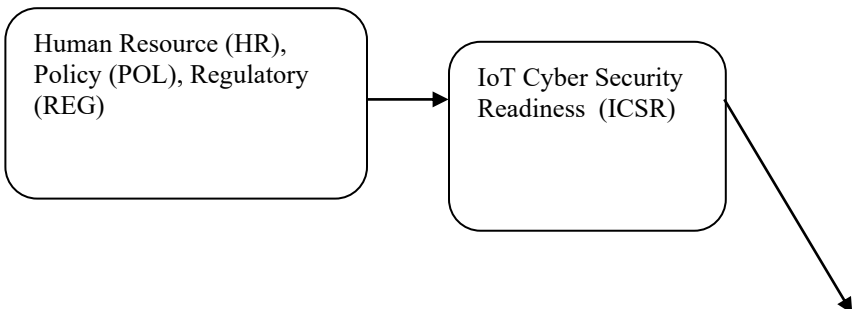
The IOTCSAM model postulated that the overall state of IoT Cyber Security for a given country, measured by the IoT Cyber Security Assessment Metric (IoTCSAM) is affected in similar or different proportions, n_x, by the three sub-indices, ICSR, ICSI, and ICSA respectively. The sub-indices were derived from the nine (9) constructs, found significant for explaining the variation of the dependable variables in the three research domains, respectively.

The significant constructs for ICSR, ICSI, and ICSA, respectively, are shown in Table 5.1

Table 5.1 Significant constructs for ICSR, ICSI, and ICSA

Sub-Index	Significant Constructs
IoT Cyber Security Readiness (ICSR)	Policy (POL), Human Resource (MBAD) Regulatory (REG).
IoT Cyber Security Intensity (ICSI)	Education (ED) and years of experience (EX), Effectiveness of IoT cyber security (EIS), Perceived implementation of IoT cyber security (ICS)
IoT Cyber Security Adoption (ICSA)	Relative Advantage (RA) and Facilitating Conditions (FC)

The IOTCSAM model, Figure 5.1, illustrates the linkages between the significant constructs for each domain, the respective sub-indices (ICSR, ICSI and ICSA), and the composite IOTCSAM metric.



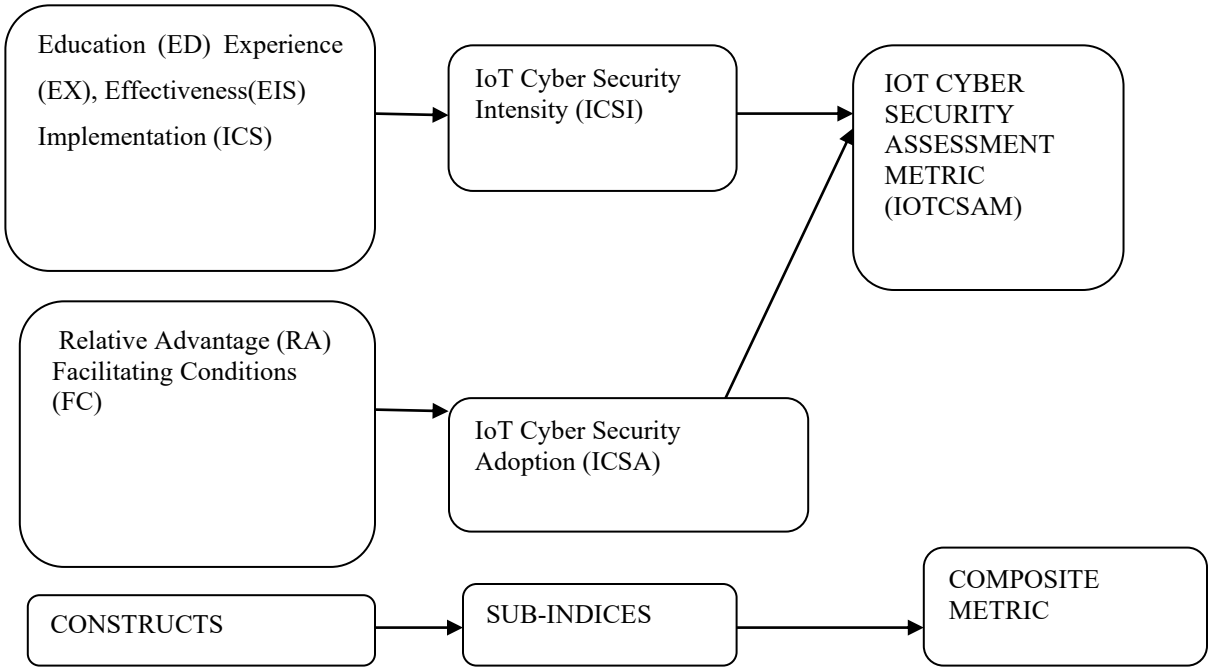


Figure 5.1 The IoT Cyber Security Assessment (IoTCSAM) model and metric

Source: Researcher

5.3.1 IoTCSAM Composition

The three IoTCSAM model sub-indices were derived using nine constructs according to the following structure (see also Figure 5.2)

A. IoT Cyber Security Readiness (ICSR) sub-index

1. Human Resource (MBAD)
2. Policy (POL)
4. Regulatory (REG)

B. IoT Cyber Security Intensity (ICSI) sub-index

1. Education (ED)
2. Experience (EX)
3. Effectiveness (EIS)
4. Implementation (ICS)

C. IoT Cyber Security Adoption (ICSA) sub-index

1. Relative Advantage (RA)
2. Facilitating Conditions (FC)

5.3.2 The IOTCSAM Equation

The IOTCSAM model postulated that the overall state of IoT Cyber Security for a developing country, measured by the IoT Cyber Security Assessment Metric (IoTCSAM) is affected in similar or different proportions, n_x, by the three sub-indices, ICSR, ICSI, and ICSA respectively. Thus, assuming a linear relationship [14][16]

$IoTCSAM_j = n_1 ICSR_j + n_2 ICSI_j + n_3 ICSA_j$……...(i)

Where n_1, n_2, and n_3 are the weightings for ICSR,ICSI, and ICSA sub-indices respectively, j= country, and

ICSR (or ICSI or ICSA)= $\sum_{i=1,m} w_{ij} e_{ij} /m$…….(ii)

Where *ICSR or ICSI or ICSA*: respective sub-index

j: country

i: each of the constructs used in computing the sub-index

wij: relative weights assigned to the construct (i)

eij : individual score for each construct on a scale of one

m: number of constructs per sub-index.

In the IoTCSAM, the three sub- indices are given equal weights, in line with [][][]arguments i.e $n_1 = n_2 = n_3 = n$. The construct weightings w_i are also equal. Thus equation (i) becomes

$IoTCSAM_j = (ICSR_j + ICSI_j + ICSA_j)/3$…….....(iii)

For ease of comparison, IoTCSAM is specified on scale of 10. Thus for country j, the IoT Cyber Security Assessment Metric, IoTCSAM is specified as follows:-

IoTCSAM = 10 (ICSR + ICSI + ICSA)/3…….....(iv)

5.3.3 General observations in specifying IoTCSAM

According to [] [] [], a variety of ways can be employed to collect data for the computation of the sub-indices, the most important of which are as follows:

(i). Questionnaire data was collected based on the perspectives of key policymakers and leaders in the information and communications technology sector.

