INTEROPERABILITY MODEL BASED ON INTERNET OF THINGS FOR SMART HOMES

By

Shadrack Kimutai Metto

A thesis submitted in partial fulfilment for the requirement of the degree of Doctor of Philosophy in Information Technology of Masinde Muliro University of Science and Technology.

May 2025

DECLARATION

This thesis is my original work prepared with no other than the indicated sources and support and has not been presented elsewhere for a degree or any other award.

Signature: ___ _____ Date: ___02/10/20205_____

Metto Shadrack Kimutai

SIT/H/15/11

CERTIFICATION

The undersigned certify that they have read and hereby recommend for acceptance of Masinde Muliro University of Science and Technology a Thesis entitled "**Interoperability Model Based on Internet of Things for Smart Homes**"

Signature: _____ Date: _____

Prof. Kelvin K. Omieno

Department of Information Technology and Informatics,

School of Computing and Information Technology,

Kaimosi Friends University.

Signature: _____ Date: _____

Dr. Jasper M. Ondulo

Department of Computer Science,

School of Computing and Informatics,

Masinde Muliro University of Science and Technology.

COPYRIGHT

DEDICATION

This document is dedicated to my dear wife Gladys, sons Lewis & Leon and daughter Lynn. May this work inspire you to a great future.

ACKNOWLEDGEMENTS

I would like to express my sincere gratitude to God in heaven for the sufficient grace he has granted me during my studies.

Special appreciation to my supervisors and mentors Dr. Jasper M. Ondulo and Prof. Kelvin K. Omieno for their expansive knowledge and impressive guidance through the research process. Special mention to Dr. Jairus Odawa, Dr. Nicholas Kiget, Prof. Elyjoy Micheni, Prof. Fred Mzee, Prof. David Gichoya and Dr. Philemon Kitur for their overwhelming support especially on literature and publications that guided my research. Thanks to the faculty from Dr. Daniel Otanga, Dr. Collins Odoyo, Dr. Raphael Angulu and Dr. Gilbert Mugeni. I appreciate the Management of the Masinde Muliro University of Science and Technology, Mr. Cyrus Kamau and The National Commission for Science, Technology and Innovation for the very fast approval and support in data collection for the research. I express my gratitude to Mr. Steve Ngigi and Tekni controls limited, Washington Jalang'o and Mary Muigai of Tumaini Innovation Centre for the opportunity to consult with them on the projects implemented. Thanks to my wife Gladys, sons Lewis & Leon and my daughter Lynn. They made my journey special. I thank my parents Mr. Daniel Metto and the late Mrs. Priscilla Metto whom even in their old age appreciate academics and lastly but not least friends at Moi University, Chebisaas Church Eldoret Family, home and colleagues at University of Eldoret who made my journey a valuable experience.

ABSTRACT

The Internet of Things (IoT) is a group of assorted technologies working seamlessly together. The recommended approach to IoT is to support interoperability in the midst of heterogeneous devices. The challenges associated with smart homes is interoperability in areas such as message exchange, difference in protocols used, energy consumption, antenna design, how to implement adaptive techniques for dynamic situations in the face of heavily constrained resources and security. The objectives of this research are: - To determine the state of device interoperability in Smart Homes, to establish the role of interoperability in Smart Homes in the Internet of Things environments, determine the factors that affect interoperability of devices in smart homes and to develop a model for interoperability in smart homes. The research contributes to the overall concept of making smart homes a reality and enhance acceptance and deployment of heterogeneous Internet of Things devices. The scope of the study included smart home users and experts who deploy smart home devices in Kenya. Two theories adopted were the standards-based theory for service providers and voluntary theory which guided the research. The population covered the users/owners and the experts/vendors or technical staff who deploy smart devices in homes. The data collection methods were interviews and observations. Purposive and snowball sampling was adopted. 18 users and 7 vendors were used. The data was analyzed to derive the mean and standard deviations using statistical package for social scientists and presented in tabular form, pie charts, bar graphs and line graphs. Critical factors found in the investigation were: - Technical, Organizational, Semantic and Legal metrics are critical in the deployment of interoperability of devices in smart homes. A model was developed and a test device implemented to prove viability of the model. The model developed meets the basic needs of the users within a heterogeneous environment however there is need for further education to users on available smart home devices solutions in view of interoperability.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS AND ACRONYMS

AR - Augmented Reality,

ASP - Application Service Providers

BLE - Bluetooth Low Energy

CPS - Cyber Physical Systems

HAN - Home Area Network

HAVi - Home Audio/Video Interoperability

IAD - Integrated Access Device

IFTTT - If This, Then That Services

IoT – Internet of Things

LBS - Location-Based Services

LOC - Lab-on-a-Chip

LPWAN - Low-power Wide-area network

LPWAN - Low-power Wide-area network.

M2H - Machine-to-Human communication

M2M - Machine-to-Machine

MC - Mobile Computing

MQTT - Message Queuing Telemetry Transport

ohNet - Open Home Network

OID - Object Identifier

OSGi - Open Services Gateway Initiative

PC - Pervasive Computing

REST - Representational State Transfer

RFD - Reduced-Function Device

RFID - Radio Frequency Identification

RNS - Radio Network Systems

RNS - Recourse Name Service

SMS - Service Management Systems

SMS - Service Management Systems

SOA - Service Oriented architecture

SOA - Service-Oriented Architecture

SOAP - Simple Object Access Protocol

ubiSD-S - Ubiquitous Service-Discovery Service

UPnP - Universal Plug and Play

WHANs - Wireless Home Automation Networks

WoT - Web of Things

WSN - Wireless Sensor Network

WSNs - Wireless Sensor Networks

DEFINITION OF TERMS

Bluetooth Low Energy (BLE) - is a wireless personal area network technology developed by the Bluetooth Special Interest Group (Bluetooth SIG) that is intended at applications in the healthcare, beacons, fitness, security and smart homes.

Constrained Application Protocol (CoAP) - is a specialized Internet Application Protocol used by constrained devices.

Home Area Network (HAN) this is a network in a home where all devices and smart appliances are interconnected.

IFTTT - It is a no-code automation platform that integrates applications, services, and devices, enabling users to automate tasks and design custom workflows through simple 'if this, then that' logic-based applets

IOT DNS - is a naming and service or device identification method used over the internet, which intends to make IoT global.

LTE – it is a 4G mobile communications standard. It is a standard in UMTS/HSPA for wireless communications in data terminals which are high-speed in nature.

MQTT (Message Queuing Telemetry Transport) – Is a lightweight protocol which works on a principle of publish-subscribe which is designed for connecting devices in resource-limited environments such as in IoT.

Object Identifier (OID) – **This** is an address that is unique used to give a name and it points to a managed device and its status.

Open Home Network (ohNet) - is a library that is generally used for the discovery, monitoring, manipulation and implementation of UPnP devices it can extend to similar protocols.

Open Services Gateway Initiative (OSGi) - is a Dynamic Module System for Java which defines an architecture for development of modules in applications.

Reduced-Function Device (RFD) - are devices, which do not allow association of devices in a branch.

Representational State Transfer (REST) - This is a large-scale networked software which takes ride on protocols of the World Wide Web.

RNS - is a Radio Network System that works by transmitting and receiving electromagnetic waves. OpenWebNet is the protocol that enables remote communication with home automation systems remotely.

SIGFOX - Is a proprietary technology that allows communication using the Medical ISM radio band in Industrial and Scientific applications.

SOAP – means Simple Object Access Protocol. It is an XML-based Messaging Protocol layer which has the ability to route messages through nodes, which perform different functions.

Universal Plug and Play (UPnP) - is a protocol that permits networked or smart devices to automatically discover each other's presence on the network and establish services, which are operational.

Web of Things (WoT) - is a network protocol intended to enable interoperability across all IoT platforms and application areas.

Wireless M-Bus- is a European standard used for remote reading of consumption meters such as gas, water or electricity meters.

Wireless Sensor Network (WSN) – this is a network that is wireless and deployed in an ad-hoc manner with a large number of wireless sensors.

ZigBee - This is a set of high-level protocols which are based on IEEE 802.15.4 used for

creating personal area communication systems with low-power digital radio, which are designed to be used in small-scale applications, that require wireless connections.

Z-Wave – This is a low-power communication protocol running on wireless platforms, which provide end users with a reliable method to remotely control devices and systems specifically in a smart home applications.

CHAPTER ONE: INTRODUCTION

1.0 Chapter Overview

This chapter introduces the background information of the study about smart homes and Internet of things technology, it identifies the problem research questions for each objective, the significance of the study, followed by the scope and limitations.

1.1 Background to the study

The modern man uses or desires to use devices that simplify many processes of life to save time and make them more comfortable. According to empirical research a person spends an average of one hour per day in the fulfilment of everyday operations which are routine and repetitive in nature, such as opening the curtains, turning on or off the lights, opening windows, checking if there is any intrusion, turning on water heaters and so on [1]. The aspect of a smart home therefore comes in to assist in resolving this issue of saving time, reduce operation costs, improve safety, comfort and quality of life. The availability of Internet connection via broadband has become part of our daily life. The connection cost is decreasing daily, all manner of electronic devices which are being developed with Wireless Fidelity (Wi-Fi) capabilities each with an inbuilt sensor and the penetration of smart phone is very high. There is an increasing system of interconnected devices which have sensors, processors and chips which work through a network. The future of smart computing is dependent on the omnipresent detection capabilities of Wireless Sensor Networks (WSNs) that will heavily influence majority of applications in the contemporary living.

Cluster of European research projects which focusses on Internet of Things define ‘Things’ as active players in information, business and social operations where they

interact among themselves within an environment where they exchange data and information which are detected from the surrounding. They respond autonomously to the physical world activities by manipulating the operating processes that induce activities and develop services with or without human engagement [2].

In 2013, the Global Standards Initiative on Internet of Things (IoT-GSI) defined Internet of Things (IoT) as a worldwide structure of interconnection for the information society, which enables progressive services by either virtually or physically interconnecting devices based on existing and emergent inter-operable information and communications (ICT) technologies [1].

The Internet of Things is not a single, unified network of interconnected devices, but a group of assorted technologies, which work seamlessly together at the service for the common good of people in developed and developing countries [3]. The force behind IoT is the development of Smart devices, Smart grids, Smart cars, Smartphones, Virtual power plants, Intelligent transportation, Smart homes, development of Smart cities and hence a smart world. IoT development is based on technology domains such as real-time computing, security, big data, machine learning, privacy and signal processing among others [4].

IoT is enhanced with attached sensors, processors, chips and actuators, where the technology becomes an occurrence of a more general form of a cyber-physical system. Each device in this environment is uniquely recognizable through an integrated computing system in an existing Internet infrastructure, there is a proposal that all imaginable object will soon be interconnected [3]. These interconnected things need to be decently secured to mitigate the risks they are exposed to and protect institutions and

individuals against attacks. Achieving the security goals has been investigated, by diverse and most of the time separate research communities. The research areas covered by these communities include: Internet of Things (IoT), Pervasive Computing (PC), Wireless Sensor Networks (WSN), Cyber Physical Systems (CPS) and Mobile Computing (MC).

IoT is expected to bring in greater cooperation and a bidirectional control on a wide measure such that vehicles can talk to each other and control each other to avert accidents of collisions. It is expected that human beings will be able to exchange data automatically when approaching each other. This will therefore affect their next course of action, and physiological data transferred to medical doctors in real-time and therefore able to get real-time answers from the specific doctor [4].

Smart homes are an emerging application of IoT where technology is used to improve the general level of living and comfort. There are however other aspects which smart homes have as value addition to its inhabitants such as security, energy efficiency, automation of daily chores, enabling more control over their residence and even alleviate the difficulties encountered by either the elderly or those who are handicapped in any way. Smart home technologies which are based on IoT have a bright future [5]. In an IoT setting, smart homes may be utilized to automate home duties. IoT in homes is a gaining a growing popularity among millennials since it is able to deliver smart gadgets that can be remotely accessed and manipulated offering increased efficiency and user comfort.

The key areas of concern in Smart Homes range from Smart Devices such as thermostats, smart lights, smart cameras and smart locks to Home assistants for instance google Home, Apple HomeKit and cloud applications. The challenges and Barriers to smart home deployments range from fragmented ecosystems, Privacy and Security Risks, High Costs for setup and maintenance to Complexity for non-tech-savvy users [6].

For IoT to be greatly successful, it requires openness where all devices can connect to it provided the minimum requirements for connection has been met. However, implementation of openness brings in many new issues hence the need for redesign of devices from composition techniques, security issues, analysis techniques and instruments needed to be implementing this openness. Securely integrated communication channels will be implemented to support efficient data exchange in different systems. Openness is a big challenge to security; on the other hand, it must give an efficient balance between access to systems functionality and security.

IoT systems need to detect attacks, analyze the attack and position countermeasures in time, but execute all of this in a lightweight style due to the low capacity devices concerned. There is a critical need to do real-time authentication of devices, encryption of confidential data, and implement systems and data integrity. Most security solutions found today require large memories due to the heavyweight computations involved, so security solutions for IoT are considered a major challenge.

IoT also has policy and regulatory implications in the areas of spectrum management, licensing, competition, interoperability standards, security and privacy. This means telecommunications regulators must take a lead in implementing this based on sound and tested models [5].

IoT objectives include communication, content and service, network discovery, device discovery, naming and addressing and security and privacy issues [6]. This further states show how communication and security are major points of concern in Internet of Things.

For technology to vanish from the cognizance of the end users, the Internet of Things needs: common understanding of the condition of its end-users and their devices or

appliances, applications architectures and ubiquitous telecommunications networks. The communication networks should be able to compute and communicate the contextual information to relevant destination and the evaluation and analytic tools in the Internet of Things that aim for smart and autonomous conduct [7]. With these central issues in place, smart connectivity and interoperability can be achieved. Generally, the models which have been developed to address various connectivity issues in the Internet of Things which all these models can be summarized as that they cover :- Interoperation of devices, Device discovery and management, inference, Security and Managing data volume in the network.

1.1.1 Basics of Interoperability

Interoperation is the capability of autonomous devices to share information across different domains of applications using a wide range of communication interfaces [8]. Interoperability can be broadly classified based on three different domains: - network Interoperability, syntactic Interoperability and semantic Interoperability [9].

Network interoperability covers the protocols used for exchange of information among autonomous devices across communication networks, it is not bothered with the content of information. It looks at the fundamentals of connectivity found in the first three layers of the OSI Model (physical, datalink and the network layers) It is also argued that occasionally the application layer of the TCP/IP stack is included so as to confirm reliability.

Syntax interoperability addresses the format and structure during encoding of exchanged information among independent devices. It covers the sixth and seventh layers of OSI Model.

Semantic interoperability explains the rules for extracting the meaning from information. It also provides a semantic model which is often domain specific for exchange of information.

1.1.2 Benefits of Interoperability

Interoperability has been recommended for several reasons such as:-first is that when devices such as home appliances or devices become interoperable, the effects on the market is that it becomes competitive and therefore lead to cheaper products for smart homes to do their operations. Secondly, other utility services will be easier to develop and deploy since all devices associated with the services are able to work together seamlessly hence less barriers on entry of new applications or services. Thirdly, Interoperability leads to uniform sharing of common information and resources, which will eventually bring lower cost of services to home dwellers. The other aspect is that there will be a drastic growth of Smart home markets and hence contribute to the Gross Domestic Product (GDP) and encourage multiple vendors compete in the market. Interoperability also provides better security management of both devices and applications. Finally, it reduces costs for operation, integration and upgrading in smart homes.

1.2 Statement of the Problem

There is a shift from “interconnection of computers” to “interconnection of things”. This calls for the need for interoperability of these “things”. It is however, notable that the Internet of Things market is quite fragmented due to device heterogeneity from different vendors although these devices are vertically integrated. Most IoT devices are “closed” whereby customers cannot update the software or add newer patches after devices have been shipped from the factory. The devices involved in the smart environment also face

issues of working with each other due to difference in technologies. Their variances could be in areas such as message exchange, data formats, infrastructure failures, trust among devices on the sense of machine to machine communication, difference in protocols used and how to implement techniques which can reconfigure themselves in a changing environment in the face of probably limited resources. Lack of interoperability implies that customers are tied to the IoT device or software offered by a particular provider and must stick with it, which may bring the probable risk of greater operation cost in the long run, product functionality and stability issues.

1.3 Research Objectives

1.3.1 General Objective

The overall objective is to assess the current state of device interoperability, examine its role within smart homes, identify the factors influencing interoperability, and develop a model that supports seamless device integration in Internet of Things–based smart home environments.

1.3.2 Specific Objectives

i. To determine the state of device interoperability in Smart Homes.
ii. To establish the role of interoperability in Smart Homes in the Internet of Things environments.
iii. To determine the factors that affect interoperability of devices in smart homes in the Internet of Things.
iv. To develop a model for interoperability in smart homes.

1.4 Research Questions

In order for the research to achieve the stated objectives above, the following research questions were used during the study.

i. What is the state of device interoperability in smart homes?
ii. What is the role of interoperability in smart homes in the Internet of Things environments?
iii. Which factors affect interoperability of devices in smart homes?
iv. How can a model for interoperability in a smart home environment be developed?

1.5 Significance of the Study

The research contributes to the overall concept of smooth communication of heterogeneous devices in a secure interactive environment in a smart home that is made up of thousands of interconnected devices that are constantly interacting through message exchange. This was guided by the principle that the common objective of all the middleware improvement research is to create a structure that has a plug-n-play mode adaptation layer in it. This will enhance acceptance and deployment of Internet of Things devices in smart homes hence making the people living in the house more comfortable. Devices and Systems with high interoperability have lower instrumentation costs and lower operational costs, higher productivity, greater conversion of data and greater competition between equipment vendors. It leads to more innovation of technology as well as applications. Inter-operable systems grow faster, utilize resources with greater efficiency and create value for their customers. Such systems systematically demonstrate that interoperability and standards enhance consumers' choices, because those requirements create a model within which competitors or vendors can innovate provided

the finished products perform the required functions and exchange data with other affiliated products.

1.5.1 Contribution to Theory and Practice

This study contributes to knowledge by providing an in-depth understanding of interoperability as a critical challenge in the Internet of Things (IoT) domain and by proposing a hybrid model that integrates both standards-based and voluntary approaches. In practice, the findings offer multiple benefits: for users, it will stimulate lower prices, wider device choices, seamless integration of new services, improved security management, and enhanced comfort. For vendors, it will stimulate faster market growth, increased competition, innovation, and value creation for customers; and for the wider economy, it will contribute to GDP growth through the expansion of a competitive smart home market.

1.6 Scope of the Study

The study focused on the smart home environments in Kenya since the researcher resides in the country. It is believed that smart home prevalence is still low and hence provide a gap that can be identified and open a way of understanding the underlying issues in its implementation. It covers the specific areas of Smart metering, Facility management services, Personal appliances and the entire Intelligence architecture of the smart home. The specific sites were identified within Kenya's capital city of Nairobi between January 2021 and December 2021.

The scope appreciates the fact that vendors of smart home devices in the country specialize in deployment of the services biased to their focus of business while ignoring

any other areas which may need to be integrated to their device of concern, for example, vendors who deal with security solutions deployments and smart devices related to physical security do not bother with facility management devices or personal appliances.

1.7 Assumptions

Assumptions are things that are generally accepted as true by researchers in a study. This study therefore made several assumptions throughout the process which include: - The respondents understood the questions posed to them and hence gave a true reflection of their perception and that they were truthful and honest. Another assumption is that the sites visited is a reflection of any other sites within the country.

It was also assumed that security is inherent or embedded in technology deployed in the devices as well as the infrastructure upon which the devices operate. Where security here includes but not limited to authentication of devices, encryption of messages, secure communication, authorization, confidentiality and integrity of devices within the network.

1.8 Limitations of the Study

Limitations in a study defines the potential weaknesses of the investigation that are mostly out of the researcher's control, this is supported by limited funding, the selection of a research design, any mathematical model constraints, or any other factors [10].

Another limitation was identified as the change in technology associated with smart homes. The pace at which the Internet of things technology and by extension smart home technology is changing is so fast to a point that users tend to be locked in a technology that cannot be upgraded or integrated horizontally.

Another aspect identified a limitation was on the funding of the research. Since the researcher did not manage to secure a research grant, the research was however funded by the research from personal savings.

1.9 Organization of the Thesis

This thesis is subdivided into six chapters, which are briefly explained in the following paragraphs.

The first chapter introduces the thesis, gives a background information about smart homes and Internet of things technology, it identifies the problem and the corresponding research questions, and this is followed by the scope of the study, the significance of the study and the limitations.

The second chapter investigates previous studies done in order to make a basis for the research. It covers interoperability in smart homes as a technology, models of interoperability, IoT applications, architectures, and the future of Internet of Things. It also identifies the strengths and weaknesses of models developed previously. An example of a post-covid 19 smart home is given towards the end of this chapter. The third chapter explains the research methodology adopted. It looks at the research design, experimental design, data collection instruments, quality control, responses, reliability, data analysis, its presentation and ethical considerations.

The fourth chapter addresses the results. It looks at how data analysis was done, software used, and the approach taken in addressing the research questions.

The fifth chapter derives how a model was developed and the algorithms proposed as well as device Modelling and further gives a sample of a model that was done during the

investigation.

The Sixth presents a discussion on the results and validates the model, makes conclusion of the study, states some recommendations and proposes future work, which can be done that is related to smart homes and Internet of things technology.

CHAPTER TWO: LITERATURE REVIEW

2.0 CHAPTER OVERVIEW

The following section investigates research work which has been done before in order to make a basis for the research. It covers a review of the objectives of the study in areas of internet of things, the role of interoperability in smart homes, models of interoperability, Internet of Things applications, Internet of Things architectures, and the future of Internet of Things.

2.1 KEY CONCEPTS

The following section investigates research work which has been done before in order to make a basis for the research. It covers a review of the internet of things, the role of interoperability in smart homes, models of interoperability, Internet of Things applications, Internet of Things architectures, and the future of Internet of Things.

Internet of Things (IoT) was first developed by Kevin Ashton in 1999 in the linguistic environment of supply chain management [7]. IoT has been defined as a global network of interconnected devices which are distinctively addressable, developed based on standard network communication protocols which are implemented either in a wired or wireless environment. Its meaning was then expanded to cover a wide range of applications such as healthcare, transport and utilities [2]. IoT devices should be able to sense actions from the environment and react independently to the events. The events influence processes which are underway, trigger actions and make up services with or without physical human participation. This implies a network of a huge number of heterogeneous devices are involved in smart environments.

A smart environment utilizes information and communications technologies (ICT) to

implement infrastructure elements and services of an administration, healthcare, education, real estate, utilities, public safety and transportation more interactive, aware and efficient [12].

Smart environments defines Interconnection of actuating and sensing devices which provide the capacity to distribute information through an integrated framework across platforms, which develops a shared picture and hence facilitate development of innovative applications [7].

The idea of IoT has been motivated by the increasing number of devices which are supported by open standards in wireless technology such as Bluetooth, Global System for Mobile communication (GSM), radio frequency identification (RFID), Wi-Fi, data services as well as embedded sensor and actuator connections, IoT is expected to be a transformative technology that will shift to an integrated internet from the current static Internet. It is projected that the next revolution will be that of smart environment where objects will be connected to make it up. It is in the year 2011 when the number of interconnected devices in the world surpassed that of the human population.

A comparable number of devices which were connected by 2020 are estimated to reach at least 24 billion devices [13]. The core motivation behind this growth is the devices that we use daily becoming interconnected entities across the entire sphere. The world where things are interconnected - where there will be humans interacting with machines and machines communicating with other machines (M2M) is expected to exponentially increase and is believed to be the new normal in the very near future.

Internet of Things and other related technologies like cloud computing, technology convergence, big data and the growth of sensor networks are bringing a technological

revolution resulting in: First, an increased monitoring and measurement of machines, human beings and things, secondly, a transition from human-to-human communications to machine-to-Machine interactions then something-to-everything communications, and eventually everything-to-everything interactions. Thirdly, a rapid awareness of the environment and a more regular status and function update from the same environment [13]. This confirms the argument that Machine-to-Machine (M2M) communication can be seen as a subset of IoT. The IoT is therefore a more of an all-inclusive phenomenon, which combines Machine-to-Human communication (M2H), Radio Frequency Identification (RFID), Location-Based Services (LBS), Augmented Reality (AR), Lab-on-a-Chip (LOC) sensors, robotics and vehicle telematics.

For greater impact to be felt as a result of IoT, the need to have greater data network deployment, legal and regulatory models, enhanced standards, device interoperability, physical and logical security, and privacy needs have to be exhaustively researched on and addressed evenly [14]. In order for interoperability to be achieved, the recommended approach is to support interoperability among heterogeneous devices so that the programmer can focus on the development of applications.

If devices are not able to interoperate among themselves, the management of smart homes will become more complex, more costly in terms of interconnectivity at the upper layers such as at the internet level. This calls for a comprehensive approach to enable interoperability within the smart home with a consideration of confidentiality, availability and Integrity of applications in Internet of Things.

2.1.1 Smart Homes

The smart home is quite a promising venture for its residents it provides convenience, energy efficiency and control and an improved quality of life, which is accompanied by a greater cost-effectiveness. The figure 2.1 below as developed by the author shows components of an ideal smart home.

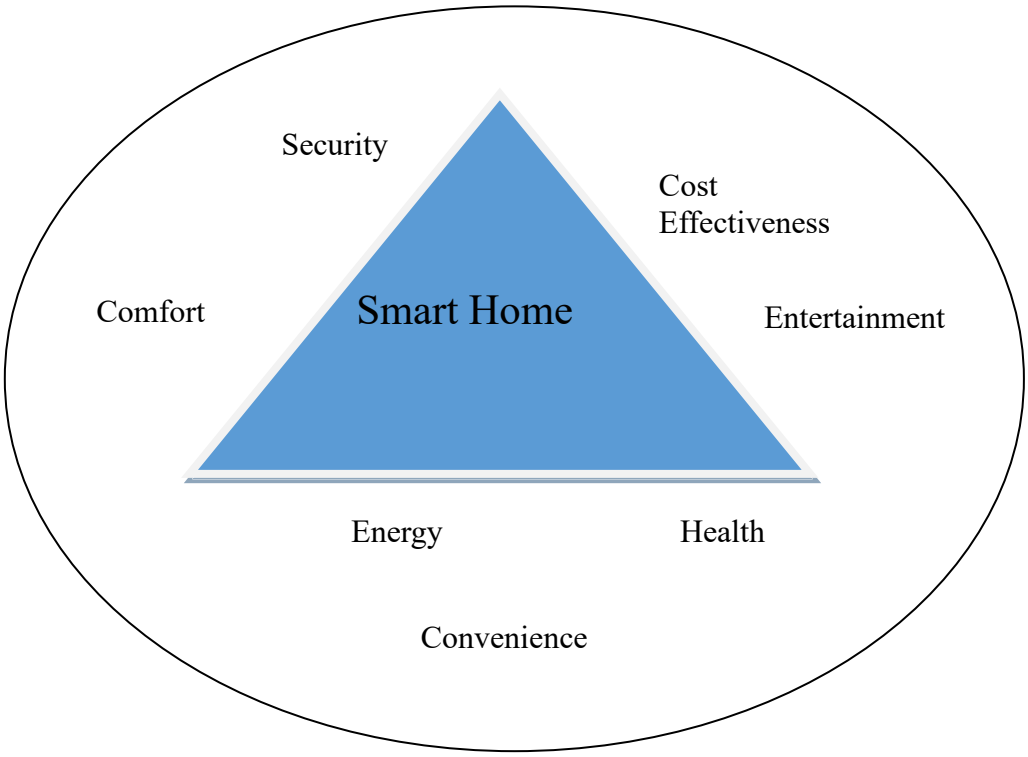


Figure 2.1: Ideal Smart Home

The conventional points used by vendors to win customers for smart home technologies are coined around security in homes, increasing energy efficiency, improved convenience, improved life style and automated entertainment. Issues of health play a role especially for the aging population with technical solutions inherent, which can evaluate the health status of the residents and propose appropriate health strategies and support them within a familiar environment at their homes hence can achieve the objective of living independently longer.