(ii) Hard data is acquired from sources such as the World Bank, the World Economic Forum, and the International Telecommunications Union, among others, by country-designated representatives such as industry regulators, who in turn collect data from industry participants.

(iii) Individual country self-assessment tools data maintained by their national bureau of statistics.

Given that it was noted that specific research relating to IoT Cyber Security models in the readiness, intensity and adoption domains are still at the infancy stage globally, the researcher chose to utilize the first option, namely, questionnaire data collected based on opinions of key policy makers and leaders in the ICT sector for specifying, evaluating, and validating the IoTSCAM model and metric respectively.

5.4 Validation of the model

With regards to Section 5.3.3, it was not possible to use hard data acquired from sources such as the World Bank, the World Economic Forum, and the International Telecommunications Union, as well as data collected from country-designated representatives such as industry regulators who in turn collect data from industry participants for validation, as such databases for IoT cyber security are still in their infancy and are not publicly available.

Similarly, It was not possible to validate this model and metric through individual country self-assessment tools data maintained by their national bureau of statistics since such data is largely not being collected by the national statistical offices.

In this regard therefore, the expert validation, or Delphi Method technique was the most suited method to use to evaluate and validate the developed IoTSCAM model and metric. The Delphi validation method has advantages of enabling a large group of geographically dispersed, time separated experts to participate in an on-line validation exercise either simultaneously or through an on-line questionnaire [27]. Using this method, 26 purposively selected experts were ustilised to validate the model and metric. The subject matter experts were asked two questions in this to gauge the suitability of the IoTCSAM model developed for modelling the state of IoT cyber security for a developing country. and the suitability of the IoTCSAM metric developed in assessing the state of IoT cyber security for a developing country. The two questions were based on a five-point likert scale type in nature, ranging from strongly disagree to strongly agree with a neutral option. They were adopted from [28]. The results of the experts validation is shown in Table 5.2, and appropriately validated the IoTCSAM model (79.3% of experts agreeing or strongly agreeing) as well as the the IoTCSAM metric developed (82.5% agreeing or strongly agreeing)

Table 5.2: Validation results of the IoTCSAM from IT/IS experts based on the parameter of functionality

Functionality	**SD**	**D**	**N**	**A**	**SA**
The IoTCSAM model developed is suitable for modelling the state of IoT cyber security for a developing country	4.0%	10.3%	6.4%	52.9%	26.4%
The IoTCSAM metric developed is suitable for assessing the state of IoT cyber security for a developing country	7.3%	8.2%	2.0%	14.3%	68.2%

CHAPTER SIX

DISCUSSION OF RESULTS

6.1 Introduction

This chapter discusses the key findings of the research in regard to the metrics responsible for increased IoT Cyber Security readiness (ICSR), IoT Cyber Security intensity (ICSI), and IoT Cyber Security adoption (ICSA), respectively, in a developing country, as well as on the developed model, and composite metric (IoTCSAM) for assessing the overall state of IoT Cyber Security of a developing country.

6.2 IoT Cyber Security Readiness (ICSR)

Considering the research findings, it emerges that in order to improve the IoT Cyber Security readiness of Uganda, more emphasis should be laid on developing the IoT Human resource capacity, as well as enacting and operationalizing the necessary IoT policy (POL) enhancing digital Literacy (DL), and regulatory (REG) aspects of cyber security respectively.

Under the Policy (POL) Construct, the research established that while the Computer Emergency Response Team/Coordination Center (CERT.UG/CC) has been established in Uganda for a while**,** there is need to improve the effectiveness of the National CIRT (CERT.UG/CC) in managing cyber incidents. Further, the research established that there is need to adopt a broader view of IoT Cyber Security as an ecosystem in order to define IoT Cyber Security beyond the traditional notion of computer security, but rather, that IoT Cyber Security be considered as an ecosystem comprised of networks, humans, devices, the applications they supply, and network services.

Research shows that Uganda has passed the Computer Misuse Act of 2011 to protect electronic transactions and information systems from illegal access, abuse, or misuse of information systems, including computers and mobile devices. However, the study

suggests the establishment of accompanying computer misuse laws in order to operationalize the Computer Misuse Act of 2011.

Furthermore, there is need to Development of a National IoT Cyber Security Strategy to guide on the implementation of the strategic activities relating to the IoT cyber security.

In terms of human resource capacity, the most significant constructs to support IoT cyber security were established to be an effective of the Cyber security policy or information security policy for the organisation including a possible security certification i.e ISMS ISO 9001:2013 or a similar standard. Further, the effectiveness of the cyber security Department/Division dedicated to overseeing cyber security management in the organisation was found to significantly positively influence IoT cyber security readiness

Further, improved digital literacy in terms of both the general digital literacy of the masses, and that of IoT cyber security experts was found to positively IoT cyber security readiness

6.3 IoT Cyber Security Intensity (ICSI)

In order to investigate the IoT cyber security intensity in Uganda, both **Demographic factors**, which are the socio-economic characteristics expressed statistically including gender, age, marital status, education level, income level, occupation, and employment, among others, and **Control factors,** which influence the state of IoT Cyber Security implementation and effectiveness were considered.

With regard to demographic constructs, it was established that majority of the study respondents were male with 74 out of the 127 respondents constituting a percentage of (58.3%) being males while 53 were females. This is consistent with the findings of other studies that showed a large percentage of individuals in Science & Technology in general, and in ICTs in particular, were males. The study therefore recommends specific

gender targeted campaigns to spur women and girls participation in Science and technology. In terms of segregation by age, nearly three quarters of the respondents were below 45 years of age. What this suggests is the need to leverage the youthful innovative populations of developing counties in general and Uganda in particular to increase the intensity of knowledge in emerging and advanced ICTs such as IoT cyber security.

In terms of level of education, over two thirds of the respondents (68.0%) had above at least a masters degree, followed by respondents with at least a first degree (40%), and with diploma holders constituting 15.0% of the respondents. The distribution of respondents by highest level of education services as an indication of the specialized knowledge required to implement IoT cyber security initiatives and therefore the need for national Governments to institute specialized postgraduate degree programmes and specialized certifications to support human capacity in emerging and advanced ICTs such as IoT cyber security.

In addition to higher qualifications in IoT cyber security related disciplines, the research established that fairly higher number of years of experience in IoT cyber security related disciplines would be required to support widespread intensity of IoT cyber security.

With regard to the control constructs that were used to measure IoT Cyber Security intensity (ICSI), the effectiveness of cyber security of IoT deployments across multimedia services, Government services, e-Commerce, e-Health, Education, Manufacturing, and Supply chain was found to most significantly positively influence IoT cyber security intensity, followed by the respondent's perception that Cyber Security was actually being implemented in IoT deployments. constructed to capture the usage item under investigation. However, the total number of IoT deployments did not significantly positively influence the intensity of IoT cyber security.