Smart homes incorporate e-walls which provide services to the elderly or those suffering from physical disability and want to live independently. The e-walls could be designed such that they would accommodate primary and secondary users. Primary users would include: - the Elderly with age related impairments, the chronic pulmonary ailment patients and the elderly who may be suffering from minor dementia. Other additional user groups comprise of friends, relatives, visiting hospital nurses and caregivers [15].

2.1.2 Functional Principles in a Smart Home

The two major components in a Smart home are Sensors and actuators. The sensors measure relevant conditions within or around the home and actuators execute actions based on the message from the sensor on the collected data. The intelligence or the ability of devices to be smart are based on the connection between sensors and actuators which are composed of if-then rules. This means that devices will act by themselves when the conditions are true. For example:

If <its dark> turn_on_security_Lights.

If <it gets dark> close_the_blinds.

If <window sensor detects opening movement> Turn_on_intrusion_alarm,

With these conditions, more complex scenarios which are routine in nature can be fully automated. These connectors can also be implemented to support some IoT device communication protocols.

A smart home is generally said to possess the following elementary characteristics: It is interleaved with sensors hence it is able to collect data from the environment and on inhabitants' lifestyles and sensitive associated characteristics. A smart home is also said to be interconnected, this enables the design of related events for different components in

the home for instance the relationship between turning on the lights when the curtains are closed. The smart system accumulates user data, learns and adapts to how elements are triggered in the home. In the long run, the smart home is expected to 'learn' and 'make autonomous decisions' regarding the devices in the home. A smart home is also controlled easily by users even remotely and including by a voice interface [16].

2.1.3 Users and Smart Homes

Smart homes are still largely focused on technical feasibility and automation, this is still heavily controlled by technology. It is therefore a concern that the ultimate consumer of the technology is still reluctant especially in developing countries to accept it. The user experience generated by the technical solutions are often neglected.

The major reason why users are still reluctant would include:- Market complexity where the smart home market is huge and hard to comprehend. Customers are often confused about which devices and components meet their requirements and possibility of how to combine them and expansion in future [17].

The other issue lies on complicated installation whereby many smart home components are available in shops. However, without sufficient installation and configuration support they are bound to fail in achieving the objectives.

There is also unsatisfactory usability. Smart home systems are not very user-friendly. They do not cover all needs of the users in a dynamic environment some data on past events may not be available or if they are there, then the format in which they are is not user-friendly. Integration of new components in the future is also unpredictable due to dynamic device designs, services and software, which are heterogeneous and may not be compatible.

The final issue is on the myth of routine. Smart homes assume that homes can be fully automated based on the assumption that residents follow certain routines in their daily lives. This is however not true because living in a home is stochastic. The aspect of several people living in the same home further complicates the myth of routine, different days of the week have different schedules and moreover, routines are influenced by the environment and that changes over time.

2.1.4 Security in a Smart Home

There is an increased utilization of IOT devices and hence an expansion of security threats too. The threats come in a wide range such as privacy intrusion, denial of service and breach of safety. The compromised devices in the smart environment ecosystem can be used as an avenue for committing a range of crimes. IoT security is considered unique because of the integral heterogeneity in services, systems, and hardware devices in IoT. The existence of dissimilar communication protocols and media further complicate the development of innovative IoT security structures. There are also existing security structures which are implemented mobile devices like smartphones which cannot be embraced by IoT systems due to the limitations in sensors, networks, and individual devices [18].

Smart homes are equipped with devices that provide the residents with all-inclusive information concerning their homes all the time and accepts them to carry out some controls remotely. This fact is the greatest contributor to the threats inherent with this technology in use [19].

The table 2.1 below summarizes threats in a smart home.

Table 2.1: Summary of Threats in a Smart Home.

Threats	**Explanation**
Physical attacks	Smart home devices are physical objects, which can be broken hence prevent functionality, and have a monetary value attached which motivates theft. Physical access to smart home sensors and objects can allow for uploading of software (whether new or malicious), addition of hardware components, resetting of device settings, and sometimes complex like extracting encryption keys. Most device manufacturers assume that it is only the device owner who will have physical access to the device which may not be true always [19].
Information leakage or sharing	Owners or visitors may disclose unnecessary information to the smart home sensors and may share the results through incorrect security paths or settings of the devices [19].
Erroneous use of devices	Smart homes have inbuilt complex systems with devices having different technologies, and varying interoperability challenges among them. The administration of these devices becomes a complex task. Devices that have incorporated

	machine-learning capabilities are also there. Misinterpretation of signals and erroneous use of signals can be easily encountered. Some voice devices for example can have multiple errors due to accents, intonations and different pronunciations of terms [19].
Using information from unexpected source	Some smart home systems that respond to the behaviour of users or the environment could be activated based on unreliable sensor systems. For example if there is a dark cloud over the home, it could activate security lights during the day adding unnecessary electricity bills. Compromised devices can also activate unexpected actuators [19].
Accidental change of data in devices	Accidental changes in signal source data can cause failure or cascaded errors within systems hence improper functioning of smart home systems [19].
Weak home designs	Some designs have weak security and privacy problems starting from the architectural part of the home. This can occur from the smart home modules and services, up to the whole installation and integration. For example, erroneously set up certificates for Secure

	Sockets Layer (SSL) implies that information is transferred without encryption. Vendors with inadequate experience of security design may develop weak components, as they integrate with existing products. Optionally the security features may be limited so as to keep devices reasonably priced during upgrades [19].
Natural disasters	Since smart home devices are incorporated into the home infrastructure, anything affecting the structure will affect the functioning of the smart home. Some devices are large and difficult to move incase of natural calamities like floods when responding to disaster. Other threats in this category include: fire, air pollution, strong wind, corrosion, lightning, excess water, heavy machinery movements and harsh climate will considerably affect smart home functionality [20]
Digital rights conflicts	Inappropriately applied Digital rights conflicts management policies might have a consequence of blocked legitimate media content. Digital rights conflict policies may limit some anticipated functions.
Loss of integrity	Smart homes collect and keep large amount of

	data which some of it is sensitive. This increases the attack surface and the opportunity for information leakage or data being altered. This is intensified by weak security design, implementation of plain text communication channels and lack of classification of collected information [20].
Destruction of storage media	There is often high probability that the storage of smart home data is within the smart home. Some smart home devices are exposed to loss or destruction due to their nature being either mobile or located in a place prone to physical loss [20].
Leakage of Information	The smart home offers substantial avenues for surveillance, social engineering and other potential intrusions into user privacy. This serves as an avenue of information being found in the wrong hands [20].
Outages	Smart homes rely on a variety of resources to provide functionality. Input failures can have wrong interpretation of signals in the smart home. Outages could range from loss of electricity, internet connectivity, loss of support services or Media access unavailability. Any

	slight outage could result in a major disruption or destabilization of the systems. Recovery once an outage occurs can be complex or need a physical device resetting or rebooting, of which sometimes the user is remote [20].
Interception	The huge number of sensors and devices keep information of how people behave or carry out routine functions. This can lead to derived actions such as regular practices, consumption preferences, absence or presence within the premises and any other detailed preferences. Authorities, marketing companies or criminals could target this information either legally or illegally. Some information could be directly where attackers target and receive signals from video-over-IP cameras [11].
Interfering radiation	Using different wireless communication protocols from different vendors may possibly interfere with each other, or contest for bandwidth. This degrades performance and causes unavailability of services [11].

The summary in the table above portrays Smart homes as having a unique requirement in ensuring data confidentiality and integrity implemented through technological controls

such as encryption, hash functions and digital signatures inherent in hardware deployment and data management [12].

The security in a smart home also logically recommends that a panic button is recommended to be fixed next to where the main resident sleeps such that when activated (pressed), all lights come on and an automatic alert call can be made to an emergency contact. The smart home should also communicate only when a certain threshold is reached. Alarm System siren is activated when the sensor is triggered. It causes the siren alert throughout the house hence deter the intruder [11].

The smart home can replay the activities in your home if in case you were away as though someone is within the home.

The smart home can also allow for combined sensors for example, motion detectors to be able to raise alarms automatically.

Automatic arming of the alarm is such that it is activated as soon as you leave the house.

The overall concept of securing smart homes requires that the application of fundamental information security principles would significantly increase the whole security in the smart home [13].

2.1.5 Energy optimization

For energy consumption is such that it can prioritize tasks, those which are critical are run using the grid source while those that can wait for free power from the solar circuit can wait. This will contribute to cost effectiveness in the long run to the users.

The smart energy intelligence can supply data to the users such that they will advise on which ones are power hungry and potential points of energy savings. All power-hungry standby units can also be identified and can be switched off all at once hence reduce cost

of power [11].

Smart homes utilize solar power hence bring the house to comfortable temperature. If integrated with smart heating, it will keep the rooms at desired temperature cost effectively.

Irrespective of the physical location of the user, the entire lighting circuit can be switched off in the whole home.

2.1.6 Luxury and lifestyle

The smart home has the ability to adjust lights for every occasion. Lights for watching a movie would differ from that of dinner or a party hence change the atmosphere in a home. These lights can be set up and adjusted at wish by the users.

The smart home is able to adjust blinds based on the position of the sun in the sky and time. For example, the blinds would open gently in the morning as it wakes you up and close in the evening as the sun sets or as it becomes dark [14].

The ability to control your home while away is key in making you more comfortable. An application installed in your mobile phone can allow you to control activities in your home all the time.

The smart home can allow for different music to be played in every room depending on the wish of the user. Different radio stations can also be tuned in depending on the time and the room as well as favorite programs. This makes life more luxurious and enjoyable.

Smart homes can allow for integration of various tasks into one switch. For example, closing the blinds, switching on the television and dim the lights to be done in one click or switch. This simplifies routine jobs and allows the users to be more relaxed.

The smart home can allow you to answer to a nock in the door from anywhere and allow

your visitors in without necessarily having to go there. This simplifies tasks and relieves users of the energy and time to do the task [14].

2.1.7 Issues Surrounding IoT

There are quite a number of issues surrounding IoT in terms of the requirements for it to succeed which may be seen as challenges as well as opportunities which include but not limited to:- First, more widespread interconnection IoT which extends from information devices to the interconnection of all devices whether intelligent or not [12]. The challenge will be how to secure the devices physically both logically and physically.

Secondly, the aspect of sensing information from every sensor may include uncertainties. Since multi-sensor networks act together to achieve the global environment awareness, there will be issues such as: - Non-uniformity of data formats, Inconsistency of information due to the misrepresentation or alteration of space-time mapping and a variety of information errors. The errors may be as a result of inconsistent sampling or the difference in sensor capabilities. The sensors may therefor experience discontinuities from intermittent signal availability especially when the network has a dynamic transmission capacity.

Third is the wide range of Intelligent Services available. The services are often based on widespread interconnection of physical devices and the rigorous perception of the physical domain. IoT has the capability to provide an all-inclusive intelligent service platform where objects are involved in the service processing actively [18].

There are quite a number of challenges facing IoT projects but two major ones have been identified which is the reliability and security of the connected devices to the solution's backend. It is also evident that IoT devices have varying properties as compared to other

clients such as mobile applications and browsers. IoT devices are frequently embedded systems without human intervention, have capability for remote deployment where physical access may be costly. These devices are considered to have limited processing capabilities, power consumption and retention because of their size. They also have limited bandwidth and intermittent network connectivity is often experienced. They also need to use varying protocols which may be proprietary, customized, or from an industry-specific dimension, and they can be developed using a varying set of hardware and software platforms[18]. Many IoT applications must be able to deliver scalable, secure and reliable results hence the connectivity requirements are a challenge as it is time-consuming to implement if conventional technologies such as web containers and messaging middleware is used.

2.1.8 Uptake of IoT

For a fast uptake of IoT, there are a few key issues which must be addressed such as identification of objects, security and semantic interoperation among devices [18]. The interaction with big data, cloud technologies and networks of the future has to be addressed by everyone.

Open standards are touted to be a major motivation for IoT uptake. The integrated IoT environments will assist the competitiveness of this technology and make people's life easier. This will lead to improved services to humanity, immense savings on the economy and a smarter utilization of resources [12].

2.1.9 IOT Implementations

IoT implementation can be carried out in three dimensions: - That which addresses middleware referred to as internet-oriented dimension, that which addresses the sensor-actuator implementation called things-oriented dimension and semantic-oriented dimension which addresses knowledge within devices **[**19**]**.

During implementation, there will be challenges such as pervasiveness of devices, general management of devices, heterogeneity and scalability of devices, distributed knowledge bases, security and trust for both information and the communicating devices. This will include the deployment of cryptographic algorithms which have dynamic capabilities and protocols that will provide all required security features. Security here becomes a challenge too to implement.

2.1.10 IoT Applications

The architecture of IoT makes it possible to develop a huge number of applications [20]. A very small part of IOT applications are implemented in our society. There are many domains in which IOT applications have the prospects to improve the quality lives. The many application areas can be roughly grouped into the following four domains: Transportation and logistics environment, Health and related environment, Personal environment and smart environment.

2.1.11 The Future of IoT and Device Interoperation

The Internet will have to follow a methodology where the complexity of the Internet Protocol stack is reduced to a point where it can handle ‘‘IP addressing over anything’’. This is seen as one of the best approaches to transform to Internet of things from the current Internet of devices. The future of IoT shall heavily operate on agents which will

center on sensing, actuation, messaging and control which will become more advanced and omnipresent, there will be an intersection in the research areas of IoT and sometimes may come with a slight difference in the approach hence a more cooperation is encouraged between these research communities. Individuals will continuously depend on the devices such as planes, trains, and cars, devices to manage healthcare and civil infrastructure that will need more intelligence as they continue to inter-operate. It is therefore not difficult to imagine how attacks on the control environments of these devices can cause fatalities [19].

The Internet of Things seems to continue in upholding a crucial orientation in the perspective of Information and Communication Technologies and the improvement of humanity. Whereas concepts and basic building blocks have been elaborated and reached maturity, there is need for further efforts in unleashing the full potential on devices and making them friendlier to users with a view to make the users more comfortable.

2.2. Related Studies

2.2.1 Models for Interoperability in a Smart Home.

The models adopted in smart homes for interoperability is perceived from several angles. A few ways of looking at it is device interoperability, semantic, network, syntactic, and platform interoperability [21]. Since IoT is composed of an assortment of devices called ‘smart devices/things’ which could be high-end devices (having sufficient resources and computational capability) or low-end devices. Low-end devices here implies they are resource-constrained in their processing power, energy consumption and communication capacities.

Devices can be connected either directly or indirectly by means of a gateway, the two may implement edge intelligence with diverse levels of processing capabilities.

For network interoperability a cloud gateway is used to provide endpoints for device connectivity and enables bidirectional exchange of messages with the backend platform. The backend encompasses various components which provide device registration and detection, data collection and analysis to correctly deduce meaning [19].

Network level interoperability allows for seamless message exchange for end-to-end communication in a grid irrespective of the platform used. To enable systems to work together in a network, each device should be capable to communicate with other systems through a heterogeneous network. The network interoperability should be able to handle issues such as addressing, Quality of Service, resource optimization, security, and provision for mobility [22].

2.2.2 Connectivity interoperability

The model approaches interoperability from a connectivity and communication point of view. The independent devices interconnect through Wireless home automation networks (WHANs) which are often adopted in smart homes. The proposal is to use z-wave protocol for connectivity in the hope that interoperability issues in smart homes will be solved. The Z-wave protocol uses a master and slave model and it subdivides the architecture into four layers, which are: - Application, Routing, Media Access Control, and the transfer this approach works well with door locks and light switches used in the smart homes [23].

2.2.3 Network Interoperability

This architecture for smart homes proposed interoperability established on Radio Network Systems (RNS) services by implementing IOT identifiers to satisfy the need for heterogeneity. A mechanism for using IoT DNS (Device Name System) is adopted so that it uses device Identification code to infer and interpret the communication in heterogeneous platforms [24].

A recourse name service (RNS) architecture for smart home suggested in [25] where use of unique IOT identifiers to cater for the heterogeneity is adopted in a network design. This was proposed so as to help in vertical integration, however issues of security, comfort and energy consumption challenges were noted.

The use of Zigbee to interconnect home appliances and JSON for data exchange was proposed by Moataz [26]. There was an achievement on data exchange between home occupiers and devices mainly to stop or start the appliances such as washing machines, refrigerators and Air conditioner.

Another proposal to use a Machine 2 Machine translator (M2M) is suggested by [27]. M2M requires an Object Identifier (OID) so as to recognize the structure and data stored in the object then the M2M translator which will reformat it so that it can be used in a heterogeneous platform.

The proposal to use Wireless Sensor Networks (WSN) with Ambient Assisted Living (AAL) is advocated by [28], so that home owners or residents can control the power using wireless devices. They proposed implementation of IPv6 protocol which allows

them to the easily configure and monitor the devices. IPv6 works best with WSN since it is low voltage and makes the model acceptable to more devices.

Universal Plug and Play (UPnP) architecture is proposed by Toschi et al [29] where the home appliances can be supervised remotely using laptops or mobile devices. The proposal is to use protocols, which allow multi-tasking and can manage multiple appliances concurrently. The use of TCP/IP protocol, Internet Protocol (IP), Transmission Control Protocol (TCP), General Event Notification Architecture (GENA), Hyper Text Transport Protocol (HTTP), Simple Object Access Protocol (SOAP), Extensible Markup Language (XML) and User Datagram Protocol (UDP) is adopted so that it can update and install drivers automatically [29].

2.2.4 Syntactic interoperability

Syntactic interoperability is the interoperation of the data structure and format of messages used in the exchange of services or information among heterogeneous devices. First, it begins by the definition of an interface for all resources, this will adopt a structure in line with a given schema. Web Services Description Language (WSDL) which is the standard format to describe a web service and Representational State Transfer (REST) which is a web access service that seeks to provide a simple method of accessing Web services are examples of syntactic interoperable services. The sender needs to use syntactic rules to encode data in a message; these rules are defined using a particular grammar. On the other end, the receiver decodes the received message based on syntactic rules developed using the same or some other version of grammar. The Syntactic interoperability problem will arise when the receiver a used different or incompatible

decoding syntax from that of the sender's encoding rules which leads to a mismatch in the message parse trees [30].

There is also a proposed intelligent interoperability framework [31] intended for use in smart homes which is developed on Simple Object Access Protocol (SOAP) which offers devices interoperation. The proposed design did the integration through a middleware for data broadcasting. The use of an API would help in management of devices particularly the use of graphics and window APIs. The proposal is able to update its functionality whenever there is a new update on the prevailing middleware specification.

2.2.5 Semantic interoperability

Semantic interoperability is defined as the ability to permit different agents, applications and services to interchange raw data, information or knowledge in a meaningful technique whether on and off the network. The semantic IoT addresses heterogeneity by exposing devices, data and related data through an Applications Programming Interface (API). The approach has been limited by the need of corresponding parties' need to share the knowledge of an API of which many devices do not communicate in an identical language and cannot exchange in a heterogeneous gateway. The data schemas and models used by two sources may be different and not at all times compatible. The data could also be represented in dissimilar units of dimensions [21].

2.2.6 Platform Interoperability

Platform interoperability is approached from the fact that there are different operating systems available for use, different programming languages, diverse data structures in use, different architectures and mechanisms for access when dealing with things and data.

There are various Operating Systems each coming with several versions developed for use in IoT devices. Such operating systems include: - Contiki, TinyOS, OpenWSN and RIOT. The heterogeneity of the platforms causes difficulty for developers to code for hetero-domain or cross-platform IoT applications [21].

2.2.7 Strengths and Weaknesses of Existing Models

The network interoperability concept has a strength in that it establishes a secure communication network between the server and the client with the help of session protocols. It is capable of resolving the failure problem which comes up due to unwanted data by clearing it. However, for developing countries, the reliable infrastructure to connect to the cloud is still limited. The aspect of network interoperability may not allow integration of newer devices to be introduced into existing IoT platform. There is a difficulty in implementing de-facto standards used in communication therefore not all smart devices implement all the communication technologies in use[19].

Challenge to the Connectivity interoperability model is adoption of mobile cells based connectivity has high chances of network failures in developing countries hence problems where a failure to receive sensor information from one device to the other is imminent and in most cases inevitable [22].

Challenges to network interoperability is that the framework for interoperability will assist in vertical solutions in multifunctional applications which will cover area of smart home security, comfort and energy hence a limited proposal hence the need to have a horizontal approach of interoperability too.

In some circumstances, the objects that desire to exchange information may be using dissimilar technologies when communicating which allows them to co-exist in the IoT

ecosystem. Devices are in a close range hence no need to move data to the cloud devices should just communicate with each other. The models also address data analytics which is not critical to end users in a home environment as their needs are different. The developers or vendors attempt to address the IoT interoperability challenge through introduction of standards but the industry is continuously changing with newer devices and changing user needs[20].

2.3 Review of Objectives

2.3.1 State of Device Interoperability in Smart Homes

The state of interoperability in smart homes is best summarized by the table 2.2 below where protocols and techniques are compared from the year 2008 to 2018. The network they support, the type of interoperability and applications supported. A summary is given in the table 2.2 below.

Table 2.2 A summary of the State of Interoperability

Protocol/ Technique	**Network**	**Type of interoperability**	**Application**	**Year**
OSGi, MA	SOA	BASIC	Mobiles	2007
SOAP				2008
SOAP, XML	WAN	NETWORK	Frameworks	2008
Zigbee, RF	HAN	SYNTHETIC	AC, Lights	2010
SOAP	LAN	SYNTACTIC	CCTV	2011
UPnP	Printer HP5xxx			2011
OHNet	Smart Home,			2011

	Smart Grid			
Zigbee, UPnP	Home Network			2011
OSGi, API		SYNTHETIC	Laptops	2012
CoAP, Propriety FS20	INTERNET	SYNTACTIC		2012
WOT	LAN	SYNTACTIC	TV, DVD	2013
JSON, Zigbee	HAN	BASIC	Air Conditioner, Washing Machines	2013
RNS	LAN	Network	iTopHome, IGRS,	2014
OpenWebNet	LAN/ WIFI	Network	Actuator, Switch,	2014
IPv6	WAN	NETWORK	Machines	2014
HEPA, REST	WIFI	SYNTHETIC	Plugs	2015
Z Wave	HAN	BASIC	Lights, Switches. Door Lock	2016
RF,Zigbee, ERDF,Bluetooth	LAN/ WIFI	BASIC	Lights, Bulb	2016
IPv6	WSN	NETWORK	Owen	2016
TCP/IP, UDP, HTTP,SOAP	HAN	NETWORK	Remotes, Laptops	2016
IPE,Z wave, M2M	LAN	SYNTHETIC	Cells	2016
IOT DNS	Internet WIFI	Network	Home Appliances	2017
RFD	WAN	SYNTHETIC	Computer Records	2017
M2M, OID	WAN	NETWORK	Device	2017

			Identification	

The various protocols [23] above designed include Z-Wave which uses a wireless radio frequency technology that permits smart devices to connect to each another. The Zigbee and Z-Wave standards have a similar nature in their applications and performance. Both run on mesh networks and specify very low-power networks. The implementation of mesh technology makes both standards desired for use in smart homes. They support widely distributed devices and the standards' low-bandwidth communications prevents attenuation hence making the technology more reliable. The low-bandwidth performance is ideal for simple devices that need only data connections for binary controls which have ON/OFF function as a feature.

RNS is a Radio Network System that works by transmitting and receiving electromagnetic waves. OpenWebNet is the protocol that enables remote communication with home automation systems remotely. Web of Things (WoT) is a network protocol intended to allow interoperability through all IoT application and platforms. It is intended to complement existing IoT standards and extend expected solutions.

IOT DNS is a naming and service or device identification method used over the internet, which intends to make IoT global. SOAP is Simple Object Access Protocol, which is an XML, based Messaging Protocol layer that has the ability to route messages through nodes which perform different functions. SOAP hence supports capabilities like addressing, security and format-independence.

Constrained Application Protocol (CoAP) is a specialized Internet Application Protocol used by constrained devices. COAP is a client-server IoT protocol that adopts UDP as the

underlying network protocol, which applies HTTP when doing request and replies to the server.

Universal Plug and Play (UPnP) is a protocol that permits networked or smart devices to automatically discover each other's presence on the network and establish services which are operational.

Open Home Network (ohNet) is a library that is generally used for the discovery, monitoring, manipulation and implementation of UPnP devices it can extend to similar protocols[23].

JSON is JavaScript Object Notation, this is a minimal format for structuring independent data. It is an ubiquitous transport protocol with a format for sending data between mobile applications and web servers through browsers.

A Reduced-Function Device (RFD) are devices, which do not allow association of devices in a branch. They are used to interconnect to a cluster-tree network as a leaf device as the branch terminates.

M2M is an open industry communication protocol built to enable both wireless and wired systems to remotely perform services and management for internet of things embedded devices and appliances. It is used to automate data transmission between electronic devices.

Object Identifier (OID) implies an address used to uniquely name and point to an object or managed device and its status.

Representational State Transfer (REST) is a large-scale networked software that takes rides on protocols of the World Wide Web. REST a client-server protocol that allows

clients to interact servers without having any preceding knowledge of the server or its contents.

Z-Wave is a low-power communication protocol running on wireless platforms which provide end users with a reliable method to remotely control devices and systems specifically in a smart home applications.

The Open Services Gateway Initiative (OSGi) is a Dynamic Module System for Java which defines an architecture for development of modules in applications.