6.4 IoT Cyber Security Adoption (ICSA)

This study investigated IoT cyber security adoption based on two main constructs namely, the Relative Advantage and the Facilitating conditions respectively.

With regard to the Relative Advantage (RA) construct, the item on perceived better user privacy and security was most significant in explaining variations in IoT cyber security adoption. The second most significant item in explaining variations in IoT cyber security adoption under the relative advantage construct was the perceived better protection of data and networks while the item on perceived better user satisfaction and experience was less significant in explaining variations in IoT cyber security adoption.
A number of items were considered under the facilitating conditions (FC) construct including

(i). Perceived declining costs of IoT Cyber Security services
(ii). Availability of IoT Cyber security as a service
(iii). Availability of different IoT cyber security service providers
(iv). Perceived reliability of IoT Cyber Security offerings
(v). Perceived knowledge or expertise in IoT cyber security
(vi). Referent's influence in the adoption of IoT cyber security

The two most significant items in the facilitating conditions category for explaining variations in IoT cyber security adoption were the perceived reliability of IoT cyber security offerings and Referents influence in adopting IoT cyber security respectively.

The availability of different IoT cyber security service providers and the perceived knowledge or expertise in IoT cyber security moderately influenced the adoption of IoT cyber security.

Finally, the perceived declining costs of IoT Cyber Security services and the availability of IoT Cyber security as a service items were less significant in influencing the adoption of IoT cyber security.

6.5 IoT Cyber Security Assessment Index (IoTCSAM) Model and Composite Metric

The IoTCSAM model and composite metric address the critical need for IoT Cyber Security metrics in the domains of readiness, intensity, and adoption in developing countries in order to facilitate informed decision-making among stakeholders in the IoT Cyber Security eco-system, including policymakers, regulators, IoT Cyber Security service providers, researchers, and the general public.

The proposed IOTCSAM model has a number of advantages. For example, a government might rapidly evaluate which IoT Cyber Security targets need to be improved in comparison to others, as well as the order in which these targets should be addressed. The IoTCSAM model highlights critical demand-side issues such as expanding digital literacy and broadening the scope of IoT cyber security.

For instance, based on the findings of an evaluation of a country's state of IoT cyber security, a policymaker in Gambia would conclude that developing a national IoT Cyber Security policy or strategy is critical for the country, whereas a policymaker or IoT Cyber Security service provider in Ghana would infer the need to increase IoT Cyber Security adoption. Additionally, a policymaker or operator in Uganda might infer the importance of increasing public knowledge about IoT Cyber Security, but a policymaker in Zimbabwe would emphasise the importance of improving digital literacy, for example.

The algorithm for computing the IoTCSAM is programmable, and the process of calculating the composite IoT Cyber Security assessment metric may easily be automated. Additionally, the weights assigned to each construct or measure in the IoTCSAM model can be adjusted to reflect the priorities of the decision modeller and to accommodate the unique requirements of a particular country.

Finally, while the IoTCSAM model and metric were developed with a particular emphasis on developing country features, they can be utilised in worldwide benchmarks for the state of IoT Cyber Security.

6.6 Summary

This Chapter discussed the key findings of the research in regard to the metrics responsible for increased IoT Cyber Security readiness (ICSR), IoT Cyber Security intensity (ICSI), and IoT Cyber Security adoption (ICSA), respectively, in a developing country. Several policy, regulatory, human resource, demographic, relative advantage, and facilitating conditions constructs as well as the items used to measure them were considered. Finally, the application of the developed model, and composite metric (IoTCSAM) for assessing the overall state of IoT Cyber Security of a developing country, and for benchmarking purposes were considered.

These discussions form the basis of the recommendations to stakeholders in the IoT Cyber Security eco-system further enumerated in the next Chapter.

CHAPTER SEVEN

RECOMMENDATIONS, FUTURE WORK, AND CONCLUSION

7.1 Introduction

This Chapter summarises the key recommendations of the research in regard to the metrics responsible for increased IoT Cyber Security readiness (ICSR), IoT Cyber Security intensity (ICSI), and IoT Cyber Security adoption (ICSA), respectively in a developing country context, with special emphasis on Uganda, as well as on the model, and composite metric (IoTCSAM) developed in Chapter Five for assessing the overall state of IoT Cyber Security of a developing country. The Chapter then enumerates limitations of this research, suggests further areas of research and concludes by examining the initial research objectives and questions as outlined in Chapter One visa-viz the research findings.

7.2 Recommendations

The research findings lead to a number of recommendations for consideration by policy makers, ICT regulators, IoT Cyber Security service providers, researchers, ICT experts and the general public in Uganda, and other developing countries for informed decision making in relation to the factors responsible for increased IoT Cyber Security readiness, IoT Cyber Security intensity, and IoT Cyber Security adoption. Further recommendations concerning the use of the developed IOTCSAM model and composite metric (IoTCSAM) tool for assessing the overall state of IoT Cyber Security of a developing country are considered.

7.2.1 IoT Cyber Security Readiness (ICSR)

Considering the research findings, the following are recommended with regard to improving IoT Cyber Security readiness in Uganda, and other developing countries.

(i). There is need to improve the effectiveness of the National CIRT (CERT.UG/CC) in managing cyber incidents by adopting a broader view of IoT Cyber Security as an ecosystem in order to define IoT Cyber Security beyond the traditional notion of computer security to include, but not limited to networks, the personnel, the devices, the applications they deliver, and services offered on the networks.

(ii). While the study found that Uganda enacted the Computer Misuse Act of 2011 to ensure the safety and security of electronic transactions and information systems and to prevent unlawful access, abuse, or misuse of information systems, including computers and mobile devices, the study also suggests that the Computer Misuse Act of 2011 be accompanied by computer misuse regulations.

(iii). Furthermore, there is need to develop of a National IoT Cyber Security Strategy to guide on the implementation of the strategic activities relating to the IoT cyber security.

(iv). There is need for organisations to develop and operationalize an effective cyber security policy or information security policy for the organisation including a possible security certification i.e ISMS ISO 9001:2013 or a similar standard.

(v). Enhance the effectiveness of the cyber security Department/Division dedicated to overseeing cyber security management in the organisation was found to significantly positively influence IoT cyber security readiness

(vi). Further, improved digital literacy in terms of both the general digital literacy of the masses, and that of IoT cyber security experts was found to positively IoT cyber security readiness

7.2.2 IoT Cyber Security Intensity (ICSI)

In order to investigate the IoT cyber security intensity in Uganda, both **Demographic factors**, which are the socio-economic characteristics expressed statistically including gender, age, marital status, education level, income level, occupation, and employment, among others, and **Control factors,** which influence the state of IoT Cyber Security implementation and effectiveness were considered. Arising from the study, the following are the key findings with regard to IoT Cyber Security Intensity (ICSI) domain.

(i). The study recommends specific gender targeted campaigns to spur women and girls participation in Science and technology and the need to leverage the youthful innovative populations of developing counties in general and Uganda in particular to increase the intensity of knowledge in emerging and advanced ICTs such as IoT cyber security.