Extensible Markup Language (XML) is where information is created, formatted and shared in a structured format through the Internet.

Home Area Network (HAN) is a network in a home where all devices and smart appliances are interconnected.

Wireless Sensor Network (WSN) is a wireless network deployed in an ad-hoc manner with a large number of wireless sensors. It is usually used to monitor the system, physical or environmental conditions.

Service-Oriented Architecture (SOA) is a model that uses Web services to enhance the capabilities of networks. Events originating from diverse network devices are linked seamlessly.

This section presents state of interoperability among heterogeneous devices in IoT particularly in smart homes. With the increasing number of heterogeneous devices, connectivity among devices is expected to be a critical component [22]. The section summarized the state of interoperability by the communication protocols or techniques used, network type, type of interoperability and the years when the work was presented.

2.3.2 Role of interoperability in smart homes

Technological fragmentation is a major problem in the adoption of smart home technologies, which implies each device in a system is controlled independently. This fragmentation does negatively influence the user experience and hence introduce an adoption barrier [32] Interoperability therefore brings a unification factor to all these diverse vendors hence communicate and work together.

Interoperability assists to reduce complexity in the smart home hence promote a common understanding among devices.

Open hardware platform for smart homes offer a high degree of interoperability this means that they can develop a solution custom-made to the specific needs of the customer.

Resource holders also gain the ability to better utilize their own information internally, and become visible to users [32].

2.3.3.1 Facilitators of interoperability of devices in smart homes

There are many enabling technologies for IoT to be achieved as follows:- The Big Data: - As more things are interconnected, more data is collected from them in order to execute analytics to ascertain their trends lead to insights and decision making. Big data refers to large data sets that need to be collected, stored, analyzed, queried and or manipulated in order to present a conclusive promise of the IoT.

The increase in device interconnectivity presents three metrics used by IoT vendors or operators to describe the big data they handle which involves volume, velocity and variety of data. Also the Digital Twin: which was introduced in 2003 by John Vickers explains the phenomenon that a digital copy of a physical asset that lives and evolves in a

virtual environment over the lifetime of a physical asset. With a further examination of the digital twin it is possible to reveal the same information in the physical smart object itself [33]. The Cloud Computing : Refers to a model for enabling ubiquitous, accessible, on-demand network rights to a common pool of computing resources that are provisioned and made available with minimum management or service provider mediation. There are the Sensors which are devices embedded in smart objects also which is the central of functionality of the IoT. Such sensors are able to detect events in a specific quantity, communicate the event to the cloud and, in at times receive data back from the cloud or are able to enable communication with other smart objects. The Communications aspect is also included and this is the part of technology which enables sending and receiving data, the wired and wireless data communication technologies have improved such that almost every electronic equipment has ability to support data connectivity. The protocols for allowing IoT sensors to relay data include wireless technologies such as RFID, Bluetooth, Wi-Fi, XBee, ZigBee, Wireless M-Bus, Z-Wave, Bluetooth Low Energy (BLE), SIGFOX and NuelNET, satellite connections and mobile networks using GSM, LTE, GPRS, WiMAX or even 5G,. There are the Analytics Software which are the programs that transform the collected data from smart objects into applicable intelligence. This software utilizes mathematical models, data mining and statistical techniques to give insight to technology users. The outputs from these software include trends and patterns which are extracted from the big data sets in form of portfolio analysis, risk analysis, predictions and optimization recommendations. There are also the EDGE devices which are instruments which provide entry point from the global, public Internet into an Application Service Provider's (ASP). They include routers, switches, multiplexers, integrated access device (IAD), or metropolitan area network (MAN) and wide area

network (WAN) access devices. These devices are becoming smarter as they are being made to be able to process data before it reaches the network's backbone [33].

2.3.4 Metrics for developing device interoperability for smart homes

There is a model proposed by Tolk et al called the Six level structure which approaches interoperation metrics as to cover: No connection which is a basic connectivity and network connectivity of devices. The concept of syntactical metric addresses the data exchange aspect in interoperability, semantic metric which enables understanding in the data or signal, pragmatic. The dynamic metric addresses applicability of the information and the conceptual view which is the shared view of the world [34]. Other researchers have supported the model, which addresses: communication, behavioural, semantic, connection, dynamic, and conceptual [59]. These six levels are equivalent to the IoT taxonomy model as developed by Tolk A. in the figure 2.1 below.

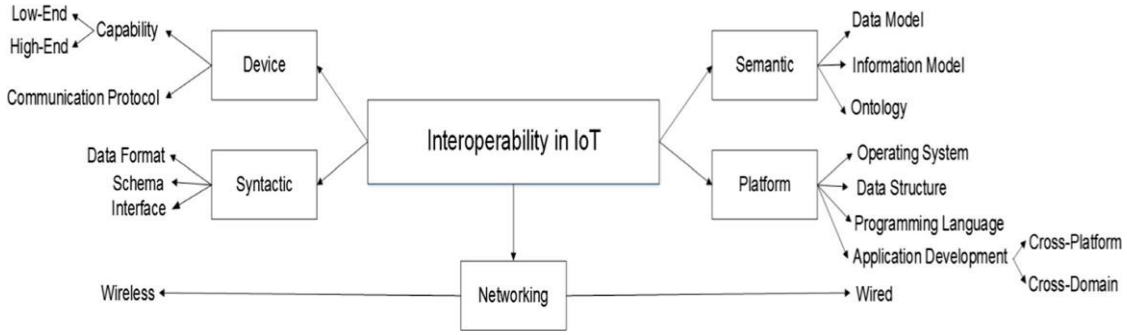


Figure 2.2: IoT Taxonomy Model [59]

The concept of applying an existing model for interoperability is recommended since it will allow a structured and steady approach to interoperability. The Modelling and Simulation field of systems design and development recommend the use of rigorous

engineering methods so as to replace ad-hoc approaches to the development of interoperability [35]. The framework, as described by [21] has both descriptive and prescriptive designs as used in systems engineering. In order to dissect the ability, characteristics, properties and the levels of conceptual interoperability of an existing system or system of systems, levels of interoperability can be seen in the table 2.2 below.

Table 2.2 Levels of Interoperability – Descriptive Model [59]

Level	Layer Name	
6	Conceptual Interoperability	Desired layer of interoperability in IoT
5	Dynamic Interoperability	Desperate interoperability systems
4	Pragmatic Interoperability	
3	Semantic Interoperability	
2	Syntactic Interoperability	
1	Technical Interoperability	
0	No interoperability	Legacy systems

The table 2.2 above according to [35] shows a summary of the various levels of interoperability, which is discussed as, follows:-

Level 6 shows the desired level of interoperability in IoT which is referred to as the Conceptual Interoperability where systems are entirely aware of each other's information processing capabilities, processes, settings, and modelling procedures.

The level 5 implies the Dynamic Interoperability of systems where they are able to re-organize information assembly and intake based on dynamic environments where meaning of information is understood as the context changes.

The level 4 shows the Pragmatic Interoperability where systems are aware of the context, states and processes as well as the meaning of information passed among heterogeneous devices.

The level 3 is the Semantic Interoperability layer where systems are exchanging a set of information and meanings that they can be semantically understood.

The level 2 is the Syntactic level of interoperability where there are some agreed protocols which assist in exchange of information. The right forms of data and in the right order is paramount, however, the implication of the data components is not well-known or defined.

The level 1 is where there is Technical connectivity and that data can be exchanged. The formatting of the data is however not understood, the context is not considered however there is some limited understanding among devices.

The level 0 is the layer where operators and vendors develop their devices without any consideration of the need for interoperability. The manufacturers and vendors here develop devices which work with each other only. This is a common feature in legacy systems.

2.4 IoT architecture

2.4.1 Introduction to IoT architecture

Several scholars have proposed another view of IOT architectures that they can be viewed from applications layer and categorized as: - Service Oriented architecture (SOA) -based architecture and Ubiquitous Service-Discovery Service (ubiSD-S) which are used for IoT-middleware semantic interoperation and Home Audio/Video Interoperability (HAVi) heavily addresses network interoperability.

2.4.1.1 Service Oriented architecture (SOA)

A service-oriented architecture (SOA) is a model of software design where communication protocols provide services to components over a network [36]. The motivation of application services are the independent manufacturers, components and technologies.

The definition of a service here being a discrete unit of functionality that can be accessed from a remote location and acted upon independently.

A Service Oriented architecture can perform any of the following three roles:

Service provider: which is a web service and provides its information to the service registry in the architecture.

The Service broker provides information about the web service to any potential requester and the Service requester or consumer who locates entries in the broker registry and binds them to the service broker to raise one of its web services.

The strengths identified here are that there is a separation of services promotes the idea that services can be delivered faster and more independently. Also, separation encourages good design in so far as the service is designed without knowing who its consumers are.

Then there is the aspect of documentation which is possible for services which need to be reused later.

The notable weaknesses include: - The application services are too constrained because there may be some stateful services which may need both the consumer and the provider to share the same consumer-specific context. This constraint could cut down the overall scalability of the service provider if there is need to retain the shared context for each individual consumer. There is also an aspect that the environments based on SOA include many services which communicate among each other to perform tasks. Since the design may involve multiple services working in conjunction, an Application may generate millions of messages which generates metadata whose management will be an issue. The concepts of SOA also lacks a uniform testing structure. There are no comprehensive known apparatus that provide the required features for testing these services in a service-oriented architecture. The major causes of difficulty are: Heterogeneity and complexity in the network, Huge number of testing combinations due to integration of independent services, Existence of services from different and potentially competing vendors, Platform is dynamic due to development and deployment of new features and services, Physical knowledge of devices, environment which is Time-dependent, High environmental dynamics and Privacy and security of devices, services and data.

2.4.1.2 Ubiquitous Service-Discovery Service

Service discovery is defined as a technique as those that help users to find services, applications and devices that are accessible in the network. This feature is useful for mobile users in foreign networks in wireless network and ubiquitous computing environment [37].

The strengths associated with this service include: - It is able to function on a local area network and wide area networks as well, it administers automatic querying using the services pointer and Preference Search Service and Querying can be done manually or automatically.

The notable weaknesses are:- The increase in number and heterogeneity of devices leads to failure, The model does not address how devices will communicate and are able to understand the different formats of data sent and received and the chances of misinterpretation is considered high.

2.4.1.3 Home Audio/Video Interoperability (HAVi)

The home audio/video interoperability (HAVi) architecture is a group of application programming interfaces (APIs), services, and an on-the-wire protocol specified by an industry initiative. HAVi enables multivendor interoperability between computing devices and consumer electronics devices. It facilitates easier development of distributed applications on home networks. It attempts to balance between consumer demands and vendors by enabling both device interoperability and the updates of patches when introducing new features or refinements.

2.4.1.4 If This, Then That Services (IFTTT)

IFTTT originates from the programming of conditional statements “if this, then that.” This is a software platform that connects apps, devices and services from multiple developers with an objective to prompt one or more automations involving those devices, apps or services.

The automations are achieved through applets which are implemented like macros that

link numerous applications and run programmed tasks. You can turn on or off an applet using IFTTT's through mobile applications (or the mobile application's IFTTT widgets). It is also possible to create own applets or implement deviations from prevailing applications through IFTTT's whose interface is user-friendly and easy to use.

2.4.1.5 Message Queuing Telemetry Transport (MQTT)

Message Queuing Telemetry Transport (MQTT) is an application layer protocol that has been extensively embraced as the preferred protocol suitable for the resource-constrained IoT environment devices. MQTT protocol is well known for its attractive features, such as high scalability, packet interoperable communication, low implementation cost, low power consumption as well as quick and reliable message transfer [1].

The MQTT protocol essentially operates under the principle of the publish/subscribe model. MQTT implements a model where message sender (here referred to as publisher) sends out messages, then receivers subscribe to them. A receiver will only check for messages which it has subscribed to and act. There exists another component which is a message broker that handles the communication between publishers and subscribers. Here the broker filters all inbound messages from publishers and distributes appropriately to subscribers. The broker decouples the publishers and subscribers based on several grounds such as space: where the subscriber and the publisher are ideally not aware of each other's network settings and do not therefore interchange information which are basically IP addresses and or port numbers. Time decoupling is another factor where the subscriber and publisher do not run concurrently. Synchronization decoupling is where both publishers and subscribers can receive or send messages without necessarily interrupting one another [1].

2.4.2 Smart Home Model Approaches

2.4.2.1 Model-Based Approach

The approach generates synthetic data using pre-defined models of activities. They specify how events are ordered, their probability of happening, and the time taken by of each activity.

The model-based approach facilitates the generation of large datasets in the shortest time possible. The tools can provide a Graphical User Interface (GUI) for visualizing activities in three dimension (3D). However, the approach cannot capture complex interactions or unexpected mishaps or accidents that are common in homes. Some tools in this category include: - SIMACT which is a 3D smart home simulator which is open-source and cross-platform developed with Java and uses Java Monkey Engine (JME) as its 3D engine that is designed for human activity recognition [38].

DiaSim is another simulator developed to deal with heterogeneous smart home devices and is developed using Java for applied in pervasive computing systems. It has a scenario editor that allows the researcher to build a virtual environment that can simulate a definite scenarios in a home environment.

The Context-Aware Simulation System (CASS) is a tool that intends to generate information based on context in smart homes. It is also able to test context-awareness applications in a virtual smart home. The CASS tool is able to discover any conflicting rules in a pre-defined scenario in a context and recommend the top-quality positioning of the sensors. CASS however only provides a 2D visualization GUI for the virtual smart home.

The Context-Awareness Simulation Toolkit (CAST) is a simulation tool developed to test

context-awareness applications. It generates context information in a virtual smart home for the researchers. CAST is however not available in the public domain because it was developed with the proprietary technology Adobe Flash [38].

2.4.2.2 Interactive Approach

The interactive approach has the ability to capture more interactions and has a capacity for fine details. This approach heavily relies on having an embodiment that can be controlled by the user either the human participant or the simulated participant. The avatar is able to move and interact with the virtual environment which has actuators and/ or sensors. It is possible for the interactions to be done actively or passively. Passive interactions have the capability to sense physical actions and generate signals. Active interactions involve physical actions such as activities in the home like opening a door or turning the light off or on. The problem with this approach is that it takes long to generate sufficient datasets since all interactions have to be captured in real-time.

There are various simulators which have been used to study this interactive approach. For example Unity3D is an interactive based simulator which presents a virtual space simulation that is able to generate data for classifications problems. This interactivity transforms static models into dynamic simulations, allowing users to explore, manipulate, and learn from virtual environments.

Generally, the model-based approach allows the researcher to generate large datasets in short simulation time but sacrifices the granularity of capturing realistic interactions. However, the interactive approach captures these realistic interactions but sacrifices the short and quick simulation time and therefore, the generated datasets are usually smaller than the ones generated by model-based approach [36].

2.4.3 Theories of Interoperability in IoT

A theory is defined as a system of philosophies or linked ideas, which are intended to expound something based on overall principles independent of the thing or object being explained. Theories provide frameworks for explaining observations since it is a guess or speculation. Theories therefore guide the researchers to finding evidence rather than of reaching objective. Theories are also said to be neutral concerning alternatives among a range of values.

A model is defined as a three-dimensional depiction of a person, thing or a proposed structure on a smaller scale than the original. It is not the real world but a human construct to help in understanding the real world systems.

There are two theories to interoperability when developing IoT ecosystems: The standards-based theory which prescribes the use of predefined standards for vendors and service providers and voluntary theory which defines the concept of interconnecting and integrating heterogeneous systems without using standardized protocols, methods, or approaches. A standards-based path would be ideal, but the diversity of standards makes it impossible for now [40]. Choosing and integrating heterogeneous systems will continue to be the common practice. This implies a Chaos theory, which exists on the initial condition of every event meaning that their future behavior is determined by their primary conditions. In a smart home setup, when an activity is observed on an IoT device, there is an automatic potential sequence of causes that lead to the next action. For each activity at the source, there is a subsequent step associated with a pre-existing model of associated behavior to the final action.

The limitations of this model is on the reliance on self-learning of the device which limits the coverage of this model to experience, which must have been learnt by the device.

There will be need to extensively expose devices to various other data from individuals so as to achieve better performance and accuracy. The model also as it is only relies on the principle of cause-effect relationships that are sequential in nature and does not handle any interrupts or delays.

A case of Modelling a POST-COVID Smart Home Temperature.

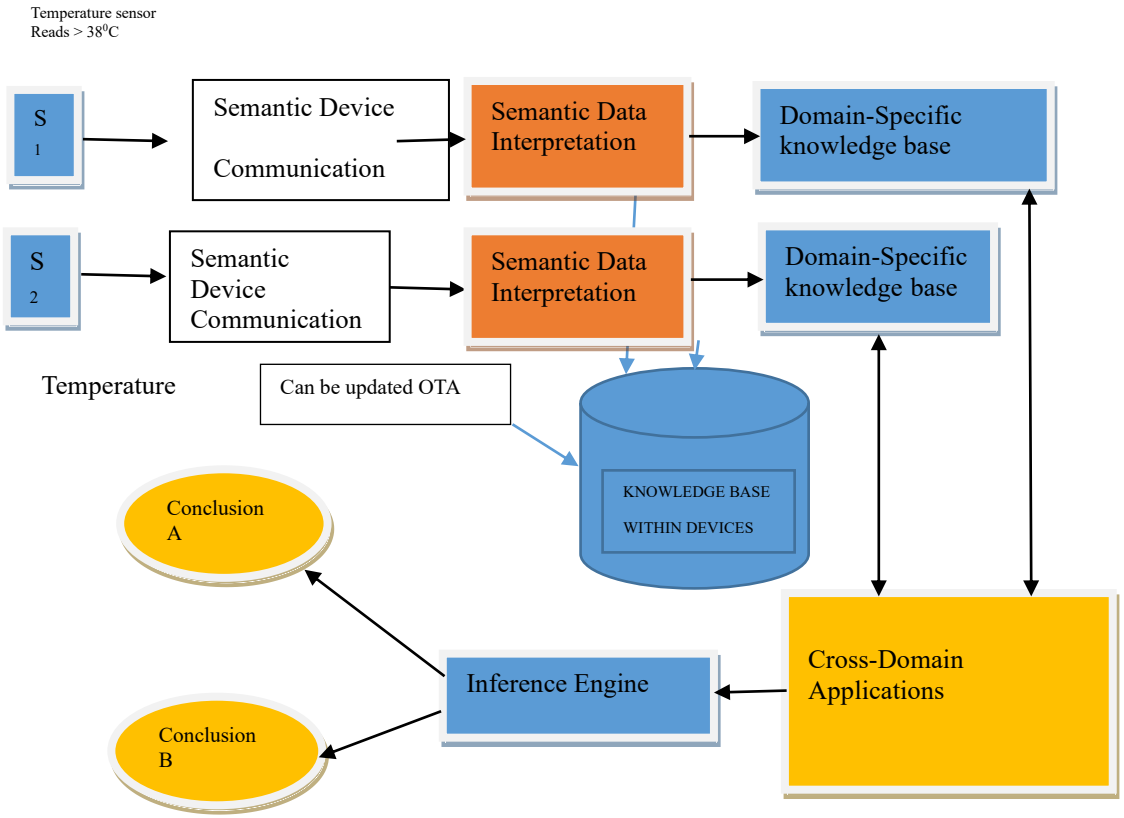


Figure 2.3: Showing A Post-Covid Temperature Sensors in a Home

The model shown in the figure 2.3 above works as follows:-

Sensor S1 from a manufacturer A detects temperature of an occupant of a smart home and reads 38^0C.

The device interprets the reading as either high or acceptable, the meaning is the derived from then domain-specific knowledge base of health, which is able to initiate another application to act and make conclusions of either escalation of the case or initiate other response mechanisms in the home.

Sensor 2 from manufacturer B detects temperature of the environment as of a smart home and reads 38^0C. The device interprets the reading as either hot, acceptable of low; the meaning is derived from the domain-specific knowledge base of environmental temperature such as seasons, which is able to initiate another application of the air

conditioning or house warmers depending on the conclusions.

The over the air (OTA) update can be implemented incase of new COVID 19 constraints which have new features, patches or innovations which need to be updated in the knowledge base.

2.5 Research Gaps

There are many research activities that have been conducted on interoperability and design of IoT devices which include: - Apple HomeKit, Alphabet Net ecosystem and the Ponte design also called If-This-Then-That (IFTTT). They however have some weaknesses such as the assumption that the primary devices support TCP/IP, there is also an assumption that devices are not constrained in terms of infrastructural support. There are projects in interoperability such as the unify-IoT project which is the most far-reaching research on interoperability that seeks to integrate all other facets of IOT from the Business models environment, academic or training platforms, open platforms, value addition and creation, innovation, International co-operation, standardization and research innovation. This research approaches interoperability as a subsidizing factor. The weakness here is that it recommends use of various middleware which do not meet all customer expectations in the various domains such as Information retrieval, automated messaging and data transmission.

The proposal to have a gateway to support interoperability is realized by a smartphone and connects networks with diverse protocols such as Bluetooth, ZigBee and Ethernet. The core limitation of their model is that users cannot access the sensor data unless they install server software on their Personal Computers. The architecture for interoperability

in various models do not support extended gateway capabilities hence a limitation in scalability features.

Research on interoperability has exposed the consequence of lack of interoperability which includes issues such as vendor lock-in, impracticality to develop IoT applications for heterogeneous or cross-domain platforms, difficulty in plugging new IoT devices into diverse IoT platforms, and eventually inhibits the emergence of IoT technology at a large-scale especially in developing countries where infrastructure is still a challenge.

Many consumers of smart home devices and technology vendors appear to be bypassing the need for discrete devices that are able to relate directly among themselves. They instead rely on intermediary devices to enable communications and trigger actions.

This research however intended to study interoperability among devices in a specific area of IoT with intention to propose a solution to heterogeneity based on an environment with unique needs (such as a developing country) and priorities in making life more comfortable in a home.

The concept of interoperability can be broken down into two broad theories: The standards-based theory and voluntary theory, which have been discussed earlier. This study gives a hybrid of the two theories such that the standards are taken care of by organizational and legal aspects of interoperability then the voluntary theory is addressed by technical and semantic aspects of devices.

On contribution to practice, the study presents a detailed model, which is simplified per module and can be adopted by any of the manufacturers in design and deployment of smart home technology.

2.6 Conceptual Framework

A conceptual framework is an analytical tool which explains an anticipated relationship among variables in a given research problem. It is used to make conceptual distinctions and organize ideas. The conceptual framework is subdivided into three sections:- First, Independent variables which are the factors which are manipulated or controlled. They are isolated from other factors derived from the research. Second, Dependent variables are factors, which are reliant on other factors of the study (the independent variables). They are subject to any modifications of the independent variables. Third is the moderating factors, which can strengthen, weaken, contradict, or otherwise adjust the association between independent and dependent variables [41].

Empirical studies have indicated four dimensions of interoperability is seen as: - Technical, semantic, organizational and legal issues as factors that affect interoperability of devices [42]. The summary is as in the figure 1.1 below as developed by the author.

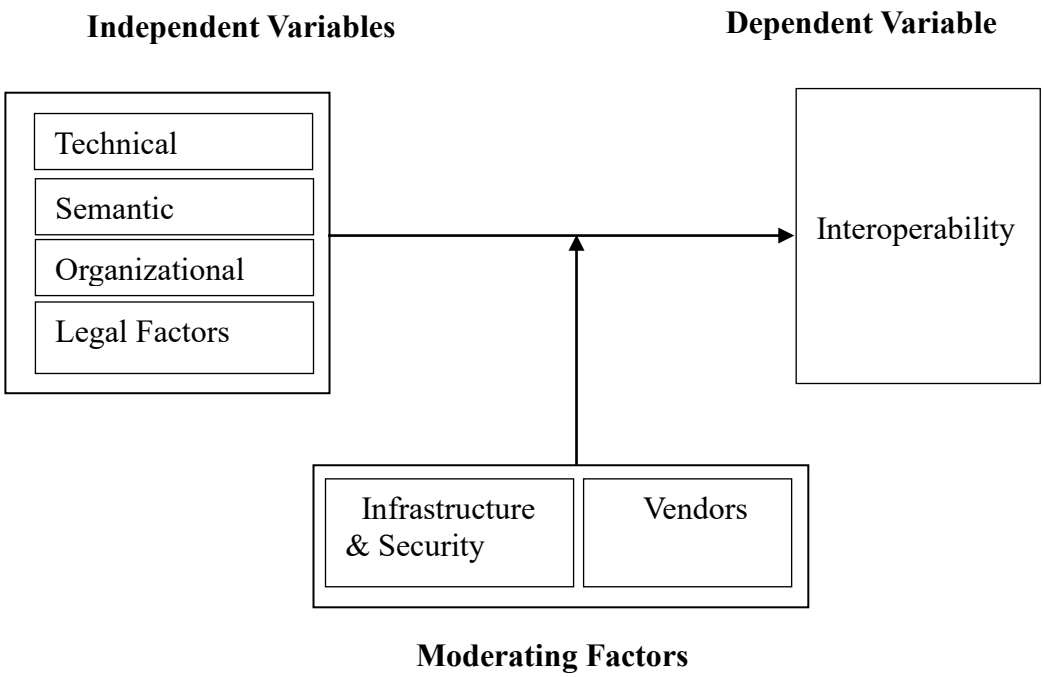


Figure 2.4 Conceptual Framework

Technical interoperability refers to the ability of more than one application to accept data from each other and execute a given activity in an appropriate and satisfactory manner without the need for any other intervention. The various aspects of interoperability such as message transmission protocols and data exchange formats are addressed.

Semantic interoperability is the capability to authorize systems, services or the devices and or users to interpret the precise meaning of exchanged content unambiguously. The concept of having a linguistic bridge that can work with a variety of protocols and interpret the signals uniformly is included.

Organizational interoperability is concerned with how more than one organization collaborate to achieve their goals. This include the strategic level interoperability which is

an enabler for partnership building such that it facilitates vendors to develop devices, which allow interoperation to effectively promote regional interests. Interoperability issues addressed include harmonization of the worldviews on devices, strategies and infrastructure [43].

Legal interoperability covers the situations that involve policies, laws, procedures and guidelines needed to allow the cooperation and exchange of information between different devices in different regions and countries.

The **Infrastructure and security** as moderating factor here refers to mechanisms for secure communication and collaboration. It implies a decentralized but consolidated and coordinated network of interconnected devices which and provide a consistent view of all the data and related information available across the network securely. The infrastructure also includes a reduced view of complexity during data exchange and provides an environment for network engagement. This infrastructure allows for numerous presentations of information based on the various requests and significances of participating data societies. Its objective is to give a universally agreeable data governance mechanism. This moderating factor includes the adoption of standards which are open and can accommodate common data and metadata models, taxonomies, patterns for the design of user interfaces. The infrastructure here includes the clouds, servers and data networks [44].