(ii). Therefore is need for national Governments to institute specialized postgraduate degree programmes and specialized certifications to support human capacity in emerging and advanced ICTs such as IoT cyber security.

(iii). The study recommends a more effective secure IoT deployments across multimedia services, Government services, e-Commerce, e-Health, Education, Manufacturing, and Supply chain among others.

7.2.3 IoT Cyber Security Adoption (ICSA)

This study investigated IoT cyber security adoption based on two main constructs namely, the Relative Advantage and the Facilitating conditions respectively. Arising from the study the following are the recommendations with regard to IoT Cyber Security Adoption

With regard to the Relative Advantage (RA) construct, the study recommends the need

for national governments to take specific steps to improve user privacy and security leading to better protection of data and networks.

With regard to the facilitating conditions, the study recommends the improvement of reliability of IoT cyber security offerings and leveraging referents influence in adopting IoT cyber security respectively. The referents influence will normally be from experts from the IoT cyber security space.

7.2.4 IoT Cyber Security Assessment Index (IoTCSAM) Model and Composite Metric

The study suggests that policymakers, regulators, IoT Cyber Security service providers, researchers, and the general public use the IoTCSAM model and composite metric to make educated decisions in the IoT Cyber Security eco-system.

The paper also suggests automating the IoTCSAM computation method, with customizable weights assigned to each construct or measure in the IoTCSAM model to represent the priorities of a particular decision modeller and to meet the unique needs of a certain country.

Finally, the study suggests that the IoTCSAM model and metric be employed in worldwide standards for IoT Cyber Security.

7.3 Limitations and Future Work

Several limitations in this research are presented.

(i). The initial research to establish the frameworks for building the IOTCSAM Model's sub-indices, namely IoT Cyber Security Readiness (ICSR), IoT Cyber Security Intensity (ICSI), and IoT Cyber Security Adoption (ICSA), were undertaken in Uganda, a representative of poor countries. While the research findings have been extrapolated to

other developing countries, future research may include additional cross-country surveys in a variety of developing countries.

(ii). Due to the difficulties to obtain appropriate advance information on IoT Cyber Security knowledge, the research sample approach was confined to purposeful judgement and snowballing.

(iv). Although the researcher was unable to collect data longitudinally due to resource restrictions, such constraints can be solved in future studies of a similar kind by extending the data collection time.

(v). Furthermore, given the impacts of cross sub-index or construct correlation and covariance, the additive functions and averaging used in the IOTCSAM model and composite metric method may not accurately reflect the composite effect of the factors. As a result, future study should moderate sub-indices and constructs in order to evaluate their cross-relationships.

(vi). Finally, the IOTCSAM Model and Composite metric's sub-index and construct weights are subjectively determined. Future study may examine more complex statistical approaches for developing the sub-indices and construct weights.

7.4 Conclusion

This research thesis sought to fill the gap in the availability of a suitable model, and metrics for accessing the state of IoT Cyber Security in a developing country context, in this instance, Uganda. Thus the general research question posed in Chapter One was

> **RQ: Which model, and metrics can be specified to measure the state of IoT Cyber Security in developing countries, with the case of Uganda?**

In order to answer this question, the research was organized into three domains of IoT Cyber Security readiness (ICSR), IoT Cyber Security intensity (ICSI), and IoT Cyber

Security adoption (ICSA), leading to the decomposition of the above research question into four specific research questions namely:

RQ1. Which metrics contribute to increased IoT Cyber Security readiness in Uganda, as developing country?

RQ2. Which metrics contribute to increased IoT Cyber Security intensity in Uganda, as developing country?

RQ3. Which metrics contribute to increased IoT Cyber Security adoption in Uganda, as developing country?

RQ4. Which model, and composite metric can be specified to measure the state of IoT Cyber Security for a developing country based on the readiness, intensity, and adoption metrics above.

The corresponding general objective, and specific objectives as outlined in Chapter One are reproduced below:

Objective: To develop a model, and metrics in the readiness, intensity and adoption domains that can be used to measure the state of IoT Cyber Security for a developing country.

Specific Objective 1. To identify the metrics that contribute to increased IoT Cyber Security readiness in Uganda

Specific Objective 2. To identify the metrics that contribute to increased IoT Cyber Security intensity in Uganda

Specific Objective 3. To identify the metrics that contribute to increased IoT Cyber Security adoption in Uganda

Specific Objective 4. To specify a model, and composite metric to measure the state of IoT Cyber Security for a developing country based on the readiness, intensity, and adoption metrics above

Based on the findings and discussions in Chapters Four to Six, three metrics namely the Policy, Human resource and Regulatory were identified to most significantly explain the variation in IoT Cyber Security readiness in Uganda, thus answering research question one, and fulfilling research objective one respectively.

Four metrics namely Education, Experience, Effectiveness, and Implementation were identified to most significantly explain the variation in IoT Cyber Security intensity in Uganda, thus answering research question two, and fulfilling research objective two respectively.

Two metrics namely Relative Advantage and Facilitating Conditions were identified to most significantly explain the variation in IoT Cyber Security adoption in Uganda, thus answering research question three, and fulfilling research objective three respectively.

Based on the metrics developed in the three domains, Chapter Five, specified a model, and composite metric the IoT Cyber Security Assessment metric (IoTCSAM) for assessing the state of IoT Cyber Security in a developing country, thus answering research question four, and fulfilling research objective four respectively.

The IoTCSAM model, and composite metric was evaluated and validated through experts groups using the “Delphi” method.

Thus the general research question, and the specific research questions posed in Chapter One have been appropriately answered. Similarly, the corresponding general research objective, and the specific objectives specified in Chapter One have been achieved. In conclusion, the thesis aim has been met.

Attention of all stake-holders in the IoT Cyber Security eco-system is drawn to the factors that are reported as significant in order to improve the readiness, intensity, and adoption of IoT Cyber Security in Uganda and other developing countries.

REFERENCES

1. Ge, M., & Kim, D. S. (2015). A model for modeling and assessing security of the internet of things. *In 2015 IEEE 21st International Conference on Parallel and Distributed Systems (ICPADS)* (pp. 776-781). IEEE.

2. Duan, X., Ge, M., Le, T. H., Ullah, F., Gao, S., Lu, X., & Babar, M. A. (2021). Automated Security Assessment for the Internet of Things. arXiv preprint arXiv:2109.04029.

3. Radanliev, P., De Roure, D. C., Nurse, J. R., Burnap, P., Anthi, E., Uchenna, A., & Montalvo, R. M. (2019). Cyber risk management for the Internet of Things. Univ. Oxford, 1-27.

4. Jyri Rajamaki, and Rauno Pirinen (2017). Towards the cyber security paradigm of ehealth: Resilience and design aspects, *AIP Conference Proceedings* 1836, 020029 (2017); doi: 10.1063/1.4981969

5. He et al. (2016). The Security Challenges in the IoT enabled Cyber-Physical Systems and Opportunities for Evolutionary Computing & Other Computational Intelligence, *In: EEE Congress on Evolutionary Computation (CEC 2016*), 1015-1021 University of Limoges, France.

6. Ana Lauge, Josune Hernantes, Jose M. Sarriegi (2015). Critical infrastructure dependencies: A holistic, dynamic and quantitative approach, *International Journal of Critical Infrastructure Protection, Volume 8, Pages16-23,ISSN 1874-5482.*

7. Cristina Alcaraz, Sherali Zeadally (2015). Critical infrastructure protection: Requirements and challenges for the 21st century, *International Journal of Critical Infrastructure Protection,* Volume 8, pages 53-66, ISSN 1874-5482.

8. Bela Genge, Piroska Haller, Istvan Kiss (2016). A model for designing resilient distributed intrusion detection systems for critical infrastructures, *International Journal of Critical Infrastructure Protection*, Volume 15, Pages 3-11, ISSN 1874-5482

9. Hathaway (20130, “Cyber Readiness Index 1.0”, Hathaway Global Strategies LLC,, 2013.

10. Barajas, (2014). Pragmatic Security Metrics: Applying Meta metrics to Information Security., 2014.

11. Teodor Sommestad, T. (2012). A model and theory for cyber security assessments. *A Ph.D thesis submitted in partial fulfillment of the requirements for the degree of Doctor of Philosophy.* Industrial Information and Control Systems KTH, Royal Institute of Technology Stockholm, Sweden

12. Herrmann,(2007). Complete Guide to Security and Privacy Metrics Measuring regulatory compliance, operational resilience., 2007.

13. ITU,(2020). Global cyber security Index, 2020

14. ITU, (2010). Toolkit for Cybercrime Legislation", 2010.

15. ITU, (2009).Draft Background Paper Cybersecurity: The Role and Responsibilities of an Effective Regulator.http://www.itu.int/ITU-D/treg/Events/Seminars/GSR/GSR09/doc/GSR-background-paper-on-cybersecurity-, 2009.

16. Tagert, (2010) .Global Cyber security challenges in Developing Nations.Carnegie Mellon University.

17. Green, (2017). A Model for Successful IoT Security Assessment. Technical Insight. https://www.whitehatsec.com/blog/a-model-for-successful-iot-security-assessment/., 2017.

18. Mavropoulos, (2017). A conceptual model to support security analysis in the internet of things. *Computer Science and Information Systems.*, 2017.

19. Mengmeng (2018), Graphical Security Modelling and Assessment for the Internet of Things. Department of Computer Science and Software Engineering,University of Canterbury., 2018.

20. Licciardello.,(2013). "Global IoT phenomenon and its challenges", ITU, 2013.

21. Saunders, (2012). "Research Methods for Business Students" 6th edition, Pearson Education Limited., 2012.

22. Saunders, (2009). Understanding research philosophies and approaches. Research Methods for Business Students. 4. 106-135., 2009.

23. Nabukenya, (2008). Improving the Quality of Organisational Policy Making . The Dutch Research School for Information and Knowledge Systems.

24. Haig, (2005). An abductive theory of scientific method. Psychological methods,10(4), 371., 2005.

25. Trochim, (2006). Deduction and Induction Approach, Department of Computer Science, University of Karachi

26. Creswell, (2013). Research design: Qualitative, quantitative, and mixed methods approaches: Sage publications., 2013.

27. Gray, (2013). Doing research in the real world. Sage., 2013.

28. Soiferman, (2010). Research design in qualitative, quantitative and mixed methods., University of Minnesota 2010.

29. Chawki, (2003). "A Critical Look at the Regulation of Cybercrime, crimeresearch.org 2003.

30. Patton,(1990) .Qualitative evaluation and research methods. SAGE Publications., 1990.

31. Livari & Venable, (2004). Action Research and Design Science Research-Seemingly similar but decisively dissimilar. *A paper presented at the 17th European Conference on Information Systems. University of Oulu, Finland*., 2004.

32. Hevner, (2004). Design Science in Information Systems Research, *MIS Quarterly*, 24, 1, 2004.

33. Krejcie, (1970). Determining Sample Sizes for Research Activities, Educational and Psychological Measurements, 30,608., 1970.

34. Mugenda & Mugenda,(1999). Research methods. ACTS press Kampala, UG

35. Amin,(2005). Social Science Research, Conception, Methodology Analysis. Makerere University Printery.,Kampala, 2005.

36. Holmström, (2009). Bridging Practice and Theory: A John Wiley & Sons, Inc (2009).Design Science Approach to bridging Practice and Theory., 2009.

37. Salant, (1994). How to conduct your own survey. John Wiley & Sons, Inc 1994, 1994.

38. Mugeni, G.B, (2012). IoT cyber security Assessment Index (BAI). A model and Composite Metric for Measuring IoT cyber security in Developing Countries. *International Journal of Information and Communication Technology Research*, Vol. 2, No. 11, pp. 850-861

39. Benedikt, (2017). Cybersecurity policy for the internet of things. A white paper .Microsoft Corporation.

40. ITU,(2014). Global Cyber security Index, ABI research, 2014.

41. Hare, (2019). Private Sector Contributions to National Cyber Security: A Preliminary Analysis. Journal of Homeland Security and Emergency Management, 6(1), pp. -. Retrieved 9 May. 2021, from doi:10.2202/1547-7355.1426, 2009.

42. Yasser I.(2019).Internet of Things (IoT). Importance and Applications.DOI: 10.5772/intechopen.90022. Open access peer-reviewed chapter.

43. Babar, (2011). "Proposed embedded security model for Internet of Things (IoT)," *2011 2nd International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace*

44. Charalampos, (2014). Dynamic Security Awareness Program Evaluation (DSAP).,Springer International Publishing Switzerland, LNCS 8533, pp. 258–269, 2014.

45. Simon,(2015). IoT-Enabled Analytic Applications Revolutionize Supply Chain Planning and Execution. A White Paper.IDC, 2015.

46. Zhijiang, (2015). ACloud computing Based Network Monitoring and Threat Detection System for Critical Infrastructures. Big Data Research. Volume 3, Pages 10-23, 2015.

47. Geir, (2014). A Participatory Design Approach in the Engineering of Ubiquitous Computing Systems, a PhD thesis, The University of Queensland, 2014.

48. Habtamu, (2012). Risk-based adaptive security for smart IoT in eHealth. BodyNets '12 *Proceedings of the 7th International Conference on Body Area Networks*. ICST . ISBN: 978-1-936968-60-2., 2012.

49. Hossain, (2017). A Hardware and Software Co-Verification Based Authentication Scheme for Internet of Things," . *5th IEEE International Conference on Mobile Cloud Computing, Services, and Engineering (MobileCloud),* San Fra, 2017.

50. Preece, (2007). Enhanced SDIoT Security Model Models. Research Article. Hindawi Publishing Corporation.International *Journal of Distributed Sensor Networks.*Volume 2016, Article ID 4807804, 12 pages., 2007.