Vendor refers to firms who engage in manufacturing, distribution, installation and maintenance of devices. For interoperability to be possible, a very high degree of partnership between a buyer and a supplier must exist. The outcome is achievable if the firm and the market or products are agreeable to each other [44].

2.7 Chapter Summary

This section provides both the theoretical and practical foundation necessary to investigate and develop models for smart home device interoperability. The first section defines key concepts, such as smart homes, their functions, users, security, energy optimization, and lifestyle benefits. It also examines issues surrounding IoT, its uptake, implementations, and applications, while projecting the future of IoT and device interoperation.

The second section reviews related studies, particularly models for interoperability, addressing connectivity, network, syntactic, semantic, and platform interoperability. Strengths and weaknesses of existing models are evaluated.

The third section revisits the research objectives, reviewing the state of device interoperability and the role interoperability plays in smart homes. This is followed by an exploration of IoT architecture, including Service-Oriented Architecture, ubiquitous service discovery, HAVi, IFTTT, and MQTT. The chapter also outlines smart home model approaches (model-based and interactive) and theoretical perspectives on IoT interoperability. Then it concludes with the identification of research gaps, the study's contribution to knowledge and practice, and the presentation of the conceptual framework that will guide the research.

CHAPTER THREE: RESEARCH METHODOLOGY

3.1 Overview

This section explains the course undertaken in answering the research questions. It explains the research design, experimental design, data collection instruments and procedure, quality control for data collection instruments, responses, reliability, data analysis and presentation and ethical considerations.

3.2 Research Philosophy

A research philosophy explores how the nature of reality is viewed. This is the ontology of nature and subsequent knowledge acquired. It is referred to as the epistemology of a study. The research was guided by Interpretivism which is preferred in qualitative research. The justification for the choice of this philosophy is that the participants are in a natural environment which is a home setup and seeks to get their experiences and preferences. Interpretivist approach seeks meanings and experiences of users (or inhabitants in this case of smart homes) within their social existence [15].

Interpretivism is particularly well-suited for this study because it focuses on human experiences, interpretations of actions and social contexts which are key factors in understanding how people interact with technology in smart homes. The focus on subjective user experiences in smart homes involve personal or context-dependent interactions such as privacy concerns and automation preferences. Interpretivism could also allow further researchers to explore how users navigate or negotiate ethical dilemmas in real-world settings. It is also important to note that for Smart home developers to achieve a Human-Centered Design Insight, the approach is quite suitable so as to improve usability and acceptance of smart home devices.

3.3 Research Approach

A research approach used in the study was Inductive. This approach begins with a detailed observation of the physical environment then moves towards a more abstract generalization [46]. The justification for this was based on the fact that when one is using an inductive approach, there are no hypotheses that are found at the preliminary stages of the research. The design sought to categorize the research operations into two: - observation data and interview data. The approach implemented data collection through interviews, observations and case studies conducted in homes with installed smart devices.

3.4 Research Strategy and Design

The research strategy is used to provide the intended direction of an identified problem during an investigation [47]. This research was guided by the following four major issues: - The research objectives, the time taken, and cost of the research and the skills of the investigator. This research was both case study and observation and sought to develop a model for the interoperability for Internet of Things in a smart homes. A sample of smart homes within the country (Kenya) was studied and observation were carried out to verify interoperability. Use cases focused on the categories as follows:

Smart metering which covered the areas of: - electricity and energy utilities gas and water. The Facility Management Services which covered: - Smart doors, Smart Light switches, Intruder alarms, fire alarms, Flood alarms, Ventilation, Air conditioning.

The Home appliances category which covered: - the refrigerator, Television, Cooker and Water Heaters.

The Personal appliances which covered: - Health parameters and Tracking of objects. Finally the device Intelligence which covered: - Learning capability of devices, Topology, Naming, System diagnostics and Security.

The objectives one and two were heavily borrowed from literature reviewed. The strategy employed for each of the objective is as summarized in the table 3.1 below:-

Table 3.1: Summary of how objectives of the research was addressed

	Objective	Strategy
1	To determine the state of device interoperability in Smart Homes.	Literature review and primary data
2	To establish the role of interoperability in Smart Homes in the Internet of Things environments.	Literature review and secondary data
3	To assess the factors that facilitate or inhibit interoperability of devices in smart homes in the Internet of Things.	Empirical or Primary Data
4	To develop a model for interoperability in a smart home.	This was informed by Secondary and Primary data.

The specific actions which were carried out for objective 1 included a survey on protocols, middleware platforms, and semantics in relation to the devices available in the market. The key databases used in literature review and search terms were identified. The relevant academic databases such as ACM Digital Library, IEEE Xplore, Scopus, Web of Science were chosen. Then a comprehensive list of terms/keywords and possible Boolean

search strings. For example ("smart home" OR "home automation") AND (interoperability OR standard*) AND (challenge* OR barrier* OR limitation), ("IoT" OR "Internet of Things") AND ("smart home") AND (protocol* OR "communication standard") AND (fragmentation) were listed to be used.

A comprehensive taxonomy table and a critical analysis report identifying key gaps and limitations in current solutions especially in developing countries, which justified the need for a new model. There were other target areas especially on the Technical, semantic, conceptual and syntactic metrics of interoperability.

Technical Interoperability was assessed through observing whether devices could connect and exchange bits based on a signal from a sensor.

Semantic Interoperability was assessed by checking if an IFTTT signal would be interpreted the same by devices from different manufacturers to establish if there was a common understanding of context.

Conceptual Interoperability was adopted to check if shared conceptual models such as ontologies and state models would be consistent.

F**or Syntactic Interoperability** use of standardized message formats were checked particular interest were JSON and MQTT topic formats.

The specific actions for objective 2 involved the use of semi-structured interviews with homeowners and technical staff to probe deeper role of interoperability. Device documentation analysis was done on technical and API specifications to evaluate openness and standards support. Some guided questions were asked and given a score for each level of agreement.

Interviews and observations were adopted in approval of the third objective when assessing factors that facilitate or inhibit interoperability of devices in smart homes in the Internet of Things.

3.4.1 Interview Design

The assessment of device interoperability in Smart Homes assessed the devices in relation to home appliances, personal appliances and facility management. Personal appliance was chosen to cut across since the person's comfort of use is the target

The checklist used is attached in the appendix section 8.0.

3.5 Case Selection

This section explores the target population, sample and sampling techniques.

3.5.1 Target Population

A target population is complete set of units for which the study data are to be used to make interpretations or inferences. The target population defines those units for which the findings of the study are meant to generalize [48]. It is worth noting that there is no documented number of smart homes in Kenya and therefore difficult to give exact numbers. According to start.io, the number of smart home devices in Kenya is 323,399 as of late 2024 [49]. The target population of this research was smart home owners and experts or technicians involved in deployment of smart home devices. Since the purpose of this research was to identify key issues in interoperability of devices in smart homes, the study population target was on all homeowners who had installed smart services in their homes and all technicians of companies who specialized in installations of the same.

3.5.2 Sample and Sampling techniques

A critical attribute in research methodology is having a representative sample which is able to represent the qualities of a target population and be able to generalize the entire population [49]. The recommended sample size as a rule of thumb a target population of over 300,000 is between 20 and 40 participants [50]. Purposive Sampling was used hence only technology-engaged households within Nairobi were visited and observations made as well as the tenants or occupiers of the homes were interviewed. Purposive Sampling is particularly suited for this research because qualitative research uses non-probability sampling, chosen deliberately to target meaningful variations. It is targeting users who have direct experience with the environment. Interviewing users who have lived in smart homes or technicians who have deployed smart homes. Maximum Variation Sampling was adopted since selected participants differed on certain characteristics like age and gender. The goal was to capture a wide range of perspectives.

There was also an adoption of snowball sampling technique where referrals from smart home deployment technicians was adopted for those who had some elements of smart homes in specified areas. There was a challenge however here since the risk of homogeneity was encountered especially when users were literally peers. To remedy the homogeneity risk, a saturation check was implemented such that if three consecutive interviews presented the same answers, a new sample was sought. A sample of customers from service provider's outlets were randomly approached for data in specific devices they were interested on. The primary strength of snowball sampling is its ability to access populations that are difficult to identify and reach through conventional means.

3.6 Data Collection

3.6.1 Respondents

Prequalification of a selected population means ensuring that the participants in the study fit the criteria for the research objectives. An inclusion criteria used in the respondents was that participants must have an eligible age range, location and experience with smart devices or smart homes. A Pre-survey involved the use of a short interview schedule to check eligibility. Questions target demographics, prior experiences, access to devices and the willingness to participate.

The respondents were classified into two: - First, the inhabitants of smart homes whose experience was captured through observations and interviews. Secondly, the vendors and technicians who sale and deploy the technology. They were assessed through interviews and visits to the sites was also done.

3.6.2 Instruments

The instruments used in the research were observation checklists and guided questionnaires in data collection with a pre-prepared list of behaviors, events, or features to look out for (Attached in Appendix 1). This was a preferred option because it ensures focus on relevant items and is the recommended option for structured observation.

Observation is noted to have a weakness of subjectivity and researcher Bias. The researcher may opt to only see what they want to see or interpret the feedback the way they would like it to look like. This was addressed by use of Structured Observation Instruments whereby a checklist was used with a rating scale. This would ensure that observations followed a pre-defined criteria rather than personal impressions. The researcher acknowledged their own biases and reflected on how they could influence their interpretation and hence complemented with objective, quantitative data.

3.7 Validity and Reliability

Validity was seen as a way to ascertain how well a test measures what it was supposed to measure. Validity is a necessity in research because it makes conclusions reliable and consistent [50]. Reliability is the level to which a tool used in an assessment produces stable and consistent outcome.

The questions used in data collection in the research were designed in such a way that it covered the whole area of study. The help of the literature reviewed and the objectives of the study were sought so as assist in coverage of the area of study. A pre-testing checklist was used to see whether the questions asked would capture what was expected.

In order to ensure findings were accurately a representation of user meanings and experiences, a triangulation method was adopted through a combination of interviews and observations to cross-verify findings. This involved testing the initial results with other users in order to see if the results were still relatively true. The output was a reduced bias and hence ensured that the results reflected the expected user experiences.

3.7.1 Validity

Validity is the degree of theory support to the interpretations proposed by the tests [50]. So as to achieve content validity, questionnaires included a variety of areas covered by a smart home. The questionnaires were based on literature reviewed to ensure a representation of all issues raised before in other models. The results were then be compared with those collected from the questionnaires and other models for validity. The concept of triangulation was adopted such that the results from the literature, the checklist and those from the questionnaire were mapped to show some relationship between them. Triangulation method was adopted because it facilitates validation of data by cross

verification from more than two sources. It is ideal because the consistency of findings is obtained through different tools of data collection and increases the chance having reliable results in the research. The study didn't rely on a single data source. The researcher cross-verified what the expert interviewees shared with the empirical data from the structured observations.

3.7.2 Reliability

Reliability is the degree to which the same instruments will give similar results at different times [50]. Since sometimes the questions in the questionnaire may have some weaknesses, a pretest was carried out to consider it for reliability, applicability and practicality before conducting the research. Two experts from the vendor category were chosen to assess the questionnaires before subjecting them to a pilot study.

Cohen's Kappa (κ), was used to determine reliability as a statistical measure used in categorical data. It was chosen because it is useful in content analysis and coding of qualitative data.

Two users were asked 24 interview responses and agreement was coded as "Positive" while a disagreement as "Negative."

- They agreed on 21 cases, disagree on 3.
- Observed agreement Po=21/24=0.875.
- Chance agreement Pe (calculated) = 0.5.

$$\kappa = \frac{P_o - P_e}{1 - P_e}$$

Where P_o = observed agreement among respondent

P_e = expected agreement by chance

$$\kappa = \frac{0.875 - 0.5}{1 - 0.5}$$

$$\kappa = \frac{0.75}{}$$

To interpret the value**s**, the scale used is as follows:

< 0.00 → Poor

0.01–0.20 → Slight

0.21–0.40 → Fair

0.41–0.60 → Moderate

0.61–0.80 → Substantial

0.81–1.00 → Almost perfect

The results on reliability was therefore considered substantial with a figure of 0.75.

3.7 Data Analysis and Presentation

Mathematical models were used and applied to the data as the basis for analysis and the analysis done in statistical packages; SPSS was chosen because basic indicators used in qualitative analysis can be easily derived using the application. Descriptive statistics was largely adopted because of the qualitative nature of the study. The tools used to present data were tables, bar graphs, line graphs and pie charts as per the objective of the presentation of the data.

Tables are used where displaying detailed raw data, exact numerical values and where comparison is deemed necessary.

Bar graphs were used where objectives included comparing categories showing frequency distributions and when there was need to highlight differences.

Line Graphs were used where tracking trends over time, displaying continuous data and Predictive modeling is required or part of the objective of the presentation.

Pie charts were used where displaying proportions of a whole or percentage breakdowns needed to be shown.

3.8 Ethical Considerations

The concept of research requires aspects of knowing what is right or wrong, this also caters for integrity and honesty. The data collected was treated in confidence when subjects asked for it so as gain credibility and trust. Respondents were first advised and requested to provide consent upon understanding how their data was to be handled, stored, processed, and shared. Confidentiality and anonymity [47] was an important aspect since there are numerous threats which are both physical and logical to homes. The results believed to be truthful were presented as accurately as possible. The researcher also ensured that the process complied with institutional and legal guidelines for data collection and presentation.

3.9 Chapter Summary

The chapter begins with an overview of the methodological framework, explaining the rationale behind the chosen research philosophy, approach, and strategy. The research philosophy defines the underlying worldview guiding the study, while the research approach clarifies the study follows a qualitative method orientation. The research strategy and design section addresses the specific methods used to gather data, including the design of interviews tailored to capture participants' experiences with smart home interoperability. Case selection is discussed, highlighting the criteria for choosing study

sites, followed by a description of the target population and the sample and sampling techniques applied to ensure relevance and diversity in participants.

Data collection procedures are described, including the identification of respondents and the instruments used, such as structured or semi-structured interview guides, observation checklists, or surveys. The chapter also addresses validity and reliability, explaining the measures taken to ensure the data accurately reflects the phenomena under study and that coding and analysis are consistent.

Finally, ethical considerations are highlighted, emphasizing informed consent, privacy, and confidentiality, ensuring the study meets ethical standards and protects participant rights.

This chapter provides a clear, systematic framework that ensures the research is credible, reproducible, and ethically sound, forming the foundation for data analysis and interpretation in subsequent chapters.

CHAPTER FOUR

RESULTS AND FINDINGS

4.0 Chapter Overview

This chapter presents the results from the data collected from the field. Interoperability process model of devices found in a smart home environment. The chapter expounds result analysis and observations made during the study.

Data analysis was done using Statistical Package for Social Scientists (SPSS). A descriptive approach was adopted in the analysis of data. Use of tables, charts, and graphs were used to demonstrate key trends in the data. User experience and expert's feedback from interviews are presented, some patterns are identified and user concerns and expectations regarding smart homes are also captured. Some of the statistical techniques include: Relative frequencies in some research questions, means scores, and standard deviations were used.

4.1 Respondents

The key respondents of the study were subdivided into two categories: - Smart Home service providers or vendors and Smart home users. The vendors refer to the people who do sales and installation of smart home devices while the smart home users are the owners or the tenants who have invested in smart homes. Demographic classifications were also used so as to capture how personal characteristics influence smart home adoption, usage and perception of interoperability. The use of age group, gender, education levels were also captured from the respondents in the research.

It was necessary to collect data from the smart home users because they are the

consumers of the products and they are the final people who stand to benefit if interoperability is fully achieved as the technology matures in developing countries.

The vendors were the providers of the technology and they understand the technical requirements of deployment and therefore are the core people since they stand to benefit if interoperability is achieved in deployment and expansion of their product portfolio.

4.1.1 Response Rate for Smart Home Users

Data was collected from customers of the various service providers. Table 4.1 below Shows that out of 24 respondents targeted 18 provided feedback which makes a response rate of 75 % response rate. A response rate of the range of 40 up to 80 percent is sufficient to make a generalized conclusion of the entire population [51]. The population that gave audience for interview was because the researcher reached the offices of the vendors who had already established a relationship with users therefore it became easier conducting the interviews from there and for them to respond.

Table 4.1: Response Rate for Smart Home users

Category	Sample Size	Response	Percentage **(%)**
Smart Home Users	24	18	75

4.1.2 Response Rate for Smart Home Device Vendors

For the vendors of smart home devices the target population was 10 (Ten) of which seven (Seven) provided audience for interview, this is a response rate of 70%. The table 4.2 below shows the response rate from vendors.

Table 4.2: Response Rate for Smart Home Device Vendors

Category	Sample Size	Response	Percentage **(%)**
Device Vendors	10	7	70

4.2 Respondents Demographics

Data collected from users of smart home devices included gender, age, level of education and how long they have lived in smart homes. This section discusses the demographic characteristics of the tenants or users of smart homes.

4.2.1 Gender of the Respondents

The Figure 4.1 below shows the statistics of the gender of the respondents interviewed. It was observed that a very high number of respondents were male at 77.78% and female 22.22% who have adopted smart home device use. The Male respondents seem to be excited in adoption of smart devices and hence living in a smart environment than female.

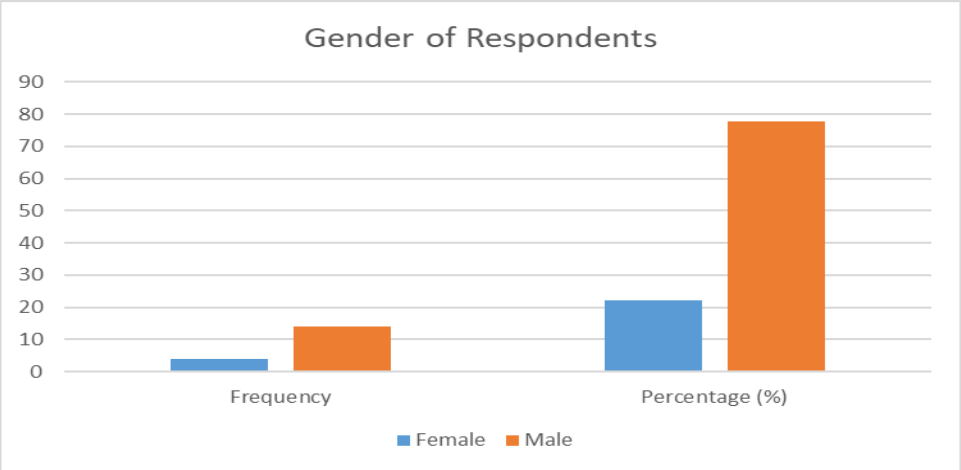


Figure 4.1 Gender of Respondents

A summary table 4.3 is indicated below.

Table 4.3 Gender of Respondents

Variable	Frequency	Percentage (%)
Female	4	22.22
Male	14	77.78

4.2.2 Age of the Respondents

The figure 4.2 below shows the statistics of the age of the respondents interviewed. A range of 10 was chosen since this was observed as sharing the same characteristics in establishment of homes. They were grouped as 25-34 Years, 35 – 44 Years, 45 – 54 Years, 55 – 64 Years and above 65 Years.

It was observed that the highest age group interested in smart homes are those between 35 – 44 years at 33.33% , followed by both those of 45- 54 Years at 27.77%, then 55-64 Years at 27.77%, the least is the range of 25-34 years at 11.11 %. The finding shows that those above 65 years are not interested in smart home solutions or deployments and yet smart homes have advantages of being aging population-friendly.

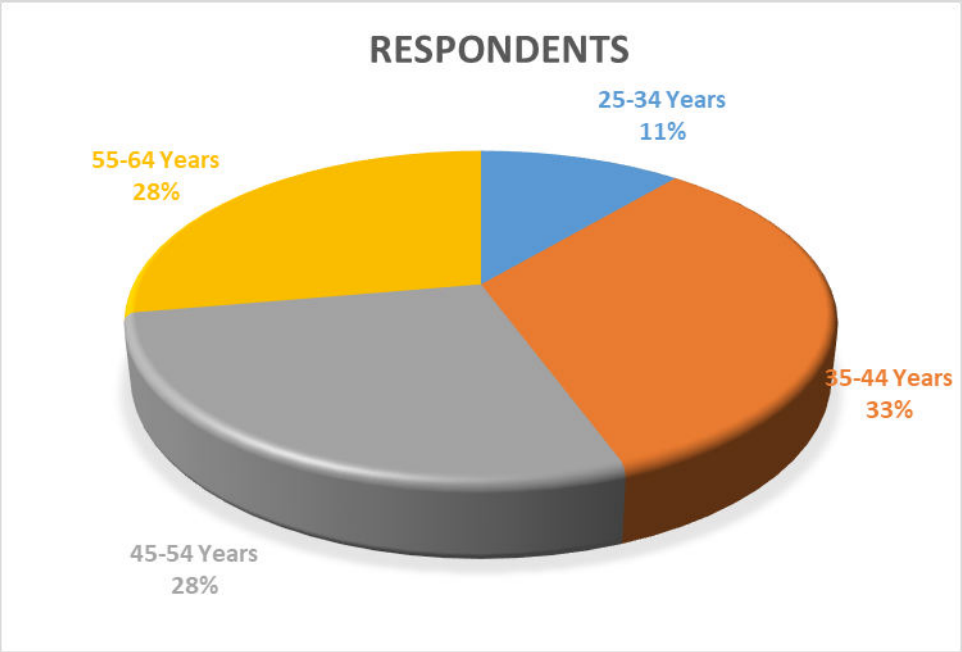


Figure 4.2 Age of Respondents

A summary table 4.4 below shows how the age of the respondents was distributed.

Table 4.4 Age of Respondents

Variable	Frequency	Percentage (%)
25-34 Years	2	11.11
35-44 Years	6	33.33
45-54 Years	5	27.77
55-64 Years	5	27.77
Above 65 Years	0	0.00

4.2.3 Level of Education of the Respondents

The study examined the level of education of respondents as shown in the Figure 4.3 below. It was established that majority of the consumers of smart home technology have an undergraduate qualification.

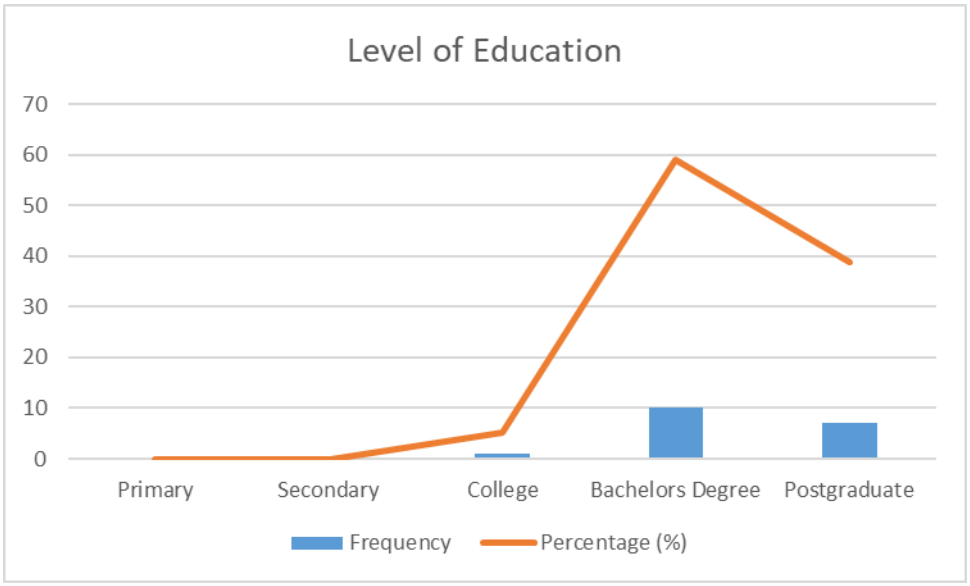


Figure 4.3 Level of Education of the Respondents

4.2.2 Length of stay in Smart Homes

The figure 4.4 below shows the length of stay in the smart home was assessed in order to establish the experience of the users or consumers of the smart home technology. It was observed that 100 percent of the tenants were less than 5 years into the smart home environment. The clustered bar chart below shows the length of stay in smart homes by the users who responded.

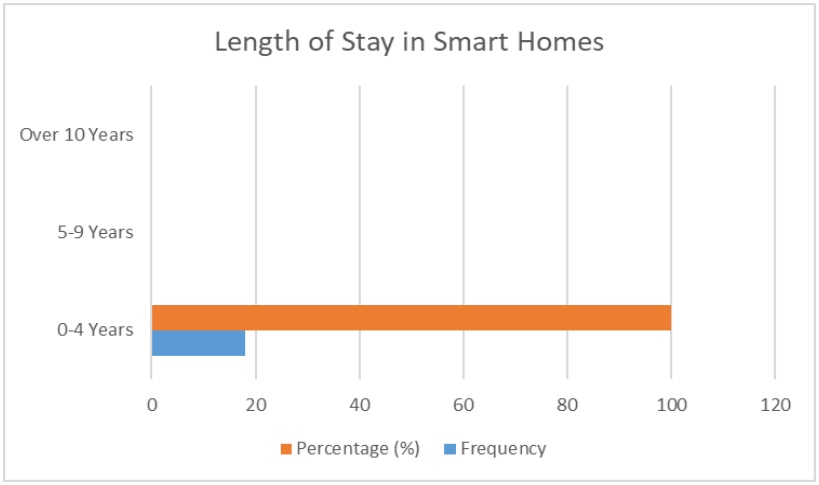


Figure 4.4 Length of stay in Smart Homes

4.3. Findings on Each Objective

4.3.1 Objective 1: To determine the state of device interoperability in Smart Homes.

To determine the state of device interoperability in smart homes deployed, the research sought to find out the extent to which home appliances and personal appliances against facility management. The user of smart homes were asked if their homes had devices which supported various services as indicated in the Figure 4.5 below. The responses were as indicated out of the 18 sampled users and how they agree on whether devices communicate seamlessly or not.