51. Oscar, (2014). Object security architecture for the Internet of Things. *Proceeding of IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks* 2014,

52. Offermann, Levina, Schönherr & Bub (2009).Outline of a Design Science Research Process., 2009

53. NITA (U), (2017). Draft Policy For ICT Infrastructure Sharing .Ministry of Information, Communications Technology & National Guidance . 2017

54. UCC, (2010). Harmonizing Cyberlaws and Regulations: The experience of the East African Community. Uganda Communications Commission, presented at UNCTAD/DTL/STICT/2012/4/Corr.1.2010

55. EY, (2015). Cybersecurity and the Internet of Things. Insights on Governance, Risk and Compliance.March 2015. Accessible at https://www.ey.com/Publication/vwLUAssets/EY-cybersecurity-and-the-internet-of-things/%24FILE/EY-cybersecurity-and-the-internet-of-things.pdf

56. Alsaadi & Tubaishat, (2015). Internet of Things: Features, Challenges, and Vulnerabilities. *International Journal of Advanced Computer Science and Information Technology (IJACSIT).Vol. 4, No. 1, 2015, Page:1-13, ISSN: 2296-1739*

57. Madakam, Ramaswamy, & Tripathi (2015). Internet of Things (IoT): A Literature Review. *Journal of Computer and Communications*,3,164173. 2015. http://dx.doi.org/10.4236/jcc.2015.35021

58. Polkinghome, (1995). Language and Meaning: Data Collection In Qualitative Research. *Journal of Counselling Pyschology*

59. Carmines & Zeller, (1979). Reliability and Validity Assessment, Newbury Park, CA, SAGE publications

60. Best & James (1998). Research in education.8th ed p. cm. ISBN 0.205.18657-Education-Research.

61. USDJ, (2008). United States Department of Justice . Cyber Crime Workshop. Computer Crime and Intellectual Property Section, Criminal Division, www.cybercrime.gov.Available at https://www.oas.org/juridico/spanish/cyber/cyb9_handout.pdf. 2008

62. Flor, (2009). Fraud, Computer-related fraud and Identity-related fraud. Creative Commons license. 2009

63. Graham (2016). First Things First: Threat Analysis and Assessment for IoT Devices. *Accessed on 02/04/2021 from https://www.iotcentral.io/blog/first-things-first-threat-analysis-and-assessment-for-iot-devices*

64. Angelo,F,Luciano,A.,Andrea,P and Antonio,P(2017) .Using virtual environments for the assessment of cybersecurity issues in IoT scenarios. Simulation Modelling Practice and Theory.Volume 73, April 2017, Pages 43-54

65. Forbes,(2014).The Half-Baked Security of Our 'Internet of Things', http://www.forbes.com/sites/kashmirhill/2014/05/27/article-may-scare-you-away-from-internet-of-things/#688f5bb323dd

66. William M.S. Stout, Vincent E. Urias (2016). Challenges to Securing the Internet of Things. SAND.2016-8524C

67. Gartner, (2019). The Internet of Things: Check Before You Implement, Gartner Inc http://www.gartner.com/technology/research/internet-of-things/

68. Osburg,T.,&Lohrmann,C.,(2017). Sustainability in a Digital World:New Opportunities Through New Technologies. *CSR, Sustainability, Ethics & Governance*. ISBN 978-3-319-54602-5

69. Nurse, Creese & De Roure. (2017). Security risk assessment in Internet of Things systems. *IT professional* 19, no. 5 (2017): 20-26.

70. Amin, S., Schwartz, G. A., & Hussain, A. (2013). In quest of benchmarking security risks to cyber-physical systems. *IEEE Network*, *27*(1), 19-24.
71. Alves, W., Colombo, C. R., Portela, C. R., Ferreira, P., & Dália, R., (2014) .The Use of the Delphi Method for the Validation of a Conceptual Model of Environmental Management Strategies. *2nd International Conference on Project Evaluation. ICOPEV 2014*, Guimarães, Portugal

72. McGeary, J., (2009). A critique of using the Delphi technique for assessing evaluation capability-building needs. *Evaluation Journal of Australasia*, *9*(1), 31-39.

73. Pan, J., & Yang, Z. (2018, March). Cybersecurity Challenges and Opportunities in the New" Edge Computing+ IoT" World. In *Proceedings of the 2018 ACM International Workshop on Security in Software Defined Networks & Network Function Virtualization* (pp. 29-32).

74. Lee, I. (2020). Internet of Things (IoT) Cybersecurity: Literature Review and IoT Cyber Risk Management. *Future Internet*, *12*(9), 157.

75. Mendez, D. M., Papapanagiotou, I., & Yang, B. (2017). Internet of things: Survey on security and privacy. *arXiv preprint arXiv:1707.01879*.

76. Melnikovas, A. (2018). Towards an explicit research methodology: Adapting research onion model for futures studies. *Journal of Futures Studies*, *23*(2), 29-44.
77. O'Cathain, A., Murphy, E. & Nicholl, J. (2007). Why, and how, mixed methods research is undertaken in health services research in England: a mixed methods study. *BMC Health Serv Res* **7.**
78. Kendra, C., (2019).How Does the Cross-Sectional Research Method Work?.Acessed on 20th April, 2021 from https://www.verywellmind.com/what-is-a-cross-sectional-study-2794978

79. Hageman, K., Kim, A., Sanchez, T., & Bertolli, J. (2015). Survey Design and Implementation. In G. Guest & E. Namey (Eds.), *Public Health Research Methods* (pp. 341–378). SAGE Publications, Inc. https://doi.org/10.4135/9781483398839.n12

80. Jansen, H. (2010). The Logic of Qualitative Survey Research and its Position in the Field of Social Research Methods. *Forum Qualitative Sozialforschung / Forum: Qualitative Social Research*, *11*(2). https://doi.org/10.17169/fqs-11.2.1450

81. Mtebe, J. S., & Raisamo, R. (2014). Challenges and Instructors' Intention to Adopt and Use Open Educational Resources in Higher Education in Tanzania. *The International Review of Research in Open and Distance Learning*, *15*(1), 249–271. https://eric.ed.gov/?id=EJ1024358

82. Stuart, K., Maynard, L., & Rouncefield, C. (2015). Collecting Data to Evaluate. In *Evaluation Practice for Projects with Young People: A Guide to Creative Research* (pp. 111–148). London: SAGE Publications Ltd. https://doi.org/10.4135/9781473917811.n8

83. Harris, D. F. (2014). The Complete Guide to Writing Questionnaires: How to Get Better Information for Better Decisions. I&M Press.

84. Boyce, C. & Neale, P. (2006) "Conducting in-depth Interviews: A Guide for Designing and Conducting In-Depth Interviews", Pathfinder International Tool Series

85. Welman, Kruger, & Mitchell. (2005). In *Research Methodology. Third Edition* (pp. 52-55). Cape Town: Oxford University Press Southern Africa.

86. Shields, J. D. (2017). Sampling, determining size. In *The SAGE Encyclopedia of Communication Research Methods* (pp. 1527–1528). Thousand Oaks, CA: SAGE Publications, Inc. https://doi.org/10.4135/9781483381411.n534

87. Budiarto, D. S., Purnamasari, R., Yennisa, Surmayanti, Siradjuddin, I., Hermawan, A., & Herawan, T. (2018). Implementation of Indonesia National Qualification Model 160 to Improve Higher Education Students: Technology Acceptance Model Approach. *International Conference on Computational Science and Its Applications – ICCSA 2018*, 293–304. https://doi.org/10.1007/978-3-319-95165-2_21

88. Saunders & Townsend,(2018). Choosing participants. In *The SAGE Handbook of Qualitative Business and Management Research Methods: History and Traditions* (pp. 480–492). SAGE Publications Ltd. https://doi.org/10.4135/9781526430212.n8

89. Taherdoost,H., (2016,).Sampling Methods in Research Methodology; How to Choose a Sampling Technique for Research. International Journal of Academic Research in Management (IJARM), 2016, 5. ffhal-02546796f

90. Nowell, L. S., Norris, J. M., White, D. E., & Moules, N. J. (2017). Thematic Analysis: Striving to Meet the Trustworthiness Criteria. *International Journal of Qualitative Methods*, *16*(1). https://doi.org/10.1177/1609406917733847

91. Braun, V., & Clarke, V. (2012). Thematic Analysis. In H. M. Cooper, P. M. Camic, D. L. Long, A. T. Panter, D. Rindskopf, & K. J. Sher (Eds.), *APA Handbook of Research Methods in Psychology* (Issue Vol 2: Research designs: Quantitative, qualitative, neuropsychological, and biological). American Psychological Association. https://doi.org/10.1037/13620-000

92. Jansen & Warren (2020). Quantitative Data Analysis 101:The lingo, methods and techniques, explained simply.Accessed on 4th April,2021 from https://gradcoach.com/quantitative-data-analysis-methods/

93. Yaqoob, et. al., (2017). The rise of ransomware and emerging security challenges in the Internet of Things. *Computer Networks*, *129*, 444-458.

94. ENISA (2017), Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures, *European Union Agency for Cyber Security*, ,November. 2017.

95. Kebande, et.al., (2020). Holistic digital forensic readiness model for IoT-enabled organizations. *Forensic Science International: Reports*, *2*, 100117.

96. ISO/IEC 27001:2013, International Standard, Informationm Security Management System – Incident Investigation Principles and Processes, ISO.org, 2015, pp. 1.

97. Shin, D. (2014). A socio-technical model for Internet-of-Things design:A human-centered design for the Internet of Things.*Telematics and Informatics*, *31*(4), 519–531.

98. Guillemin, P., & Friess, P. (2009, September). *Internet of things strategic research roadmap*. The Cluster of European Research Projects. Technical Report.

99. Andrew, (2007).nSecurity Metrics: Replacing Fear, Uncertainty, and Doubt. Upper Saddle River, NJ: Addison-Wesley, 2007.

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

101. Mallory,P., (2021). Cyber Threat Analysis. [Updated 2021]. Management, compliance & auditing. Accessed on 25th -4-2021 from https://resources.infosecinstitute.com/topic/cyber-threat-analysis/

102. Chen, R., Liu, C. M., & Xiao, L. X. (2012). A security situation sense model based on artificial immune system in the internet of things. In *Advanced Materials Research* (Vol. 403, pp. 2457-2460). Trans Tech Publications Ltd.

103. Bajramovic, E., Waedt, K., Ciriello, A., & Gupta, D. (2016, September). Forensic readiness of smart buildings: Preconditions for subsequent cybersecurity tests. In *2016 IEEE International Smart Cities Conference (ISC2)* (pp. 1-6). IEEE.

104. Conklin, W. A. (2006). Computer security behaviors of home PC users: A diffusion of innovation approach. *Ph.D. dissertation*. Retrieved from Dissertations & Theses: Full Text. (Publication No. AAT 3227760)

105. Padyab, A., Habibipour, A., Rizk, A., & Ståhlbröst, A. (2020). Adoption barriers of IoT in large scale pilots. Information, 11(1), 23.

106. Lakmali, Vidanagamachchi & Nanayakkara (2019) . Readiness Assessment for Industry 4.0 in Sri Lankan Apparel Industry.

107. Hu, Chen, He, & Chen, (2013). Protection Intensity Evaluation for a Security System Based on Entropy Theory. *Entropy*, *15*(7), 2766-2787.

108. Østby, Berg, Kianpour, Katt & Kowalski, (2019). A Socio-technical model to improve cyber security training: A work in progress. *CEUR Workshop Proceedings.*

109. Al Sabbagh, B. (2019). Cybersecurity Incident Response: A Socio-Technical Approach (Doctoral dissertation, Department of Computer and Systems Sciences, Stockholm University).

110. Ghaffari, K., Lagzian, M., Kazemi, M., & Malekzadeh, G. (2019). A socio-technical analysis of internet of things development: an interplay of technologies, tasks, structures and actors. foresight.

111. CRA, (2021). Visioning Activity:Sociotechnical Cybersecurity, Computing Research Association, Computing Community Consortium (CCC).Accessed on 5th -05-2021 from https://cra.org/ccc/resources/workshop-reports/

112. Walker, Stanton, Jenkins, Salmon, Young, and Aujla,(2007), "Sociotechnical theory and NEC system design", in Harris, D. (Ed.), *Engineering Psychology and Cognitive Ergonomics, Springer-Verlag, Berlin.*

113. Al Sabbagh, B., & Kowalski, S. (2015). A socio-technical model for threat modeling a software supply chain. IEEE Security & Privacy, 13(4), 30-39.

114. Braun, V., & Clarke, V. (2013). Successful Qualitative Research: A Practical Guide for Beginners. SAGE Publications Ltd.

115. AlEnezi, A. (2019). Internet of Things & Cybersecurity Readiness in Smart-government and Organizations.

116. Ukil, (2011). Embedded Security for Internet of Things (IoT) Market Global Industry Analysis and Opportunity Assessment, 2017-2027.

117. Deloitte, (2020). Increase IoT adoption through a secure cloud approach. Available at https://www2.deloitte.com/content/dam/Deloitte/us/Documents/risk/us-increase-iot-adoption-through-secure-cloud-approach.pdf

118. Kumar, S., Tiwari, P. & Zymbler, M. (2019). Internet of Things is a revolutionary approach for future technology enhancement: a review. J Big Data 6, 111. https://doi.org/10.1186/s40537-019-0268-2

119. Russo, et. al., 2015. Exploring regulations and scope of the Internet of Things in contemporary companies: a first literature analysis. *Journal of Innovative Entreprises 4, 11.*

APPENDIX I:

PUBLICATIONS RELATED TO THIS RESEARCH

1.Ocen, G. G., Mugeni, G.B., Matovu, D. (2016). Role of ICT in Disaster Response and Management: A Review Study of ICT Challenges and Adoption Approaches by Developing Nations, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 6, Issue 5, May 2016 ISSN: 2277 128X, www.ijarcsse.com

2. Ocen, G. G., Mutua, M. S., Mugeni, G. B., Karume, S., & Matovu, D. (2019). An Algorithm and Process Flow Model for the extraction of Digital Forensic Evidence in Android Devices. ISJ Theoretical & Applied Science, 04 (72), 1-10. Soi: http://s-o-i.org/1.1/TAS-04-72-1 Doi: https://dx.doi.org/10.15863/TAS

3.Davis Matovu, Mugeni Gilbert B., Karume Simon, Mutua Stephen, Gilbert Gilibrays Ocen (2019). The Internet of Things: applications and security metrics with the Ugandan perspective. International Journal of Advance Research, Ideas and Innovations in Technology, 5(2) www.IJARIIT.com.