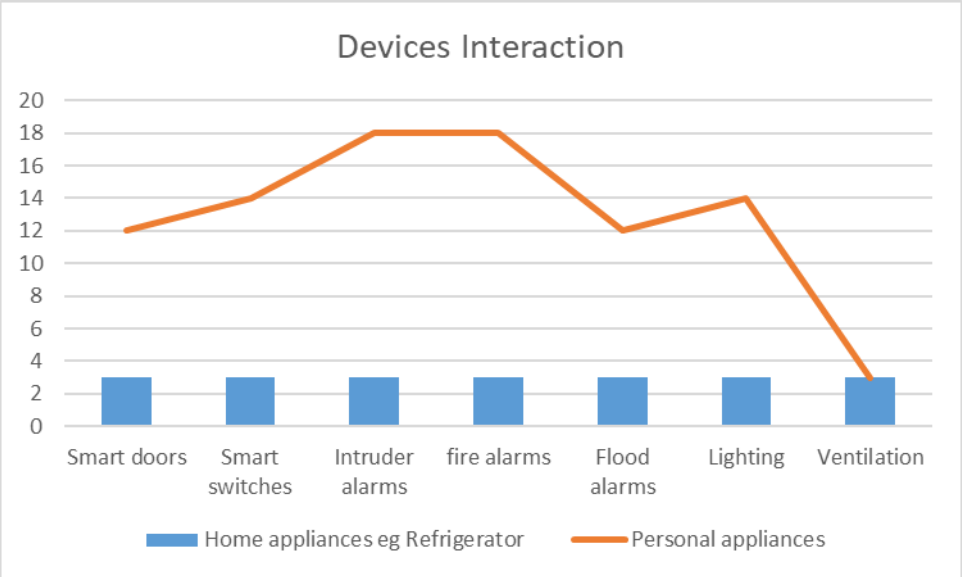


Figure 4.5 Devices Interaction

The observation was that the 3 home users who agreed on their home appliances having an integration with interoperability were all from the same vendor who had installed the service for them. That is why they yielded the same results. The implication is that device interoperability deployed in the country is at its infancy state.

For appliances and Interoperation, it was noted that most users were able to use their mobile phones to interact with devices in their homes remotely such as lighting and door locks. This seems to be the most widely accepted product.

4.3.2 Objective 2: Role of Interoperability in Smart Homes

The assessment of interoperability was assessed form the point of view of whether users would be aware of why we need interoperability. A scale of 1-5 (where 5 – Strongly Agree, 4- Agree, 3- Neither Agree nor Disagree, 2- Disagree, 1 – Strongly Disagree) was chosen and choices from literature was given to the users of smart devices in smart homes.

The areas of assessment was:- Quality of Service, Response to services in emergencies, Costs of deployment of solutions, introduction of new services to integrate existing and new services, Reduction of unnecessary administrative functions, Software modifications and/or addition of new elements, the elimination of discrepancy of operators' expectations in relation to integration, Introduction of attractive services hence reflects positively on vendor's competitiveness, impact on income of vendors, consolidates continuous service and criteria for decision making.

A majority of respondents indicated that the highest valued among the factors that promote interoperability is that it promotes quality of service and affects the criteria for decision making both having a mean of 4.89. This implies that users of smart homes are heavily inclined towards quality of service and guides how they make choices in buying devices in a smart home. The second factors which are perceived as roles of interoperability is on reduction of the Costs of Deployment of solutions and that of Consolidation of continuous Services both at a mean of 4.72 which are also ranked very highly. Majority of respondents agree that this is a major role of interoperability in smart homes. The next role is that of elimination of discrepancy among Operators who deal with smart home deployment at a mean of 4.67. The other role is seen as that which allows for Integration of New Services and devices at a mean of 4.61. Interoperability is

also seen as being able to reduce unnecessary Administrative Activities at 4.56. Interoperability is also key in elimination of the need for frequent software modifications which has a mean of 4.33. Response to Emergencies is also seen as a role of interoperability in enabling different devices to respond during emergencies having a mean of 4.22. The other two issues which were measured on the role of interoperability are that Interoperability allows introduction of attractive services which reflects positively on Vendor's Competitiveness and Eliminates hitches that may negatively affect income of vendors both at 4.00. This low rating of vendors may have been caused by the fact that the aspects were subjected to users of smart homes who may not really care about vendors and their profitability. The Table 4.8 below summarizes the responses of the various factors believed to play a role of Interoperability among devices found in a Smart Home.

Table 4.3 Responses of various roles of Interoperability among devices found in a Smart Home: -

	Mean	Std. Deviation
Promotes Quality of Service	4.890	0.323
Response to Emergencies	4.220	0.428
Allows for Integration of New Services	4.610	0.502
Reduction of Unnecessary Administrative Activities	4.560	0.511
Reduce Costs of Deployment of solutions	4.720	0.461
Eliminate the Need for Frequent Software Modifications	4.330	0.485

Eliminates discrepancy among Operators	4.670	0.485
Allows Introduction of attractive Services which reflect positively on Vendor's Competitiveness	4.000	0.485
Eliminates Hitches that may Negatively affect income of Vendors	4.000	0.343
Consolidates continuous Service	4.720	0.461
Interoperability Affects the Criteria for Decision Making	4.890	0.323

In the results tabulated above, the analysis was done on a range between 0 and 5 (both included) and the highest factor of 5 (or close to 5) implies a factor that plays a greater role according to the respondents. This implies the higher the mean, the higher the role on interoperability. The standard deviation was used to define either a high deviation or low deviation. A high deviation would be greater than 1 and a low deviation less than 1. Since all values are less than 1 then it implies the respondents did not differ much in their belief about the role of interoperability. This implies that all factors assessed are believed to have an impact on as a role which interoperability plays.

The order of acceptance of the factors are as follows:- interoperability promotes quality of service, affects the criteria for decision making, eliminates hitches that may negatively affect income of vendors, reduces costs of deployment of solutions, makes work easier during emergencies, consolidates continuous service, allows introduction of attractive services which reflect positively on vendor's competitiveness, allows for integration of

new services and eliminates discrepancy among operators, reduction of unnecessary administrative activities in that order.

4.3.3 Objective 3: Factors that facilitate or inhibit interoperability of devices in smart homes in the Internet of Things.

Responses of Factors that facilitate interoperability of devices in Smart Homes

The study pursued to know from respondents the importance of the various factors that facilitate interoperability of devices in smart homes. The findings are as shown in the Table 4.9, using a Likert Scale of 1 to 5 where 1 – Strongly Disagree, 2- Disagree, 3- Neither Agree nor Disagree, 4- Agree and 5 – Strongly Agree. The factors measured were: - Growing availability of Web Services, Growing availability of data, development and diffusion of more universal Solutions, Novel Machine2Machine technology solutions, Smart phone and Smart objects diffusion and the Need for reduction of costs.

Table 4.4 Responses of Factors that facilitate interoperability of devices in smart homes in reference to dealers and vendors

	Mean	Std. Deviation
Growing availability of data	4.94	0.236
Growing availability of web services	4.78	0.428
More universal solutions	4.67	0.485
Novel machine2machine technology solutions	4.94	0.236
Smart phone and smart objects diffusion	4.33	0.485
Need to reduce costs	4.11	0.676

In the results presented above, the analysis was done on a range between 0 and 5 (both included) and the highest factor of 5 (or close to 5) implies a factor that is higher in preference as a promoter of interoperability than others. The standard deviation was used to define either a high deviation or low deviation. A high Deviation would be greater than 1 and a low deviation less than 1. Since all values are less than 1 then it implies the respondents did not differ much in their confidence about the factors that promote interoperability.

4.3.3.1 Responses of factors inhibit interoperability among devices

The study also sought to know from respondents the importance of the various factors that inhibit interoperability of devices in smart homes. The findings are as shown in the Table 4.15 below, Using a Likert Scale of 1 to 5 where 1 – Strongly Disagree, 2- Disagree, 3- Neither Agree nor Disagree, 4- Agree and 5 – Strongly Agree. The factors measured were:- Lack of regulations, Profitability of the solutions, High time-to-market for new applications, Broadband network which has multimedia capability, Scalability of devices, Security issues, Changing enabling technologies such as 3g to 4G and deployment of 5G networks, RFID or Wi-Fi technologies, Vendor device incompatibility, User-centric perceptions, Lack of compelling success stories and Unavailability of testing centers, Non-standardized interfaces or protocols, Equipment from one manufacturer, but with different software revisions resulting in incompatible, Different middleware manufacturers, Complexity of networks through integration of networks and devices requires additional cost of hiring knowledgeable staff in various brands of equipment, There are applications, which are launched by vendors who do not provide infrastructure and support to enable interoperability, Loss of independence among vendors is a threat

especially for emergency response service providers, Limitation to implement new features and services which can run on all platforms inhibit interoperability among vendors, Reduces the need for additional costs and time to solve problems which arise from lack of interoperability, and whether it eliminates the delays of projects caused by difference among vendors, additional costs for upgrades and the extra tests needed after upgrades

Table 4.11 Responses of factors inhibit interoperability among devices based on users

	Mean	Std. Deviation
Lack of regulations	4.83	.383
Different middleware manufacturers	4.83	.383
Reduces the need for additional costs and time to solve problems which arise from lack of interoperability.	4.78	.428
Limitation to Implement new features and services which can run on all platforms inhibit interoperability among vendors	4.72	.461
There are applications, which are launched by vendors who do not provide infrastructure and support to enable interoperability.	4.67	.485
Eliminates the delays of projects caused by difference among vendors, additional costs for upgrades and the extra tests needed after upgrades	4.61	.502
Security issues	4.61	.502
Equipment from one manufacturer, but with different software revisions resulting in incompatibility	4.61	.502

Complexity of networks through integration of networks and devices requires additional cost of hiring knowledgeable staff in various brands of equipment.	4.61	.502
Loss of independence among vendors is a threat especially for emergency response service providers	4.56	.511
Lack of compelling success stories and Unavailability of testing centers	4.56	.511
Changing enabling technologies such as 3g to 4G and 5G networks, RFID, Wi-Fi	4.56	.511
Non-standardized interfaces or protocols	4.56	.511
Vendor device incompatibility	4.56	.511
Scalability of devices	4.39	.502
High time-to-market for new applications	3.06	.998
Profitability of the solutions	2.56	1.199
User-centric perceptions	2.06	1.162
Broadband network - Capacity for transmission of multimedia when users add much to the network	1.72	.461

In the results presented above, the analysis was done on a range between 0 and 5 (both included) and the highest factor of 5 (or close to 5) implies a factor that is higher in preference as a promoter of interoperability than others. The standard deviation was used to define either a high deviation or low deviation. A high Deviation would be greater than 1 and a low deviation less than 1. There are two factors which differ with a greater than 1 deviation which are:- Profitability of the solutions and User-centric perceptions which

attracted a wider view from the users. This means they may not care about profitability and perceptions of users.

The data exchange formats assessed fall under semantic factors and those that inhibit are as shown in the table 4.15 as follows:-

Table 4.15: Data Exchange Formats

	Mean	Std. Deviation
Security issues	4.61	.502
Equipment from one manufacturer, but with different software revisions resulting in incompatibility	4.61	.502
Loss of independence among vendors is a threat especially for emergency response service providers	4.56	.511
Non-standardized interfaces or protocols	4.56	.511
Vendor device incompatibility	4.56	.511

The data exchange format assessed that stimulates Interoperability as shown in the table 4.16 below:-

Table 4.16: Data Exchange Format

	Mean	Std. Deviation
Growing availability of web services	4.78	0.428

There is an indication that data exchange formats stimulates Interoperability since each of the factors tested have a close agreement as shown in the data. Security issues and

Equipment from one manufacturer, but with different software revisions resulting in incompatibility related to data exchange format is seen as the highest rated factors. If message transmission protocols do not agree then technical Interoperability is not achievable. An agreeable data exchange format by all manufacturers in smart home devices is therefore a factor of promotion.

Factors that promote interoperability as shown in the table 4.17 below:-

Table 4.17: Factors that promote interoperability

	Mean	Std. Deviation
Lack of regulations	4.83	.383
Different middleware manufacturers	4.83	.383
Reduces the need for additional costs and time to solve problems, which arise from lack of interoperability.	4.78	.428
Limitation to Implement new features and services which can run on all platforms inhibit interoperability among vendors	4.72	.461
There are applications, which are launched by vendors who do not provide infrastructure and support to enable interoperability.	4.67	.485
Eliminates the delays of projects caused by difference among vendors, additional costs for upgrades and the extra tests needed after upgrades	4.61	.502
Security issues	4.61	.502
Equipment from one manufacturer, but with different software revisions resulting in incompatibility	4.61	.502
Complexity of networks through integration of networks and devices	4.61	.502

requires additional cost of hiring knowledgeable staff in various brands of equipment.		
Loss of independence among vendors is a threat especially for emergency response service providers	4.56	.511
Lack of compelling success stories and Unavailability of testing centers	4.56	.511
Changing enabling technologies such as 3g to 4G and 5G networks, RFID, Wi-Fi	4.56	.511
Non-standardized interfaces or protocols	4.56	.511
Vendor device incompatibility	4.56	.511
Scalability of devices	4.39	.502
High time-to-market for new applications	3.06	.998
Profitability of the solutions	2.56	1.199
User-centric perceptions	2.06	1.162
Broadband network - Capacity for transmission of multimedia when users add much to the network	1.72	.461

Table 4.18 below shows the data exchange formats assessed that stimulates Interoperability are as follows:-

Table 4.18: Data Exchange Formats Assessed

	Mean	Std. Deviation
Growing availability of data	4.94	0.236
Growing availability of web services	4.78	0.428
More universal solutions	4.67	0.485

Novel machine2machine technology solutions	4.94	0.236
Smart phone and smart objects diffusion	4.33	0.485
Need to reduce costs	4.11	0.676

High time-to-market for new applications, Profitability of the solutions and User-centric perceptions seem to be at the bottom of the list in preferences when assessing if Systems, services or devices and or users that interpret signals correctly promote interoperability in smart homes.

Growing availability of data and Novel machine2machine technology solutions are major issues acceptable to vendors when assessing if Systems, services or devices and or users that interpret signals correctly promote interoperability.

Legal frameworks do not positively affect the development of cooperation and exchange of information between different devices in different regions used in smart homes.

The factors that affect the legal framework are shown in the table 4.19 below and indicates if it allows the development of cooperation and exchange of information between different devices in different regions used in smart homes according to users were assessed as follows:-

Table 4.19: Factors that affect the legal framework

	Mean	Std. Deviation
Lack of regulations	4.83	.383
Different middleware manufacturers	4.83	.383
Security issues	4.61	.502

User-centric perceptions	2.06	1.162

In this factors analyzed in the table above, it is only User-centric perceptions that seems to be outside the expectation of users. The other three factors: - Lack of regulations, Different middleware manufacturers and Security issues are close hence acceptable to be affecting interoperability.

The factors that affect the legal framework if it allows the development of cooperation and exchange of information between different devices in different regions used in smart homes according to vendors were assessed as shown in the table 4.20 below:-

Table 4.20: Cooperation and exchange of information data

	Mean	Std. Deviation
Growing availability of data	4.94	0.236
Growing availability of web services	4.78	0.428
More universal solutions	4.67	0.485
Novel machine2machine technology solutions	4.94	0.236
Smart phone and smart objects diffusion	4.33	0.485
Need to reduce costs	4.11	0.676

There is an indication from the data that User-centric perceptions is not a factor that would influence this issue of legal framework. The rest of the factors are acceptable since they have a value deviation close to the mean and is less than one.

The table 4.21 below indicates the acceptable factors for building partnerships according to users of smart homes:-

Table 4.21: Factors for Partnership building.

	Mean	Std. Deviation
Reduces the need for additional costs and time to solve problems, which arise from lack of interoperability.	4.78	.428
Limitation to Implement new features and services which can run on all platforms inhibit interoperability among vendors	4.72	.461
There are applications, which are launched by vendors who do not provide infrastructure and support to enable interoperability.	4.67	.485
Eliminates the delays of projects caused by difference among vendors, additional costs for upgrades and the extra tests needed after upgrades	4.61	.502
Security issues	4.61	.502
Equipment from one manufacturer, but with different software revisions resulting in incompatibility	4.61	.502
Complexity of networks through integration of networks and devices requires additional cost of hiring knowledgeable staff in various brands of equipment.	4.61	.502
Loss of independence among vendors is a threat especially	4.56	.511

for emergency response service providers		
Lack of compelling success stories and Unavailability of testing centers	4.56	.511
Changing enabling technologies such as 3g to 4G and 5G networks, RFID, Wi-Fi	4.56	.511
Vendor device incompatibility	4.56	.511
Scalability of devices	4.39	.502
High time-to-market for new applications	3.06	.998
Profitability of the solutions	2.56	1.199

The table 4.22 below indicates how vendors of smart home devices feel if partnership building is key in facilitation of vendors:-

Table 4.22: Partnership building in facilitation of vendors.

	Mean	Std. Deviation
More universal solutions	4.67	0.485
Need to reduce costs	4.11	0.676

Profitability of the solutions is a minor issue as far as Partnership building is concerned. Vendors are willing to sacrifice profitability for the sake of interoperability.

4.3.3.3 Other Observations from the Data collected

Design and deployment of smart homes still at its infancy stage in developing countries.

Companies involved in the smart home markets in Kenya are small start-up companies, which deal with home appliance companies, security applications, and infrastructure control applications and therefore are limited in funding which limits their budgets on security of the systems and limited to accessing security research networks and communities.

Smart homes are created with different capabilities and hence they are not equal. There are numerous design approaches that contribute to the aspect of a house being referred to as smart. The approach in Kenya is heavily on integration of autonomous home-automation systems which face a challenge of control from various independent points. It is worth to note that these approaches have their own uniqueness in addressing security and privacy. They also may experience shared concerns and vulnerabilities.

Smart homes are likely to have substantial privacy and data safety impacts. With the increased number of integrated sensors, the logs of activities in smart home based on stochastic activities and behaviour of users or visitors will be a definite source of big data, which will be accompanied by dozens of challenges on privacy and safety matters. The application of basic information security would considerably escalate the overall level of security in the smart home.

The user needs of different property owners or managers in the smart home may be in conflict, for example, a user wants a complex secure platform with simple access controls, which produces a complex environment for security activity.

Another technical comment from one user is that the security challenge for camera devices is that the images captured are plain text not encrypted which poses a challenge to users on how secure the entire network would be.

4.4 Chapter Summary

This chapter presents the findings from field data collected on the interoperability of devices in smart home environments. Descriptive statistics, including relative frequencies, mean scores, and standard deviations. Tables, charts, and graphs were used to illustrate key patterns, while user and expert feedback from interviews provided insights into experiences, expectations, and concerns.

The chapter establishes that while smart homes in Kenya are growing, interoperability is still limited. Users value quality of service and cost reduction, while vendors acknowledge the need for universal standards and partnerships. However, regulatory gaps, technical incompatibilities, and security risks remain significant barriers to achieving a universal objective of interoperability in Internet of Things.

CHAPTER 5

DEVELOPMENT OF A MODEL FOR INTEROPERABILITY IN A SMART HOME.

5.0 Chapter Overview

This chapter presents the proposed model for achieving interoperability in smart home environments. It gives a deep explanation on modelling device interoperability, proposed design guidelines, factors affecting or inhibit interoperability, proposed interoperability model, each framework component is explainedan example of a prototype device developed and implemented and model validation.

5.1 Introduction to Modelling Device Interoperability

This section discusses the proposed model in order to achieve objective 4 which seeks to develop a model for interoperability in smart homes. The chapter first indicates the proposed design guidelines, an algorithm for interoperability, it then assesses responses of the various factors for interoperability and the desired aspects of interoperability then the design of the proposed model.

5.1.1 Proposed Design Guidelines

The process of specifying the factors used in interoperability involves first identifying the process, which fulfils a successful interoperable device ecosystem. The following algorithm shows how interoperability is achieved for two sample devices.

i. A sensor from a manufacturer A and/or B detects an action initiated by a smart home user.

ii. The sensor A sends a message to a device actuator of device A or can send a message to a sensor of device actuator from a manufacturer B mounted on a device from a manufacturer C

iii. The device actuator receives the message and decodes it to understand the signal

iv. The actuator queries the meaning from a universally acceptable knowledge base

v. The database returns the actions needed.

vi. The device actuator acts as per the conclusion from the returned function.

vii. If an error is detected, a return message is sent either to the sensor, another sensor in the next alternative loop from the knowledge base or to the output display of the device at the origin of the signal.

viii. The signal is interpreted and communicated to the user through an appropriate interface which maybe either a specific beep or an error code which should be captured in user manual documents attached to each device during shipment.

The figure 5.1 below developed by the author shows a summary of how the proposed model should be implemented.

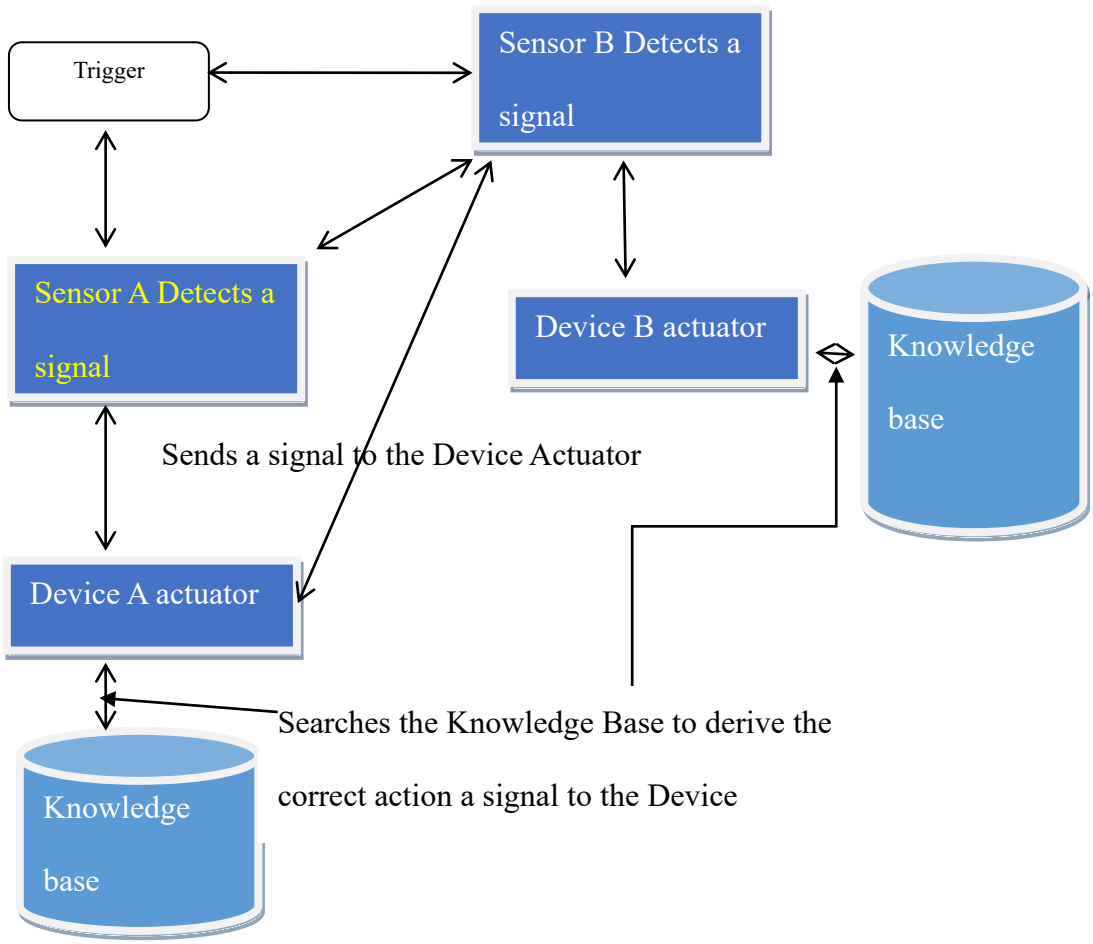


Figure 5.1: A structure showing implementation of interoperability in devices

The following section discusses the various factors adopted for the research.

5.1.1.1 Technical Factors

The study sought to know from respondents their view on Technical metrics that affect interoperability. The findings are as shown in the Table 4.10 below, Using a Likert Scale of 1 to 5 where 1 – Strongly Disagree, 2- Disagree, 3- Neither Agree nor Disagree, 4- Agree and 5 – Strongly Agree. A majority of respondents strongly agree that if interoperability of the networks is required of the vendors then, the technical problems are deterred during the interconnection procedures at a mean of 4.23. This issue is followed by the strong agreement that How to update newer software on devices will be a non-issue if devices are made to be interoperable shown by a mean of 4.14. This was

followed by the issue of main interoperability problems being a result of proprietary and non-standard interfaces of vendors at 3.00, which is neutral. The issue that the respondents disagreed with as a technical aspect of interoperability is where vendors deploy terminals that have no function for emergency reporting at 2.29. The table 5.1 below shows the responses of technical factors that affect interoperability.

Table 5.1: Responses of Technical Factors for interoperability

	N	Mean	Std. Deviation
If interoperability of the networks is required of the vendors then, the technical problems are deterred during the interconnection procedures	7	4.29	.488
The main interoperability problems are due to proprietary and non-standard interfaces of vendors.	7	3.00	1.000
Vendors deploy terminals that have no function for emergency reporting.	7	2.29	.951
How to update newer software on devices will be a non-issue if devices are made to be interoperable	7	4.14	.690

In the results above, the range of 0 to 5 inclusive was adopted where the higher the mean the more the factor is seen as an influence technically. It is noted that the standard deviation is employed in the data analysis to indicate if it is less than one shows a close agreement to the issue among the respondents, while those equal to or above one are seen to be more divergent in views of the respondents.

5.1.1.2 Semantic Factors

The study sought to know from respondents their view on Semantic metrics that affect interoperability. The findings are as shown in the Table 4.27 below, Using a Likert Scale of 1 to 5 where 1 – Strongly Disagree, 2- Disagree, 3- Neither Agree nor Disagree, 4- Agree and 5 – Strongly Agree. Since the investigation is based on a home, Home appliances have the highest mean of 4.43 such that the support for these devices is very strong. Device intelligence followed with 4.14, Facility Management services followed with 3.86 and Personal appliances are perceived to be least in semantic interoperability preference at 3.71. The support for semantic Factors support among devices is summarized in the table 5.2 indicated in the following section.

Table 5.2 : The support for Semantic Factors Support among Devices

	N	Mean	Std. Deviation
Home Appliances	7	4.43	.535
Personal Appliances	7	3.71	.756
Facility Management Services	7	3.86	1.069
Device Intelligence	7	4.14	.900

In the results above, the range of 0 to 5 inclusive was adopted where the higher the mean the more the issue is seen as more influential. It is noted that the standard deviation is employed in the data analysis to indicate if it is less than 1 shows a close agreement to the issue among the respondents, while those equal to or above 1 are seen to be more

divergent in views of the respondents.

The correlation among the semantic factors assessed is as shown in the table 4.28 below:-

All values are high meaning each of the factor is significant in ensuring that authorized systems, services or the devices within a smart home and users are able to interpret the precise meaning of exchanged content unambiguously.