4. Ocen, G. G., Stephen, M., Gilbert, M., Samuel, K. & Davis, M. (2019) A Metric for the Specification of a Consistent Digital Forensic Evidence Extraction Process Model in Mobile Devices. International Journal of Science and Engineering Investigations (IJSEI), 8(88), 88-93. available at http://www.ijsei.com/papers/ijsei-88819-16.pdf

APPENDIX II

QUESTIONNAIRE FOR RESPONDENTS

Dear Respondent, I am a PhD student carrying out a study entitled *"An IoT Cyber Security Assessment Model and Metrics* ". I request you to spare a few minutes of your valuable time to fill this questionnaire. The information you provide will be treated with confidentiality and shall be used for academic purposes only. Please do not put your name on the questionnaire.

Signed (Researcher)_____ **Date**_____

Section A: Demographic data of respondents

1. Gender

Male ☐ Female ☐

2. Age bracket of respondent
   a) Between 18-34 years ☐
   b) Between 35-44 years ☐
   c) Between 45-54 years ☐
   d) Above 55 years ☐
3. Educational level

   Certificate ☐ Diploma ☐ Bachelo☐ Masters and above ☐
4. Number of years of experience in IoT cyber security practice
   a) Less than 5 years ☐
   b) 5-10 years ☐
   c) 10-15 years ☐
   d) Above 15 years ☐

SECTION B

B1) FACTORS THAT DETERMINE THE IoT CYBER SECURITY IN THE DOMAIN OF READINESS

Readiness: These metrics are concerned with the technical, commercial, and physical infrastructures necessary to support IoT cyber security.

On a scale of 1-5, please indicate the degree of your agreement or disagreement with each statement by ticking on the option that applies to you.

1. Strongly disagree 2. Disagree 3. Neutral 4. Agree 5. Strongly agree

	READINESS	1	2	3	4	5
POLICY (POL)						
DSD	Effectiveness of National CERT.UG/CC in managing cyber incidents					
BES	IoT Cyber Security view as an Eco-System					
NBS	Effectiveness of the Cyber Crimes Act					
REGULATORY (HO)						
HOS	Development of regulations to operationalise the cyber security Act					
HON	Establishment of a specific entity to operationalise the cyber security law					
HOO	Development of National IoT cyber security strategy					
HUMAN RESOURCE (MBAD)						
MBR	There is an effective cyber Security Department/Division dedicated to overseeing cyber security management in my organisation					
MBS	There is a corresponding effective Cyber security policy or information security policy for the organisation					
MBE	My Orgaisation is information security certified, i.e ISMS ISO 9001:2013 or certified to a similar standard.					
MBC	The is sufficient effective personal qualified in Information security, and with corresponding certifications					

DIGITAL LITERACY						
ATE	Availability of technical cyber security expertise					
DLM	Digital literacy of the masses					

B2) FACTORS THAT DETERMINE THE IoT CYBER SECURITY RISKS IN THE DOMAIN OF INTENSITY

IoT cyber security constructs are concerned with the state IoT cyber security implementation and effectiveness respectively

On a scale of 1-5, please indicate the degree of your agreement or disagreement with each of the statements below

1. Strongly disagree 2. Disagree 3. Neutral 4. Agree 5. Strongly agree

INTENSITY						
IoT CYBER SECURITY INTENSITY (ISCI)						
TID	Total number of IoT deployments					
ICS	Extent of IoT cyber security Implementation					
EIS	Effectiveness of IoT cyber security					

B3) FACTORS THAT DETERMINE THE IN THE DOMAIN OF ADOPTION

IoT cyber Security metrics are concerned with the Attitudinal, Normative and control factors that influence IoT Cyber Security Adoption

On a scale of 1-5, please indicate the degree of your agreement or disagreement with each statement by ticking on the option that applies to you.

1. Strongly disagree 2. Disagree 3. Neutral 4. Agree 5. Strongly agree

IoT Cyber Security Adoption (ICSA)
RELATIVE ADVANTAGE (RA)

PDN	Perceived better protection of data and networks					
USE	Perceived better user satisfaction and experience					
UPS	Perceived better user privacy and security					
FACILITATING CONDITIONS (FC)						
PDC	Perceived declining costs of IoT Cyber security Services					
SSS	Availability of IoT Cyber Security as a Service					
FCC	Availability of different IoT Cyber security providers					
PRS	Perceived reliability of IoT Cyber Security offerings					
PKC	Perceived Knowledge or expertise in IoT cyber security					
SRI	Referent's influence influence in the adoption of IoT cyber security					

Please insert here any additional information about IoT Cyber Security that would be useful to this research?

.....

.....

.....

Thanks for your time

APPENDIX III
INTERVIEW GUIDE FOR RESPONDENTS

1. What do you think of the effectiveness of the National CERT.UG/CC in managing cyber incidents in Uganda?
2. What is your view of the IoT cyber security eco-system?
3. In your view, how effective is the Cyber crimes Act in enforcing IoT cyber security?
4. How would effective regulations enhance the cyber security act?
5. How do you think the establishment of a specific entity to operationalise the security law?
6. How would the development of the National IoT cyber security strategy aid in improving National IoT cyber security?
7. How effective is your organistional cyber security policy or information policy ?
8. Is your organisation ISO/IEC 27001: 2013 or certified on any security standard? .If so, how has this improved IoT cyber security readiness?
9. What would you say about the availability of technical cyber security experts in your organisation?
10. How would you rate the general digital literacy of the population in Uganda?
11. How do you think an increase in total IoT deployments will affect IoT cyber security in Uganda?
12. How do you think an increase in the total IoT cyber security implementation will affect IoT cyber security in Uganda?
13. How do you think an increase in the total IoT cyber security implementation will affect IoT cyber security in Uganda?
14. Overally, how would rate the effectiveness IoT cyber security in Uganda?

15. What are the perceived relative advantage if IoT cyber security in terms of perceived protection of data and networks?
16. What are the perceived relative advantage if IoT cyber security in terms of perceived protection of data and networks, better user satisfaction and experience, and better user privacy and security respectively?
17. How would you rate the perceived increase in adoption of IoT cyber security due to perceived declining costs of cyber security services?
18. How would you rate the perceived increase in adoption of IoT cyber security due to the availability of IoT cyber security as a service?
19. How would you rate the perceived increase in adoption of IoT cyber security due to the availability of different IoT cyber security offerings?
20. How would you rate the perceived increase in adoption of IoT cyber security due to perceived knowledge or expertise in IoT cyber security ?
21. How would you rate the perceived increase in adoption of IoT cyber security due to the referent's influence of the different stakeholders in the IoT cyber security eco-system?

THANK YOU VERY MUCH FOR YOUR RESPONSES