5.1.1.3 Legal Factors

The study sought to know from respondents their view on Legal metrics that affect interoperability. The findings are as shown in the Table 4.31 below, Using a Likert Scale of 1 to 5 where 1 – Strongly Disagree, 2- Disagree, 3- Neither Agree nor Disagree, 4- Agree and 5 – Strongly Agree. The argument that there are too many standards is seen to be the highest with a mean of 4.29, then Workflow procedures not organized to collect required data is next with 3.00 while Lack of specificity in standards (not constrained), too much optionality makes exchange impossible has a mean of disagree with a mean of 2.29. The Assessment of Legal Factors on Interoperability is as show in the table 5.3 below

Table 5.3: Assessment of Legal Factors on Interoperability

	N	Mean	Std. Deviation
Too many standards	7	4.29	.488
Workflow procedures not organized to collect required data	7	3.00	1.000
Lack of specificity in standards (not constrained), too much optionality makes exchange impossible	7	2.29	.951

In the results shown in the table 4.31 above, it is noted that the standard deviation is employed in the data analysis to indicate if it is less than 1 shows a close agreement to the issue among the respondents, while those equal to or above 1 are seen to be more divergent in views of the respondents. A range of 0 to 5 inclusive was adopted where the higher the mean the more the influence. The factor that there is lack of specificity in standards, too much optionality makes exchange impossible is a strong issue affecting legal aspects with a very small standard deviation.

The data displayed in the table 4.32 below shows a correlation matrix which implies an strong correlation between the existence of too many standards and Lack of specificity in standards (not constrained), too much optionality makes exchange impossible. This means the legal factors that affect standardization makes exchange of data among devices difficult hence difficulty in interoperability.

There are two factors which are very significant in this section which are:- Workflow procedures not organized to collect required data and Lack of specificity in standards (not constrained) and too much optionality makes exchange impossible.

The major legal factor affecting interoperability is Lack of specificity in standards (not constrained), too much optionality makes exchange impossible at 0.881 which is a very strong factor. The fact that there is too many standards implies an influence on the legal factor but very minor.

5.1.1.4 Organizational Factors

The study sought to know from respondents their view on Organizational metrics that affect interoperability. The findings are as shown in the Table 4.35 below, Using a Likert

Scale of 1 to 5 where 1 – Strongly Disagree, 2- Disagree, 3- Neither Agree nor Disagree, 4- Agree and 5 – Strongly Agree. The highest point as strongly agreed by the respondents is the fact that there is no clear direction if market is there for a product at 4.57, followed by Standards don't apply to things I value at 4.43, Lack of clear direction or priorities is next at 4.14 and Standards Workflows are not organized to collect required data at 3.71. The Table 5.4 below shows Assessment of Organizational Factors on interoperability

Table 5.4 : Assessment of Organizational Factors on interoperability

	N	Mean	Std. Deviation
Standards don't apply to things I value	7	4.43	.535
Standards Workflows are not organized to collect required data	7	3.71	.756
Not clear if market is there for a product	7	4.57	.535
Lack of clear direction or priorities	7	4.14	.900

The results from the table above shows the range of 0 to 5 inclusive was adopted where the higher the mean the more the issue is seen as more influential. It is noted that the standard deviation is employed in the data analysis to indicate if it is less than 1 shows a close agreement to the issue among the respondents, while those equal to or above 1 are seen to be more divergent in views of the respondents. There is only one factor, Lack of clear direction or priorities. This factor seems to be almost out of range of agreement with the rest. This implies that the most of the vendors have their priorities in place for interoperability provision.

5.2 Proposed Model

The overall aim of this research was to propose an interoperability model for devices in a smart home environment which would be adopted as smart homes are rolled out in developing countries.

This section deliberates on interoperability indicators, framework proposal and tests the applicability of the anticipated framework. The areas addressed as indicators covers areas of technical viability and operational concepts as well practical deployment of the same.

The conceptual framework of the research anchors on four major areas of interoperability, these are:- Technical, Semantic, Organizational and Legal issues based on the IOT Taxonomy model in the figure 2.1. The proposed model is therefore based on these factors incorporated and extended to give a comprehensive model. The moderating variables are Network infrastructure & Security and vendors. The figure 5.2 below shows a summary of desired aspects of interoperability.

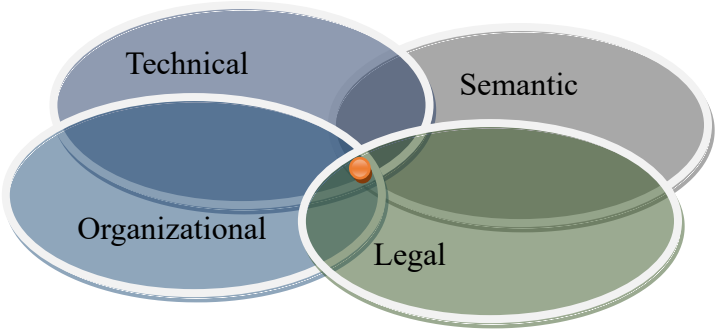


Figure 5.2 : Showing Desired Aspects of Interoperability

Technical issues in the framework refers to ability of more than one device and related application to send or receive data from each other and execute a given activity in a satisfactory manner without the need for any other intervention, interconnection of devices without technical problems arising, support for open architectures, resolution of

non-standard interfaces, emergency reporting included and easy updates of newer software.

Semantic issues deals with the capability to authorize services or the devices to be able to interpret the accurate meaning of exchanged content explicitly. This addresses issues of communication among the four specific areas in smart homes:- Home appliances, Personal appliances, facility Management and the intelligence of the devices used in the interoperation ecosystem.

Organizational issues involve how more than one organizations collaborate to enable interoperability by having a mechanism to capture customer needs, joint market survey and having a clear direction or priorities in development of devices.

Legal aspects need to address the issue of policy to the manufacturers of devices hence guide them on how to achieve standards which are interoperable.

Model Development

The development phase was a structured process of understanding the problem, designing a solution, and building a sample prototype of a device that can implement interoperability from a customer perspective.

1. Problem Analysis and Requirements Gathering

This was a foundational phase which sought to answer the "why" and "what". The Interoperability problem was identified as the existence of heterogeneous devices which use different communication protocols for example Wi-Fi, Zigbee, Z-Wave, and Bluetooth. It was also noted that a fragmented ecosystem of devices from different manufacturers operate within themselves and do not communicate seamlessly. Diverse

data formats used by devices, such that **s**ensors and actuators generate data in various structures and semantics, making it difficult for other devices to work as a unified system.

2. Establishment of the objectives of the Model was done which were considered as:

Seamless Integration: New devices should be discovered and integrated automatically, proposal of a unified control where a single platform should be able to control all devices, cross-platform communication should also be possible for example a zig-bee light bulb to be triggered by a Wi-Fi camera and a scalable and Secure solution.

3. Stakeholder requirements Consideration

These were subdivided into three: - First, End-User Requirements**:** Easy setup, plug-and-play functionality, a single unified app for control, reliability, and privacy. Second was to check developer requirements: Standardized APIs, clear documentation, integration tools, and third was manufacturer requirements where a model that doesn't require complete overhaul of existing products, maintaining brand identity, and security.

4. Design of the Model

This was the core of the development, where the theoretical model was designed. A recommended and effective approach was the use of a layered architecture framework as documented in the table 5.5 below.

Table 5.5: The Proposed Interoperability Model:

Layer	**Core Function**	**Components and Technologies**
5. Application and	Provides a cohesive	**Unified Mobile/Web App,** Voice

Layer	Core Function	Components and Technologies
Interface Layer	user interface and enables cross-device communication.	Assistants (Alexa, Google Assistant), Automation of the knowledgebase (e.g., "If button pressed, then turn on release amount of water assigned to the button").
4.Semantics Layer (Meaningfulness of data Layer)	Gives meaning to data so devices can understand each other's context and signals from actuators.	Data Models, JSON-LD. This layer translates "Signals" from sensors to actuators of another device.
3. Platform Layer	Is a message broker. Manages devices, data flow, and provides a common API.	**IoT Platforms** (Home Assistant, OpenHAB), **Message Brokers** (MQTT, AMQP), **API Gateways.** This is a central software. (In the model MQTT is adopted)
2. Network Layer	Handles the layer 1 and layer 2 connectivity issues of devices.	**Protocol Translation Gateways** (e.g., a hub that speaks both Zigbee and Wi-Fi), **IP-based Networks** (Wi-Fi, Thread).
1. Sensor and Actuator Layer	The physical IoT devices themselves and their sensors/actuators.	**Sensors** (motion, temperature), **Actuators** (smart plugs, lights, locks)**.**

The following section explain each of framework components.

5.2.1 Sensor and Actuator Modelling

The figure 5.3 below proposed by the author shows the desired device-to-device communication for a door lock and a sensor associated with it.

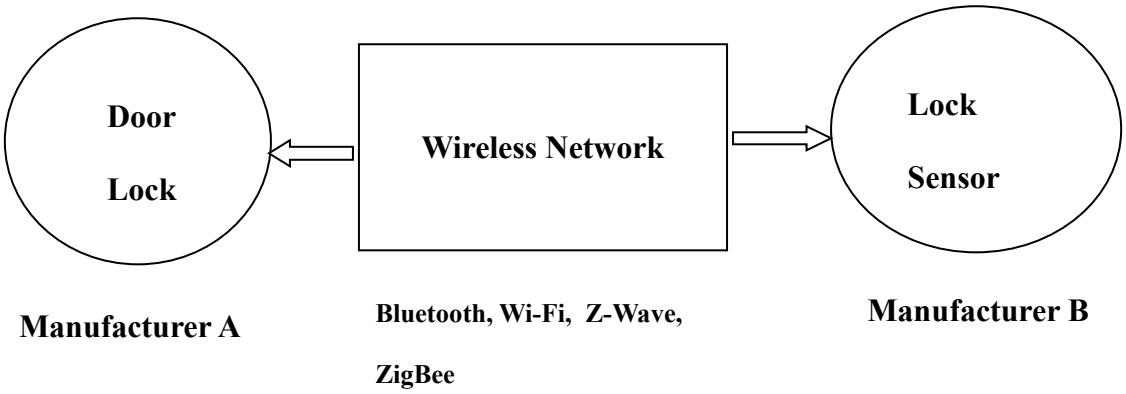


Figure 5.3: Showing Desired device-to-device communication in a Smart Home

This is a manufacturer's view of the device such that its design is able to describe the contents and circumstance in which the data is sent or received by a particular device. The device should also have an express capacity to interpret it with minimum or no error experienced. The actual meaning of data can be discovered by examining the software that produces and processes the data independently before integration into the device to approve of its' operation as correct. The data sent through the network infrastructure must implement authentication so that it is deemed as secure for implementation. The table 5.6 below shows how different levels of data interpretation can be deduced in the attempt to make devices interoperate. It depicts desired meaningfulness and interpretation of signals or data as devices communicate.

Table 5.6 : Modelling Meaningfulness of the data within devices

	Data Detection and Interpretation	**Meaning**
More meaningful	Physical Location of the Sensor for the	Measure the physical

physically Least Physical meaning	intended Location	temperature of a Room
	The physical meaning is derived	Manufacturer design is on temperature detection/ management domain
	Meaning of the raw data is converted to a datatype e.g float	
	Raw data Detected (in Binary)	

The interpretation of source data by devices is key in enabling semantic interoperability as it interpretation and understanding by successive processors.

For devices to be interoperable, the base should be on the ability of device manufacturers to have a semantic for each of the vertical domain. The table 5.7 below shows how horizontal and vertical interoperability is necessary and how it can be implemented to allow horizontal communication. The vertical aspects on the domain is left for specific domain manufacturers, however it is required that the meaningfulness of the data within these devices are guaranteed.

Table 5.7 : Modelling Meaningfulness of the data within devices

Metering Devices	Personal Appliances	Home Appliances	Facility Management
Meaningfulness of the data within devices			

For Device interoperability to be achieved, Tolk's Model proposes that devices must be able to communicate (irrespective of protocols used and capabilities i.e. whether High end or Low end), their syntactic constitution (irrespective of data formats, schema and interfaces). Since smart homes encountered during data collection is heavily wireless, the

model considers semantic and platform interoperability as already inbuilt into device operations.

By combining all wireless network standards including Wi-Fi, Zigbee, Z-Wave, RF and infrared technologies, most smart home devices would easily integrate either directly through an interface or through numerous software application programming interfaces (APIs).

5.2.2 Event Modelling

The figure 5.4 below shows how a desired Sensor and Actuators should be. The sensor has an integrated environment which must perform all activities with minimum time lag. An event causes a sensor ecosystem to react by first understanding the source of the event (who caused the event), the event itself, then assess the current state of itself and integrate the knowledge it has so as to correctly interpret the event and context. The process involves the sensor undergoing some brainstorming session, which a pre-fetch algorithm should be implemented in order to speed up the operations. The sensor then generates an appropriate message (based on the event) which is sent to the actuator based on its understanding of the signal. The actuator responds to the massage independently by the action it takes.

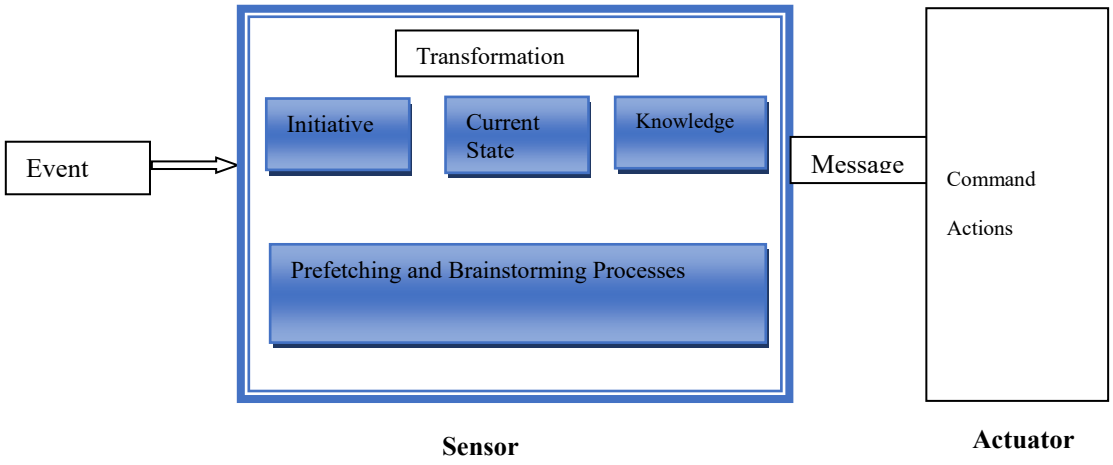


Figure 5.4: Diagram Showing Sensor and Actuator Modelling

5.2.3 Sensor and Devices Modelling

The fact that IoT is a cross-domain technology, there is a necessity to capture the knowledge shared across both the vertical and horizontal linkages between the domains. The diagram 5.5 below shows how devices are modelled to cater for sensors and devices.

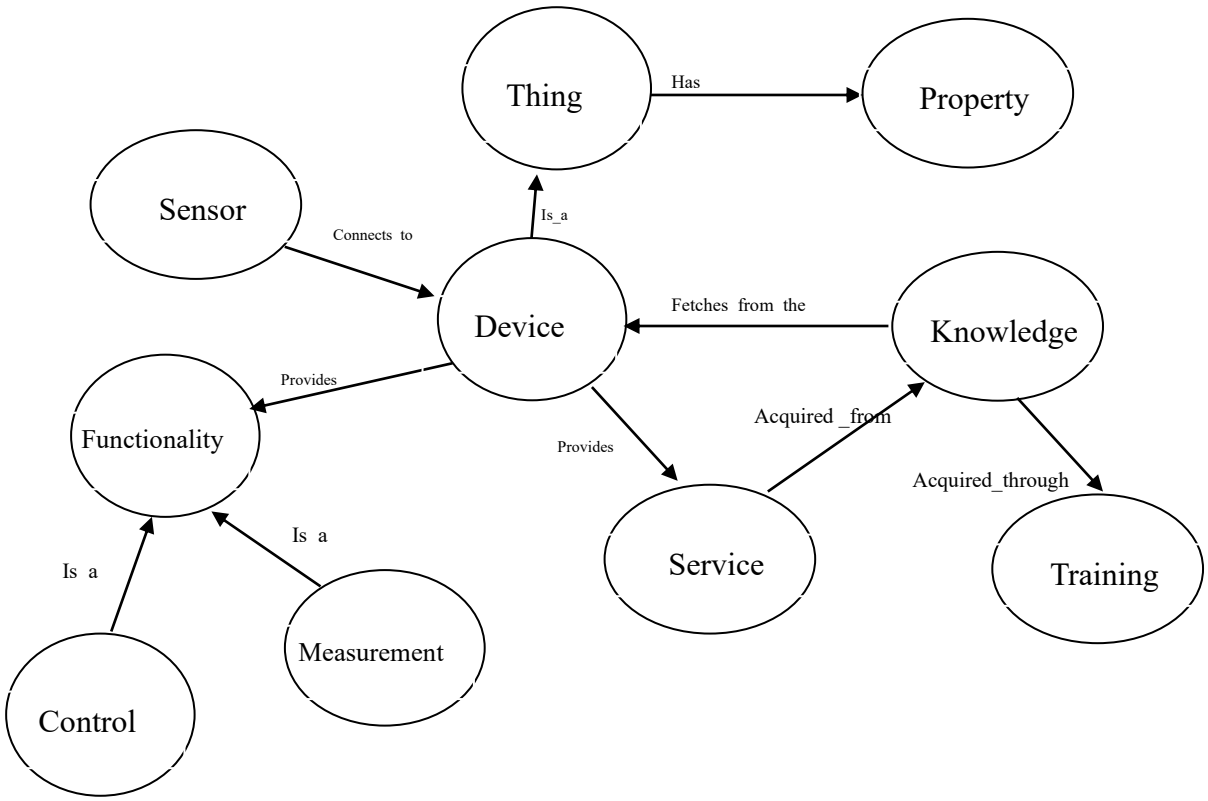


Figure 5.5 : Sensor and Devices Modelling

The heterogeneity of IoT domains will drive the development of a language through terminology creation, extension and recycle; this stimulates requirements for vocabulary management capabilities and updates. The recommended management of the vocabulary in this model is an over the air (OTA) update capability to be integrated. The updates can be released periodically by the manufacturers to the devices directly as long as they support the technology. The semantic data model needs to be extensively rich and can be at the same time can be simplified to enable seamless operation of IoT ecosystems as newer and complex devices join smart envirnments and where minimal or no human intervention is expected to be implementd or is completely unavailable. There is however a concern of updates which could create more security vulnerabilities in the ecosystem which necessitates the need to have a robust testing and deployment procedure before the

release.

5.2.4 Location-Based Modelling Probabilistic approach

The concept of location–based modelling in a smart home is based on a stochastic process which is dynamic as occupants of a smart home will move in an undefined format. A probabilistic method is seen to be more accurate as a reflection of how a true system responds considering that smart homes have residents within them who have stochastic reactions. The behaviour of devices is interdependent and most of the objects operate in an Inter-Dependent Markov Chain (IDMC) model. IDMC provides a probabilistic framework that is able to capture the effects of interdependencies among physical networks within a physical setting. The choice of this approach is to build an integrated probabilistic framework involving a system of a heterogeneous Markov chains (MCs) where there is a chain for each physical system action. The transitions are captured such that the interdependencies in a Markov chain affects the transition probabilities of the next and subsequent Markov chains.

5.2.5 **Proposed Process Model**

The proposed model has four domains namely: - Sensor ecosystem, Network Support Infrastructure, Actuators and Processing Centre. These domains are intertwined together to give an operational ecosystem of IoT devices as shown in the figure 5.5 below.

The figure 5.6 below shows the proposed model.

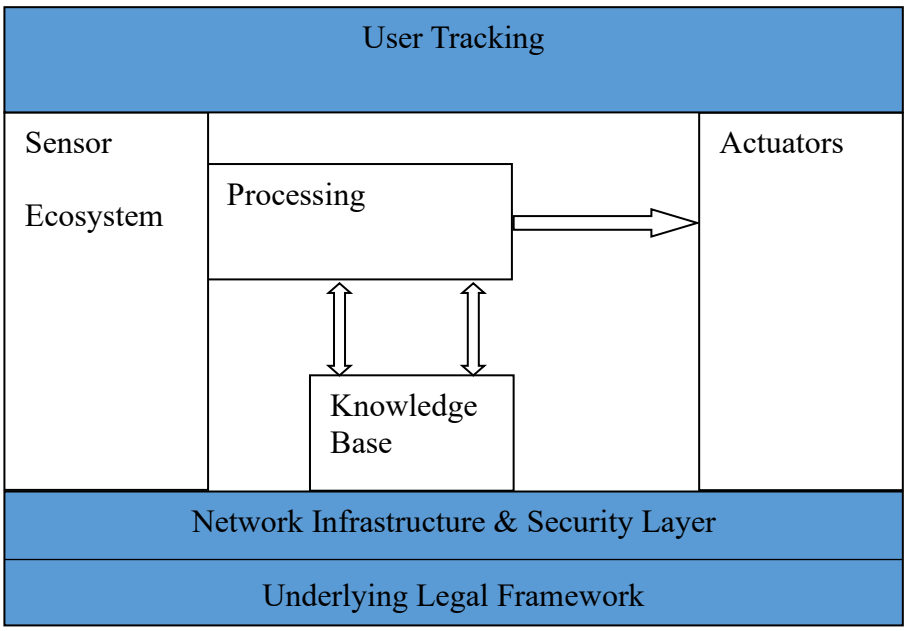


Figure 5.6: Proposed Model.

The various entities in the diagram together with their variables are further explained in the following section:-

Sensor Ecosystem:- The sensor ecosystem involves sensors which have improved capability. The sensors here are activated based on an external action or environmental trigger. The devices at this level often face challenges of memory capacity and power capability. They are also limited by the technology deployed, for example the distance a signal covers and the intensity of the trigger signal. The devices in this level have however continued to improve in their designs and moving to higher capability sensors is inevitable. Device management platforms continue to improve and capability to update them should take an Over-The-Air (OTA) approach so as to make firmware updates easier in future especially with the constantly changing network protocols and deployment of more intelligent infrastructure. This will address issues of any upcoming

patches and integration with cloud-based infrastructure solutions.

The raw measurements created by the sensors should be transformed into a metadata version that will include additional attributes such as Unit of Measurement, the time associated with the action, Software Version, naming model of the devices, type of quantity being sensed and the domain of operation as shown in the figure 5.7 below.

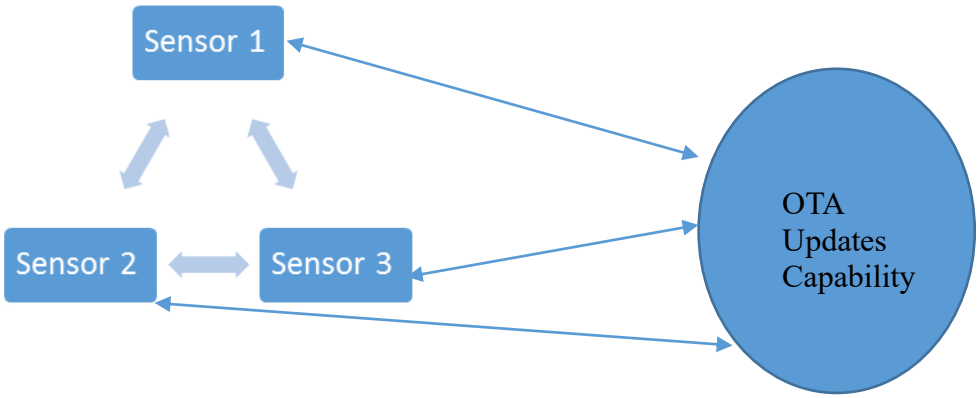


Figure 5.7: Showing How Sensor Ecosystem should work.

Processing: - The processing is attached to the sensor ecosystem. The proposal is such that once a device is manufactured, an accepted standard ontology is inbuilt to it. The logic is such that it should be able to detect and convert the domain data and relay to any other device without necessarily having to search in a knowledge base. The idea is to implement a plug-and-play option in the device. The transmission capability is critical for this device such that it should integrate with the network even if it is upgraded. Device memory has continued to increase and processing capabilities have since improved hence it would be sustainable for low powered devices to join in implementation of multiple protocols. This should also allow for stochastic requests for connections dynamically.

Knowledge Base – this is implemented by If – This – Then - That Model. This should be able to integrate with online or cloud based solutions. For example

If <Even_Light_outside_detected > Then

<Switch_off_security_Light_circuit>

If <Dark_outside> Then

<Switch_on_Secuirty_Light_Circuit>

If <Dark_outside> Then

<close_curtains>

The figure 5.8 below shows how the if-this-then-that knowledge base interacting with sensors.

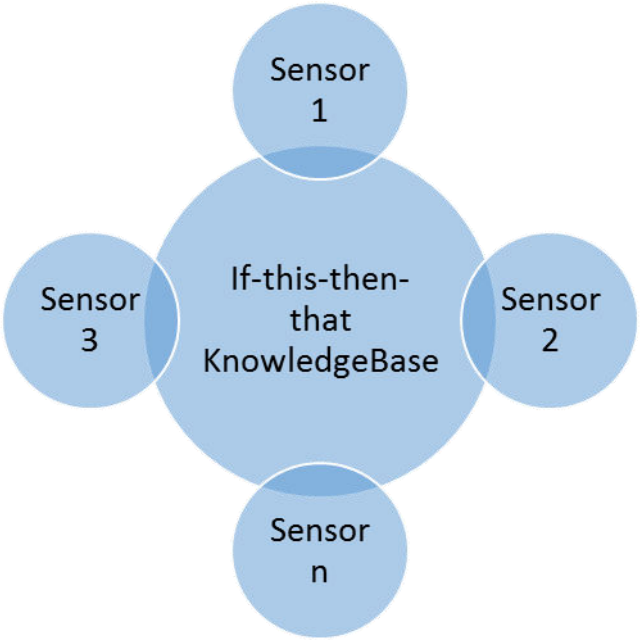


Figure 5.8: Knowledge Base implementation

Network Infrastructure

The figure 5.9 below shows how the network infrastructure can be implemented in the model.

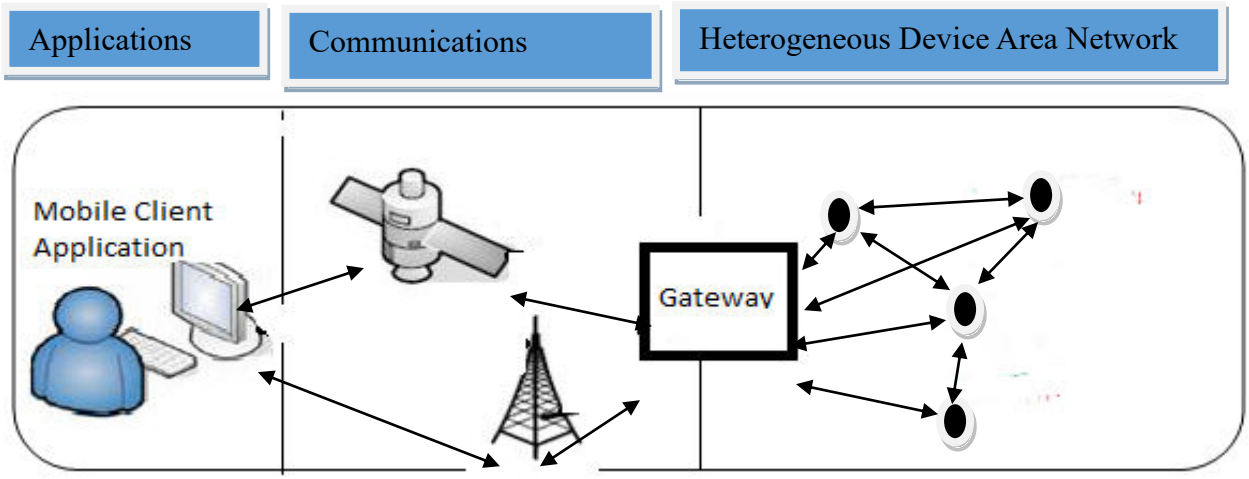


Figure 5.9: How the Network Infrastructure should work

The Heterogeneous Device Area Network involves devices loaded with sensors, processors and communication transceivers which can detect and derive conclusions of data within those devices autonomously using protocols such as Bluetooth or ZigBee.

A better scenario would be a hybrid network architecture, in which Wi-Fi is attached to low power devices with protocols that support mesh topology design within sensors. The designed network architecture in a smart home needs to provide connections both to the internet and appliance connectivity to the network.

The **Gateway** Concentrates device traffic towards the wireless telecommunication core on one side and interconnects with the internal network on the other side.

The **clients** can access data from a server which contains the middleware (application, services, and data) which is able to host business intelligence for execution of any machine to machine business transactions or logic.

Data Security

The best approach to secure communication between devices would be to employ Backend-as-a-Service (BaaS) during code development of the devices. This is an emerging trend for cloud models which provides IOT device designers with a pre-built backend substructure setup for their APIs. This will simplify their work as they do not have to worry about security of their devices during communication such as authentication aspects and hence focus on building the business logic. The infrastructure management and backend functionality is left to the BaaS provider.

Summary of Proposed Model components

The following section summarizes exclusively the expected model inputs, processing, storage and outputs as shown in the table 5.8 below.

Table 5.8: Inputs into the model

Basic Input	**Examples of Triggers**
Device-Level Inputs such as Sensor Data:	Temperature, humidity, air quality Motion detection, occupancy status Energy/water consumption readings Smart meter data Actuator Commands: Lock/unlock (doors, windows) Turn on/off (lights, appliances) Adjust (thermostats, water flow, fan speed)
Communication and Protocol Inputs such as Message Payloads, Messaging Protocols,	MQTT, CoAP, Zigbee, Z-Wave, Bluetooth, Wi-Fi, Publishing and subscription topics

Device Identifiers, Device Topics/Channels	defined for message flow, packets containing data or commands, Unique IDs, MAC addresses, manufacturer details
User and Application such as Inputs User Preferences, Controls, Schedules/Rules	Desired temperature, lighting levels, security modes , Button presses, mobile app inputs, voice commands and Timed automations
Environmental Inputs such as External Conditions, System and Integration Inputs, Contextual Data and Utility Inputs	Weather forecasts, daylight intensity, outdoor temperature, Location info (GPS), presence of residents, Grid signals (e.g., demand-response events, water availability)
Developer Configurations which are topics and permissions registered by developers such as Device Registration Data, Security Credentials and Interoperability Standards	Supported capabilities and interoperability metadata, Keys, tokens, certificates for authentication/authorization, Defined message formats, semantic rules, ontologies

Processing

The processing in the model will carry out the following activities:

1. Data Acquisition and Normalization which involves collection and standardization of data from heterogeneous devices.
2. Message parsing which break down incoming payloads into structured fields for

interpretation.

3. Validation and Verification which checks message types, formats, and authenticity against designed schemas.
4. Protocol Interpretation which mediates between different communications protocols (e.g., Zigbee ↔ MQTT).
5. Routing which direct messages from publishers to the expected subscribed devices.
6. Rule Execution which applies automation rules, schedules, and conditional logic.
7. Actuator command generation which transforms processed data into device instructions to be acted on.
8. Data storage and logging which is to save readings, commands, and events into databases for monitoring and or auditing.
9. Security enforcement whose function is to authenticate devices, authorize actions, and encrypt communications.
10. Optimization and Learning which does the analysis of usage patterns, predict needs, and adapt to user behavior.

Storage

A unified data storage structure for sensor readings and automatically generated schemas/models for new devices joining the ecosystem will be expected from the storage used by the knowledgebase. Event logs capturing device actions, message flows, and failures for auditing.

Outputs

Actions form the actuators which include: Device Communication Outputs, Data Management, Control and Actuation Outputs, Validation reports, Notifications/alerts and

Authentication/authorization logs showing successful or failed access attempts.

The specific events include: Successful messages exchange, logs showing devices subscribing/publishing to topics correctly, Standard message formats and Error messages or alerts when unsupported protocols or formats are used. Unified data storage structures for sensor readings (temperature, water usage, energy consumption,), Triggered actuator responses (e.g., smart lock engaging after valid command), and Performance metrics such as latency, throughput, and reliability of interactions and alerts on anomalous device behavior are also possible outputs.

5.3 Example of a Prototype Device Developed and Implemented.

Aquavendor Solution

Aquavendor Solution was developed and deployed as part of the testing for interoperability in a practical environment that enables integration of water vending IoT devices regardless of the hardware manufacturer. What was tested here was based on messaging, sensor and actuator Modelling. The sensor was modelled then several hardware manufacturers were given the code to run on sample hardware. The aquavendor uses Message Queuing Telemetry Transport (MQTT) based protocol which allows devices to interact with the service and each other through a message platform.

Through the API, the developer of the software uploads the list of topics the devices in the ecosystem will use. This is also the point at which, each topic must be exclusively defined as either a publishing or a subscription topic. A subscription allows listening to the incoming message while publishing allows sending/broadcasting a messages to the platform.

Subscription Topics were used where devices are expecting incoming messages from

other devices in use within the ecosystem. If a device is expecting an incoming message, it subscribes to the particular topic. If it is not necessary for them to communicate, then it is not subscribed to it. Once registered, the platform's broker performs polling where it continuously listens if there is a broadcast message on the topics it is subscribed to. When devices publish messages, the platform receives and broadcasts the published message to those devices subscribed to it.

For instance a button pressed by the water dispensing operator publishes the amount of water to be dispensed, the platform receives and stores this information or triggers a response through an actuator to another topic. For validation and verification purpose, each message sent to the platform has a standard format which includes a type field which is used to categorize the message for appropriate handling. The type field is defined during hardware development or implementation and linked to the actuator. On receiving communication, the platform validates the message type against the registered list, Parses the payload based on the type and forwards the new message to another device if it is a trigger message, stores the data in the appropriate database / logs the action and dynamically creates data storage models if necessary. The application also has a remote command capability. The code used in the device deployed is attached in the appendix. The weakness of this implementation however is the legal and regulatory standards to adhere which has been consolidated in the final model.

The pseudo code is attached in the appendix 2.

Desired Sensor/Device Ecosystem

A sensor/device ecosystem is thus summarized in the figure

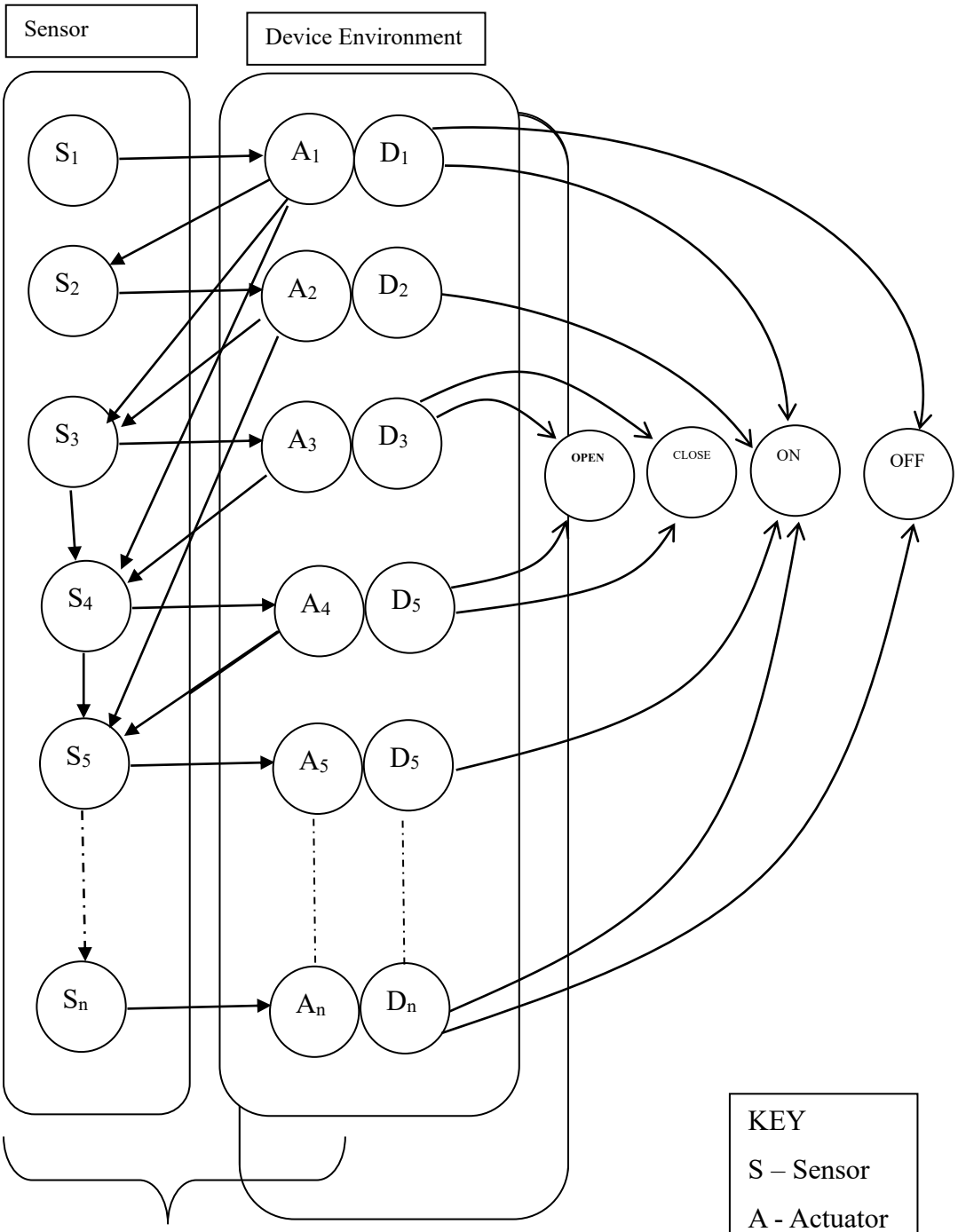


Figure 5.10: How devices Interact

The model from figure 5.10 above relies on the fact that an average smart home owner does not have the time to understand or research on which products or protocols will

work for them on their devices seamlessly. Smart home owners in most cases purchase multiple smart devices, install and then struggle to configure them for many hours and then realize they are not compatible. This is a very frustrating approach to users and definitely not the path to mainstream deployment and adoption. To realize the full potential of smart homes, device manufacturers should develop products that communicate with each other and have a complementary capability as well.

5.4 Model Validation

Model validation is a critical phase in development of any model in research. It is a proof that a proposed model is viable, reliable and accurate in addressing the objectives for which it was designed for. Validation serves as the link between theoretical frameworks and real life application hence increase adoption confidence. Model validation took a multi-faced approach of three options: - Functional testing and scenario-based validation, Scalability benchmarking and Standardized validation frameworks (which is also often called the academic focus framework)

Method 1: Functional Testing and Scenario-Based Validation

Was used to verify whether the model correctly represents different layers of interoperability - device, network, syntactic, semantic, and platform and whether the relationships among them are logical and consistent.

A test scenario was carried out on the model sample device developed. It was subjected to a network with a wi-fi sensor attached to a Bluetooth low energy control switch to see if it was able to send and receive signals through a common gateway, this functional test ensured that it was able to behave as expected.

Scenario-Based validation is an approach which acknowledges that smart homes operate in diverse and dynamic environments, where devices from multiple vendors must coexist, communicate, and adapt to user needs. Scenarios may include situations such as integrating a new IoT device into an existing ecosystem, coordinating responses between sensors and actuators in an emergency (for example smoke detector triggering sirens), or ensuring seamless operation when internet connectivity is disrupted.

A test scenario was used in the sample prototype on device discovery and scalability: When a new additional smart tap from a different manufacturer was introduced and it would integrate with existing infrastructure. What was measured here was the success rate of the device discovery and ability to be added into existing infrastructure without having to change a lot.

Method 2: Standardized validation framework

A Standardized validation framework was also used in validation. This involved the use of an established Interoperability framework. Levels of Conceptual Interoperability Model (LCIM) framework was adopted. The goal of LCIM is to achieve the highest level which is dynamic Interoperability where systems can automatically adapt to changes. LCIM has **seven levels** (from lowest to highest) that represent increasing degrees of interoperability:

Table 5.9: Conceptual Interoperability Model

Level of interoperability	Characteristics	Assessed
Level 0 : No Interoperability	• Systems are completely independent.	Interaction occurs

	• No exchange of data or interaction occurs between them.	
Level 1 : Technical Interoperability	• Systems can exchange raw data using standard technical connections (e.g., network protocols, APIs). • Focuses on the ability to transmit bits and bytes reliably.	Data packets move between systems. Which is true in the scenario implemented.
Level 2 : Syntactic Interoperability	• Data exchanged follows a common structure or format. • Systems understand how the data is organized but not necessarily its meaning.	JSON was implemented to standardize message formats.
Level 3: Semantic Interoperability	• Shared meaning of data between systems. • Agreed-upon definitions, vocabularies, or ontologies are used.	"Open_tap" means dispense for the inlet and the outlet controls

Level 4 : Pragmatic Interoperability	• Systems not only understand the meaning of data but also how it is applied in context. • Contextual rules and intended usage of the information are clear to all parties.	A storage capacity monitor in a tank and a tap dispenser both understand that "tap closed" means water quantity does not change.
Level 5 : Dynamic Interoperability	• Systems adapt to changing contexts, assumptions, or operating conditions. • They can negotiate meanings and adjust operations dynamically.	IoT devices being able to adjust exchange protocols depending on network conditions.
Level 6 : Conceptual Interoperability	• The highest level. • Systems share common conceptual models, underlying assumptions, and constraints.	There exists agreement on the theories, processes, and representations of the world being simulated or operated.

5.5 Chapter Summary

In this chapter, the proposed model is presented and discussed in detail with each element in the proposed model dealt with separately. The chapter interprets the meaning of the

data presented in each table and establishes the key factors that promote or inhibit interoperability in a smart home as an Internet of Things implementation structure. The conclusion from this chapter is that for interoperability to be achieved, Technical, Semantic, Organizational and Legal aspects must agree for interoperability in devices in a smart home. The chapter further demonstrates an implemented project in a real life environment with attached related code in the appendix.

CHAPTER SIX:

DISCUSSION, CONCLUSION AND RECOMMENDATIONS

6.1 Chapter Overview

This chapter discusses the results achieved in the previous chapter as it relates to Emerging technologies and standards such as those that are protocols implemented in the market. The chapter then makes a conclusion of the research and gives some recommendations on possible areas of research, which can add value to the body of knowledge and practice in the field of smart homes and internet of things environment.

6.2 Discussion

Interoperability is an inevitable factor in the current world of technology and therefore aligns with current needs in the industry and technological trends of the future of Internet of Things. The implementation of a section of the model indicates that if adopted it will enhance the model's robustness and contribute to development of devices which are interoperable. Emerging technologies and standards such as those that are protocol based for example MQTT and IFTTT are significant if it is adopted by the regulators. The model also presents a unique advantage in terms of scalability, flexibility, and implementation ease as it takes care of all aspects needed to implement interoperability. The proposed model seeks therefore to fill a gap in interoperability research.

To help simplify or contextualize the model's significance the figure 6.1 below developed by the author summarizes the expectations of implemented model while demonstrating practical and theoretical implications.

Challenges in Implementation of the model include would range from legacy system

integration, data security, and standardization impact deployment now that there are already technical and regulatory barriers to adopting this model in real-world scenarios.

Based on the findings, a conceptual model for interoperability was developed to guide smart home integration. The model incorporates: Device layer which covers Standardized APIs, Knowledgebase compatibility, and communication protocols. Infrastructure and Security layer which addresses reliable connectivity, data routing, and protocol translation. Service layer addresses Messaging platforms, event handling, and composition of device actions. User layer addresses the interfaces for monitoring, configuration, and control, ensuring human factors are addressed.

The model emphasizes a layered and modular approach that enables heterogeneous devices to communicate effectively while maintaining flexibility for future IoT developments. This approach reflects best practices from existing frameworks (e.g., SOA, IFTTT, HAVi) while addressing the gaps identified in the study.

6.3 Conclusion

This study was developed to investigate interoperability among devices with the argument that interoperability of devices have a key role in realizing the IoT, thus a vital need to consider their capabilities in addressing interoperability. The intention is to have an IoT platform that could be able to offer a pool of standardized communication where device manufacturers can work with. The overall objective was to develop a model for the interoperability of devices for Internet of Things architectures in a smart home.

The study based the investigation on the conceptual framework of interoperability and hence the finding that most IoT proposals concentrate on interoperability from a specific perspective rather than providing interoperability among all perspectives within a smart

environment. The proposed interoperability model directly addresses the study objectives by first assessing the current state of device interoperability, then identifying its role in IoT environments, analyzing the factors that influence it, and finally integrating these findings into a structured model that enhances seamless interaction among devices in smart homes.

The specific objective number one was to establish the role of interoperability in smart homes in the Internet of Things environments. Based on the study results and literature, it was observed that enabling interoperability between diverse platforms which have been previously deployed with different technologies and underlying features and possibly from different vendors should be integrated. When a de-facto standard does not exist, it is critical that a uniform protocol is established for all devices. Users are interested in service provision by the devices and therefore quality of service and the criteria for decision-making is key. The model developed therefore meets the basic needs of the users within a heterogeneous environment as well as giving room for expansion of services and updates. It was observed that providing interoperability between IoT devices should not require a major change in systems and the solution should not be dependent on the particular stakeholder's system.

The specific objective number two was to assess the factors that affect interoperability of devices in smart homes in the Internet of Things. The approach taken was to first assess those factors that promote interoperability and those that inhibit or hinder interoperability. Based on the conceptual framework adopted, it was observed that a growing availability of Web Services, Growing availability of data, development and diffusion of more universal Solutions, Novel Machine2Machine technology solutions, Smart phone and Smart objects diffusion and the Need for reduction of costs are all significant in

contributing to the need for interoperability. There was a significant support from literature on the same factors as having been significant in affecting interoperability. The factors that hinder interoperability of devices were also assessed in the research, The factors measured include:- absence of regulations, Profitability of the solutions, High time-to-market for new applications, Broadband network with multimedia capability, Scalability of devices, Security of data and infrastructure, Changing enabling technologies especially the deployment of 5G networks, RFID or Wi-Fi technologies, Vendor device incompatibility, User-centric perceptions, Lack of compelling success stories, Unavailability of testing centers, Non-standardized interfaces or protocols, Equipment from one manufacturer, but with different software revisions resulting in incompatible, Different middleware manufacturers, Complexity of networks through integration of networks and devices requires additional cost of hiring knowledgeable staff in various brands of equipment, There are applications, which are launched by vendors who do not provide infrastructure and support to enable interoperability, Loss of independence among vendors is a threat especially for emergency response service providers, Limitation to Implement new features and services which can run on all platforms inhibit interoperability among vendors, Reduces the need for additional costs and time to solve problems which arise from lack of interoperability, and whether it eliminates the delays of projects caused by difference among vendors, additional costs for upgrades and the extra tests needed after upgrades. All factors seem to have an influence on decisions of whether to promote interoperability or not. It was also observed from the industry that design and deployment of smart homes still at its infancy stage in developing countries.

The specific objective number three was to determine the factors that affect interoperability of devices in smart homes in the Internet of Things. The factors were derived from the conceptual framework, which informed the development of the model. The approach was subdivided into four namely: - Technical, Organizational, Semantic and Legal factors. Technical factors assessed - interconnection procedures, proprietary and non-standard interfaces of Vendors, deployment of terminals that have capacity to integrate emergency reporting and upgrade software on devices. The support for open architectures is key to making interoperability a reality technically. The Semantic factors assessed the communication between devices and conversion of signals to a language that is understood by the devices based on the domain of use. It was seen that home appliances, personal appliances and Facility management devices need a common semantics framework for interoperability to succeed. Organizational metrics assessed include - if standards apply to things users' value, whether Standards workflows are organized to collect required data or not, if there exists a market for a given product, and if there exists a clear direction or priorities. The organizational metrics are significant if interoperability is to be achieved. Legal factors which include the existence of too many standards, Workflow procedures which are not organized to collect required data and the lack of specificity in standards such that there exist too much optionality making exchange impossible. There is a significant aspect of legal frameworks to support interoperability at the manufacturing level. It was established that all these factors need to work together to achieve interoperability.

The fourth specific objective was to develop a model for interoperability in a smart home. Having derived the metrics which affect interoperability the model which consists of

Technical issues which is the ability to have more than one device and related application to send or receive data from each other and execute a given activity in a satisfactory manner without the need for any other intervention, Semantic issues which deals with the capability to authorize services or the devices to be able to interpret the accurate meaning of exchanged content explicitly. Organizational issues involve how more than one organizations collaborate to enable interoperability by having a mechanism to capture customer needs and development of devices and Legal aspects, which address the issue of policy to the manufacturers. The model therefore addresses each independently then combines in one overall structure. There must be an adequate regulatory framework for manufacturers to make interoperability a reality in IoT.

The relationship between the research objectives and data collected revealed that there are numerous design approaches that contribute to the aspect of a house being referred to as smart, the approach in developing countries is heavily on integration of autonomous home-automation systems which face a challenge of control from various independent points and hence difficulty in integration. The companies involved in the smart home markets in developing countries are small start-up companies, which deal with home appliance companies, security applications, infrastructure control applications and therefore are limited in funding which limits their budgets for further expansion of businesses and or investment in research. It can also be derived that smart homes are likely to have substantial privacy and data safety impacts. With the increased number of integrated sensors, the logs of activities in smart home based on stochastic activities and behaviour of users or visitors will be a definite source of big data, which will be accompanied by challenges on privacy and safety matters. The application of basic

information security would considerably escalate the overall level of security in the smart home. The user needs of different property owners or managers in the smart home may be in conflict, for example, a user wants a complex secure platform with simple access controls, which produces a complex environment for security activity.

For interoperability to be achieved in IoT, users require that the introduction of attractive new services be done without having to change the entire infrastructure of the existing structures. The failure to introduce new and attractive services echoes negatively on vendors' competitiveness. The integration should be made easy on plug-and-play format, software updates should also be easily done from either over the air (OTA) or WIFI networks. Users want a provision for monitoring of Quality of Service and service availability as this will reduce unnecessary administrative activities. Since hardware or software updates require additional investments, vendors may need to include contracts and warranties to make users believe their products and increase confidence. Interoperability problems often have a negative impact to vendors on income hence the need to substantially address the issue. From the point view of the IoT vendors, lack of interoperability means that vendors are limited to the IoT device or software offered by a single provider and must stick with it, which will bring the possible risk of higher cost in the long run, product functionality and stability issues. It will be very expensive for start-up companies to support heterogeneous interfaces of all the diverse platforms. From the view of application developers, incompatibility brings adaption of applications to a crossroad and hence prevents cross-platform operations.

The proposed model can be seen from three different contexts: Theoretical, Practical context and Value contribution. Theoretical context where the model is grounded in

interoperability frameworks for instance the Levels of conceptual interoperability model, IoT reference architectures, and smart home standards architectures. Practical context addresses real-world fragmentation in smart home IoT devices (various vendors, standards like Zigbee, Z-Wave, Wi-Fi are considered). Value contribution is where the model provides a structured way to achieve interoperability, guiding designers, policymakers, and homeowners toward integrated IoT ecosystems.

6.4 Recommendations

The study achieved what it was set to accomplish by providing a model that will enable device-level interoperability. The model can be used to guide in development of devices deployed in smart homes as has been established previously of the need for interoperability among different manufacturers. In order to have a higher uptake of smart homes, there is need to address the issues of interoperability among other aspects. Some other aspects that need to be addressed are as indicated in the next paragraphs.

As a multifaceted interconnected system, smart homes will require users to be further educated in home so as to be able to operate their smart home safely and maintain their anticipated levels of privacy and data protection. The consideration of training should include the reasonable behaviour expected from users for smart home functionality to be achieved.

A further development of good practices needs to be addressed by researchers and vendors. The earlier known good practices address some areas of smart home security, and if deployed more widely would have substantial impact. Good practices for sharing and expanding smart home accommodation should be further developed and explored.

There is need to develop an interface between the smart home and the smart city. Existence of multiple smart homes leads to development of smart residential estates and eventually smart cities. The smart cities have been seen to be developing in parallel with smart homes and employ some shared technologies. There is need to assess the extent at which smart homes and the smart cities are connected, integrated or communicating and hence extend interoperability. Aspects of Security management like approaches to patching, updates, relay of information to mobile networks and incident determination and logging should be developed so that it can cater for particular smart home needs. It is worth noting that it is still too early in developing countries to fully understand the implications of smart homes. This calls for a long-term study on practical implications on privacy, security failures, reporting failures and hence supplement or expand the information available for trend mapping.

Although both the deployment of semantic technologies are at fairly embryonic stages, there is a growing understanding that shared approaches to semantic interoperability is one of the keys to cracking the potential of interoperability in IoT. On the matters of Naming of devices, it is recommended that manufacturers should adopt naming conventions, which enforce minimum changes should need arise in upgrading or deployment of new services, names with spaces in strings should be replaced with underscores, the use of lower-case ontologies for metadata is recommended for ease of use, and use mixed-case for property names to make semantics easily understood. Realizing interoperability will require collaboration across standards organizations, associations, treaties, and open source projects. The need for a shared roadmap and commitment to work together is inevitable.

IoT ecosystem on the interoperability frameworks should deliberate linking more than two platforms. The solutions should be scalable with the possibility to add additional platforms whenever new platforms are developed.

Improving interoperability in IoT is central for the accomplishment of IoT.

6.5 Future Work

The following section proposes some of the research areas, which are open for further investigations or research in order to enrich the body of knowledge in interoperability of devices in the Internet of Things environment.

1. **Development of Interoperability Testing Solution**

   Currently the process of testing the success of a solution comprises the stakeholders who include vendors, developers and service providers who do a face-to-face meeting to validate their implementation alongside existing standards. The process is therefore labor-intensive. This study is intended to develop a testing tool and standards to solve the different types of interoperability. Interoperability testing needs to be programmed so as to motivate developers to create interoperable solutions.

2. **Modelling smart home response to natural disasters**

   This study should seek to determine the impacts and options for smart homes in the resilience of smart homes at the face a natural disaster such as earthquakes, floods, strong wind or fire. The research should consider the way in which smart homes may be designed to mitigate impacts of natural disasters.

3. **Modelling smart homes and emergency response.**

The study should assess the extent at which smart homes be designed to support emergency responses, either in the context of information sharing, incident response, additional difficulties caused by smart home systems during emergency response and if it would call for a different approach in design. The same could compare with how computing opens up for new types of crime, how the smart home will react upon criminal behaviour as opposed to emergency.

4. **Integration of Smart homes with critical infrastructure.**

   The research should focus on association with other critical infrastructure like smart grids. It should assess how smart home can contribute to the protection of this infrastructure.

5. **Law, policy and the smart home.**

   The study could include the extent to which existing laws and policies are guiding or affecting deployment of smart homes. How the laws and policies affect smart home security, cyber security policies and international law on cyber conflict advances should be given consideration particularly for smart homes [52].

6. **Power Generation and Storage**

   The study could look at how smart homes can generate solar power during the day and store it for use at night especially in developing countries many of which are found in the tropics and have sunshine for at least ten hours a day throughout the year.

Chapter Summary

This section synthesized the results achieved in the previous chapters as it relates to the objectives of the study. The discussion highlighted how interoperability is influenced by technical, semantic, legal, and organizational factors, and how these dimensions interact to either facilitate or hinder device integration. The chapter then makes a conclusion of the research and gives some recommendations on possible areas of research, which can add value to the body of knowledge and practice in the field of smart homes and internet of things environment.

References

[1] Gmelin, J. H., Peter de Jonge, and E. S. Kunnen. "“I’m Totally Different”-Developmental Processes Underlying the Recurrent Construction of Identity Content Within Everyday Interactions." Emerging Adulthood 13, no. 2, 2025.

[2] Al Tareq, Abdulla, Md Riad Mostofa, Md Juel Rana, and Md Sadiqur Rahman. "A Comprehensive Review of Intelligent Home Automation Systems Using Embedded Devices and IoT." Control Systems and Optimization Letters 2, no. 2 2024.

[3] Al-Fuqaha, Ala, et al. "Internet of things: A survey on enabling technologies, protocols, and applications." IEEE communications surveys & tutorials 17.4 (2015).

[4] Karunarathna, Indunil, P. Gunasena, T. Hapuarachchi, and S. Gunathilake. "The crucial role of data collection in research: Techniques, challenges, and best practices." Uva Clinical Research 2024.

[5] Hossain, M., Kayas, G., Hasan, R., Skjellum, A., Noor, S., & Islam, S. R. A Holistic Analysis of Internet of Things (IoT) Security: Principles, Practices, and New Perspectives. Future Internet, 16(2), 40. 2024.

[6] Magara, T. and Zhou, Y., 2024. Internet of things (IoT) of smart homes: privacy and security. Journal of Electrical and Computer Engineering, p.7716956, 2024,

[7] K. Ashton, "That ‘internet of things’ thing.," RFiD Journal, Vols. 22(7),, pp. 97-114., 2009.

[8] Atzori, L., A. Iera, and G. Morabito. "" The internet of things: A survey," Computer Networks, vol. 54, no. 15, pp. 2787-2805." (2010)2010.

[9] Baldini, Gianmarco, et al. "Internet of things privacy, security and governance." Internet of Things. River Publishers, 2022.

[10] J. Bélissent, "Getting clever about smart cities: New opportunities require new business models.," *Cambridge, Massachusetts, USA. ,* 2010.

[11] Bello, Oladayo, Sherali Zeadally, and Mohamad Badra. "Network layer inter-operation of Device-to-Device communication technologies in Internet of Things (IoT)." Ad Hoc Networks 57. 2017..

[12] Bassbouss, Louay, et al. "Semantic interoperability for the web of things." ResearchGate Online resource (2016).

[13] Cherbal, Sarra, Abdelhak Zier, Sara Hebal, Lemia Louail, and Boubakeur Annane. "Security in internet of things: a review on approaches based on blockchain, machine learning, cryptography, and quantum computing." The Journal of Supercomputing 80, no. 3: 3738-3816. 2024

[14] J. Creswell, "Educational research: Planning, conducting, and evaluating quantitative and qualitative research.," *Upper Saddle River, NJ: Prentice Hall..*

[15] Trangbæk, Amalie, and Mathilde Cecchini. "Using the interpretivist methodology." Handbook on Ministerial and Political Advisers. Edward Elgar Publishing. 2023

[16] Y. Chaudhary Sajjad Hussain, "Ubiquitous Service Discovery in Pervasive Computing Environment.," *Information Technology Journal,* vol. 7: , pp. 533-536., 2008.

[17] Gubbi, Jayavardhana, et al. "Internet of Things (IoT): A vision, architectural elements, and future directions." *Future generation computer systems* 29.7. 2013.

[18] H. Zhao, "Harnessing the Internet of Things for Global Development. CISCO publication.," *International Telecommunication Union Place des Nations CH-1211*

Geneva. Switzerland, 2016.

[19] Padmavathi, V., and R. Saminathan. "Security for the Internet of Things." In Computer and Information Security Handbook, pp. 353-368. Morgan Kaufmann, 2025.

[20] Lakshminarayana, Sujitha, Amit Praseed, and P. Santhi Thilagam. "Securing the IoT application layer from an MQTT protocol perspective: Challenges and research prospects." IEEE Communications Surveys & Tutorials 2024.

[21] J. Buckley., "The Internet of Things: From RFID to the Next-Generation Pervasive Networked Systems," *Auerbach Publications, New York,* 2006.

[22] G. C. N. C. Synnott J., "The Intelligent Environment Experiment Assistance Tool to Facilitate Partial Environment Simulation and Real-Time Activity Annotation.," *In: García C., Caballero-Gil P., Burmester M., Quesada-Arencibia A. (eds) Ubi,* 2016.

[23] Vermesan, Ovidiu, Peter Friess, Patrick Guillemin, Sergio Gusmeroli, Harald Sundmaeker, Alessandro Bassi, Ignacio Soler Jubert et al. "Internet of things strategic research roadmap." In Internet of things-global technological and societal trends from smart environments and spaces to green ICT, pp. 9-52. River Publishers, 2022.

[24] Babar, Sachin, et al. "Proposed security model and threat taxonomy for the Internet of Things (IoT)." International Conference on Network Security and Applications. Berlin, Heidelberg: Springer Berlin Heidelberg, 2010.

[25] D. K. M. Tanmaya Kumar Das, "Addressing the Influencing Factors for Interoperability in a Global Domain.," *OSR Journal of Computer Engineering (IOSRJCE) publication.,* 2012.

[26] P. Urien, "LLCPS: A New Secure Model For Internet of Things Services Based On The NFC P2P Model," in *IEEE Ninth International Conference on Intelligent Sensors*, 2014.

[27] Rubí, Jesús Noel Suárez, and Paulo Roberto de Lira Gondim. "IoT-based platform for environment data sharing in smart cities." International Journal of Communication Systems 34, no. 2 2021.

[28] Vermesan, Ovidiu, Peter Friess, Patrick Guillemin, Harald Sundmaeker, Markus Eisenhauer, Klaus Moessner, Franck Le Gall, and Philippe Cousin. "Internet of things strategic research and innovation agenda." In Internet of things, pp. 7-151. River Publishers, 2022.

[29] M. Corporation, "Chapter 1: Service Oriented Architecture (SOA).," Microsoft, 2017. [Online]. Available: msdn.microsoft.com.. [Accessed 18 11 2022].

[30] Dhinakaran, D., S. M. Sankar, Dharani Selvaraj, and S. Edwin Raja. "Privacy-preserving data in IoT-based cloud systems: A comprehensive survey with AI integration." arXiv preprint arXiv:2401.00794 2024.

[31] Hmissi, Fatma, and Sofiane Ouni. "A survey on application layer protocols for iot networks." arXiv preprint arXiv:2405.15901 , 2024.

[32] R. G. Ronak Sutaria, "Making sense of interoperability: Protocols and Standardization initiatives in IOT.," *Mindtree Research Labs publication, Bengaluru, India.,* 2013.

[33] Ajithraj, R. A., and Narendran Rajagopalan. "A method of preventing endpoint exploits in healthcare with block-chain token authorization implementation in SDN stack." In AIP Conference Proceedings, vol. 3031, no. 1. AIP Publishing, 2024.

[34] Bandyopadhyay, Soma, et al. "A survey of middleware for internet of things." International Conference on Computer Networks and Communications. Berlin, Heidelberg: Springer Berlin Heidelberg, 2011.

[35] Bharathi, M., M. Dharani, Sivaram Rajeyyagari, and B. M. Rajeswari. "An Investigation of Future Research Directions In Secure Internet of Things Systems and Applications." Innovations in Computational Intelligence, Big Data Analytics and Internet of Things. 2024.

[36] S. Corporation, "An Internet of Things Reference Architecture.," *Symantec publicaion,* 2016.

[37] Terziyan, Vagan, Olena Kaykova, and Dmytro Zhovtobryukh. "Ubiroad: Semantic middleware for context-aware smart road environments." *2010 Fifth international conference on internet and web applications and services*. IEEE, 2010.

[38] Safari, Sepideh, Mohsen Ansari, Heba Khdr, Pourya Gohari-Nazari, Sina Yari-Karin, Amir Yeganeh-Khaksar, Shaahin Hessabi, Alireza Ejlali, and Jörg Henkel. "*A survey of fault-tolerance techniques for embedded systems from the perspective of power, energy, and thermal issues*." *IEEE Accessed* 10 2022.

[39] Azad, Tanzima, MA Hakim Newton, Jarrod Trevathan, and Abdul Sattar. "IoT edge network interoperability." Computer Communications 236, 2025

[40] Noura, Mahda, Mohammed Atiquzzaman, and Martin Gaedke. "Interoperability in internet of things: Taxonomies and open challenges." *Mobile networks and applications* 24.3. 2019.

[41] Hussein, AbdelRahman H. "Internet of things (IOT): Research challenges and future applications." *International Journal of Advanced Computer Science and*

Applications 10.6 2019.

[42] Golestan, Shadan, Eleni Stroulia, and Ioanis Nikolaidis. "Smart indoor space simulation methodologies: A review." *IEEE Sensors Journal* 22.9 2022.

[43] ITU, "Report on the results of the Questionnaire on the status of Conformance," in *Regional ITU Consultation on Conformance Assessment and Interoperability for the Africa Region*, Nairobi, 2010.

[44] Harkness, Geoff. "Research methods." In DVS Mindz, pp. 321-326. Columbia University Press, 2023.

[45] Rose, Karen, Scott Eldridge, and Lyman Chapin. "The internet of things: An overview." *The internet society (ISOC)* 80.15 2015.

[46] Fernandez-Gago, Carmen, Davide Ferraris, Rodrigo Roman, and Javier Lopez. "Trust interoperability in the Internet of Things." Internet of Things 26, 2024

[47] M. Swan, " Sensor mania! the internet of things, wearable computing, objective metrics, and the quantified self," *Journal of Sensor and Actuator networks,* pp. 217-253., 2012.

[48] Denny, Elaine, and Annalise Weckesser. "How to do qualitative research? Qualitative Research Methods." Bjog 129, no. 7. 2022.

[49] Rossi, Sippo, Matti Rossi, Raghava Rao Mukkamala, Jason Bennett Thatcher, and Yogesh K. Dwivedi. "Augmenting research methods with foundation models and generative AI." International Journal of Information Management 77. 2024

[50] Sen, Jaydip, ed. *Internet of things: Technology, applications and standardization*. BoD–Books on Demand, 2018.

[51] Ahmadin, Mr. "Social research methods: Qualitative and quantitative

approaches." Jurnal Kajian Sosial Dan Budaya: Tebar Science 6, no. 1 2022.

[52] Yong, Wooi Keong, Md Husin Maizaitulaidawati, and Suzilawati Kamarudin. "Understanding research paradigms: A scientific guide." *Journal of Contemporary Issues in Business and Government* 27, no. 2 2021.

[53] Irsova, Zuzana, Hristos Doucouliagos, Tomas Havranek, and Tom D. Stanley. "Meta-analysis of social science research: A practitioner's guide." Journal of Economic Surveys 38, no. 5. 2024.

[54] Bassbouss, Louay, et al. "Semantic interoperability for the web of things." ResearchGate Online resource. 2016.

[55] Jakobi, T., Ogonowski, C., Castelli, N., Stevens, G., & Wulf, V. The catch (es) with smart home: Experiences of a living lab field study. In Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems (pp. 1620-1633).2017.

[56] Mahamure, Sandesh. "Communication protocol and queuing theory-based modelling for the internet of things." *Journal of ICT standardisation* 2016.

[57] Barnard-Wills, D., L. Marinos, and S. Portesi, *Threat Landscape and Good Practice Guide for Smart Home and Converged Media,* European Union Agency for Network and Information Security, 2014.

[58] Susanto, Primadi Candra, Lily Yuntina, Euis Saribanon, Josua Panatap Soehaditama, and Esti Liana. "Qualitative method concepts: Literature review, focus group discussion, ethnography and grounded theory." Siber Journal of Advanced Multidisciplinary 2, no. 2 2024.

[59] Andreas, Tolk, and J. A. Muguira, The levels of conceptual interoperability model., in *Proceedings of the 2003 fall simulation interoperability workshop.*, Citeseer.

[60] PhDStudent.com, "Writing Assumptions, Limitations, and Delimitations," 2021. [Online]. Available: https://www.phdstudent.com/thesis-and-dissertation-survival/research-design/stating-the-obvious-writing-assumptions-limitations-and-delimitations/#:~:text=One%20of%20the%20more%20common,of%20honesty%20and%20truthful%20responses.&text=For%20example%2C%20as. [Accessed 29 March 2021].

[61] R. Gallery, "Understanding the Smart Home Concept," 2018. [Online]. Available: http://www.rocagallery.com/smart-interiors#:~:text=The%20main%20characteristics%20of%20a,of%20elements%20in%20the%20home.&text=One%20additional%20aspect%20worth%20explaining,Internet%20of%20Things%2C%20or%20IoT.. [Accessed 29 March 2021].

[62] Taj, Summia, et al. "Interoperability in IOT based smart home: A review." *Journal homepage: http://iieta. org/Journals/RCES* 5.3 (2018): 50-55..

[63] Koo Jahoon, "Interoperability of device identification in heterogeneous IoT platforms," in *Computer Engineering Conference (ICENCO)*, 13th International 26-29. IEEE, 2017.

[64] Kraijak s. and P. Tuwanut, "A survey on internet of things architecture, protocols, possible applications, security, privacy, real-world implementation and future trends," in *International Conference on Communication Technology (ICCT)*, IEEE, 2015.

[65] Kostelic, C. "Applying the Levels of Conceptual Interoperability Model to a Digital Library Ecosystem – a Case Study," in *Proc. Int'l Conf. on Dublin Core and Metadata Applications* , Dublin , 2017.

[66] Yang, C., Yuan, B., Tian, Y., Feng, Z. and Mao, W, "A smart home architecture based on resource name service," in *IEEE 17th International Conference*, IEEE , 2014.

[67] Koo, Jahoon, and Young-Gab Kim. "Interoperability of device identification in heterogeneous IoT platforms.," in *Computer Engineering Conference (ICENCO)*, IEEE, 2017.

[68] Soliman, M., Abiodun, T., Hamouda, T., Zhou, J., & Lung, C. H, "Smart home: Integrating internet of things with web services and cloud computing," in *International Conference on Cloud Computing Technology and Science*, IEEE, 2013.

[69] Seo, Sangwon, Jaehong Kim, Sangbae Yun, Jaehyuk Huh, and Seungryoul Maeng., "HePA: hexagonal platform architecture for smart home things. In Parallel and Distributed Systems," in *IEEE 21st International Conference*, IEEE , 2015.

[70] Palma, Lorenzo, Luca Pernini, Alberto Belli, Simone Valenti, Lorenzo Maurizi, and Paola Pierleoni, "IPv6 WSN solution for integration and interoperation between smart home and AAL systems.," in *Sensors Applications Symposium*, IEEE, 2016.

[71] Toschi, Guilherme Mussi, Leonardo Barreto Campos, and Carlos Eduardo Cugnasca., "An upnp architecture for interoperability in home area network.," in *Consumer Electronics* , IEEE, 2016.

[72] Perumal, Thinagaran, Abdul Rahman Ramli, Chui Yew Leong, Shattri Mansor, and Khairulmizam Samsudin, "Interoperability for smart home environment using web services," *International Journal of Smart Home,* vol. 2, no. 4, pp. 1-16, 2008.

[73] DeNardis, Laura, and Mark Raymond, "The internet of things as a global policy frontier.," *UCDL Rev. 51,* p. 475, 2017.

[74] Zhao, Kexin, and Mu Xia., "Forming Interoperability Through Interorganizational Systems Standards," *Journal of Management Information Systems ,* vol. 30, no. 4, pp. 269-298, 2014.

[75] S. Solutions, "Factor Analysis," [Online]. Available: https://www.statisticssolutions.com/free-resources/directory-of-statistical-analyses/factor-analysis/. [Accessed 12 06 2022].

[76] Hossain, Mahmud, Golam Kayas, Ragib Hasan, Anthony Skjellum, Shahid Noor, and SM Riazul Islam., “A Holistic Analysis of Internet of Things (IoT) Security: Principles, Practices, and New Perspectives. Future Internet,," MDPI , 2024.

[77] Sundmaeker, Harald, Patrick Guillemin, Peter Friess, and Sylvie Woelfflé Sundmaeker, "Vision and Challenges for Realising the Internet of Things.," *CERP IoT,* 2010..

[78] Padmavathi, V. and Saminathan, R., "Security for the Internet of Things. In Computer and Information Security Handbook," in *Computer and Information Security Handbook*, Morgan Kaufmann., 2025, pp. 353-368.

7.0 Appendix 1 :

7.1 Questionnaire for Users/ Tenants.

Dear Respondent,

You are requested to help in filling this questionnaire on Interoperability Architecture in Smart Homes Based on Internet of Things. Any information provided will be treated in confidence and will not be used in any other resolve other than the research study strictly.

Biodata

1. Gender [] Male [] Female
2. Age in years [] 25 -34 [] 35-44 [] 45-54 []55-64 [] above 65
3. Level of Education [] Primary []Secondary [] Diploma [] Bachelor's Degree [] Postgraduate
4. For how long have you lived in a smart home environment?

   [] 0-4 [] 5-9 [] Over 10 Years

5. Use the scale below to answer the questions that follow:

   5 – Strongly Agree

   4- Agree

   3- Neither Agree nor Disagree

   2- Disagree

   1 – Strongly Disagree

The state of device interoperability in Smart Homes.

The following devices communicate seamlessly in my home:-

Smart doors	Smart switches	Intruder alarms	fire alarms	Flood alarms	Lighting	Ventilation	Air conditioning

Home

appliances

eg

Refrigerator

Personal

appliances

The following devices in the support interoperability with the Home appliances

Refrigerator Television Cooker Water Heaters

Facility

management

services

Personal

appliances

Role of interoperability in smart homes in the Internet of Things environments.

The role of Interoperability among devices promote the following:-

	5	4	3	2	1
Quality of Service					
Response to services in emergencies.					
Reduce costs of deployment of solutions					
Allow for introduction of attractive services to integrate existing and new services					

Reduction of unnecessary administrative activities					
Eliminate the need to frequently do software modifications and/or addition of new elements.					
Eliminates discrepancy of operators' expectations in relation to integration with existing elements.					
Allows the introduction of attractive services hence reflects positively on vendor's competitiveness;					
Eliminate hitches which may negatively impact income of vendors.					
Interoperability consolidates continuous service, while maintaining access to the applications					
Interoperability affects the criteria for decision making					

6. Factors that facilitate or inhibit interoperability of devices in smart homes in the Internet of Things.

a) The following factors promote interoperability among devices:-

	5	4	3	2	1
Need for reduction of costs					
Growing availability of Web Services					

Growing availability of data					
More universal Solutions					
Novel machine2Machine technology solutions					
Smart phone and Smart objects diffusion					

b) The following factors inhibit interoperability among devices:-

	5	4	3	2	1
Lack of regulations					
Profitability of the solutions					
High time-to-market for new applications					
Broadband network - Capacity for transmission of multimedia when users add much to the network.					
Scalability of devices					
Security issues					
Changing enabling technologies such as 3g to 4G and 5G networks, RFID, Wifi					
Vendor device incompatibility					
User-centric perceptions					
Lack of compelling success stories and Unavailability of testing centres					
Non-standardized interfaces or protocols					
Equipment from one manufacturer, but with					

different software revisions resulting in incompatibility					
Different middleware manufacturers					
Complexity of networks through integration of networks and devices requires additional cost of hiring knowledgeable staff in various brands of equipment.					
There are applications, which are launched by vendors who do not provide infrastructure and support to enable interoperability.					
Loss of independence among vendors is a threat especially for emergency response service providers					
Limitation to Implement new features and services which can run on all platforms inhibit interoperability among vendors.					
Reduces the need for additional costs and time to solve problems which arise from lack of interoperability.					
Eliminates the delays of projects caused by difference among vendors, additional costs for upgrades and the extra tests needed after upgrades					

7.2 Questionnaire for Experts/ Dealers/ Vendors of Smart Home devices.

Dear Respondent,

You are requested to help in filling this questionnaire on Interoperability Architecture in Smart Homes Based on Internet of Things. Any information provided will be treated in confidence and will not be used in any other resolve other than the research study strictly.

Biodata

1. Gender [] Male [] Female
2. Age in years [] 25 -34 [] 35-44 [] 45-54 []55-64 [] above 65
3. For how long have you dealt with deployment of smart homes?

   [] 0-4 [] 5-9 [] Over 10 Years

State of Interoperability of Devices in Developing Countries

I have come across the devices that support interoperability:-

5 – Strongly Agree

4- Agree

3- Neither Agree nor Disagree

2- Disagree

1 – Strongly Disagree

	5	4	3	2	1
Home appliances eg Refrigerator					
Personal Appliances					
Facility Management Services					
Personal appliances					

Technology: Determining Interoperability Requirements

Metrics used in developing device interoperability for smart homes in the Internet of Things.

State how you rate the truth of the following statements:-

	5	4	3	2	1
If interoperability of the networks is required of the vendors then, the technical problems are deterred during the interconnection procedures					
The main interoperability problems are due to proprietary and non-standard interfaces of Vendors.					
Vendors deploy terminals that have no function for emergency reporting.					
How to update newer software on devices will be a non-issue if devices are made to be interoperable.					

I would support the following devices to support **open architectures**:-

5 – Strongly Agree

4- Agree

3- Neither Agree nor Disagree

2- Disagree

1 – Strongly Disagree

5 4 3 2 1

Health parameters;

Tracking of objects

Learning capability of devices

Naming

System diagnostics

Security

Semantics

5. The following devices should be able to communicate:-

	Smart doors	Smart switches	Intruder alarms	fire alarms	Flood alarms	Lighting	Ventilation	Air conditioning
Home appliances eg Refrigerator								
Personal appliances								

6. The following devices in the sensing layer must support interoperability with the Home appliances?

	Refrigerator	Television	Cooker	Water Heaters
Facility				

management

services

Personal

appliances

7. Which devices in the Intelligence category need to support interoperability?

	Learning capability	Topology	Naming	Security	System diagnostics
Home appliances					
Facility management services					
Personal appliances					

8. In your opinion, which of the following devices in the Personal appliances category need to support interoperability?

Health parameters Tracking of objects

Home appliances

Facility management services

Legal

9. In your opinion what are the reasons why interoperability has stalled?

	5	4	3	2	1
Too many standards					
Lack of specificity in standards (not constrained), too much optionality makes exchange impossible					

Organizational

10. In your opinion what are the reasons why interoperability has stalled?

	5	4	3	2	1
Standards don't apply to things I value					
Standards Workflows are not organized to collect required data					
Not clear if market is there for a product					
Lack of clear direction or priorities					

Any other observations?

7.3: Interview/ Experiment Checklist

	Smart doors	Smart switches	Intruder alarms	Fire alarms	Flood alarms	Lighting	Ventilation	Air conditioning
Home appliances eg Refrigerator								
Personal appliances								

Any other observations?

_____

_____

8.0 Appendix 2 : Sample Pseudcode in a device

```
BEGIN AQUAVENDOR_SOLUTION

// Initialization

INITIALIZE Broker

INITIALIZE Database

INITIALIZE MessageFormatRegistry



// API Setup for Developer

FUNCTION registerTopics(topicList):

   FOR EACH topic IN topicList:

      IF topic.mode == "publish":

         ADD topic TO Broker.publishTopics

      ELSE IF topic.mode == "subscribe":

         ADD topic TO Broker.subscribeTopics

      ENDIF

   ENDFOR

END FUNCTION



// Device Registration

FUNCTION registerDevice(deviceID, supportedTopics):
```

```
    FOR EACH topic IN supportedTopics:
        IF topic IN Broker.subscribeTopics:
            SUBSCRIBE deviceID TO topic
        ELSE IF topic IN Broker.publishTopics:
            ALLOW deviceID TO publish TO topic
        ENDIF
    ENDFOR
END FUNCTION

// Message Flow
FUNCTION publishMessage(deviceID, topic, message):
    IF topic NOT IN Broker.publishTopics:
        RETURN "ERROR: Invalid publish topic"
    ENDIF

    // Validate message format
    IF validateMessage(message) == TRUE:
        Broker.broadcast(topic, message)
    ELSE
        RETURN "ERROR: Invalid message format"
```

```
    ENDIF
END FUNCTION

FUNCTION subscribeHandler(deviceID, topic):
    WHILE TRUE:
        IF Broker.hasNewMessage(topic):
            message ← Broker.getMessage(topic)
            processMessage(deviceID, message)
        ENDIF
    ENDWHILE
END FUNCTION

// Message Validation
FUNCTION validateMessage(message):
    IF message.type IN MessageFormatRegistry:
        RETURN TRUE
    ELSE
        RETURN FALSE
    ENDIF
END FUNCTION
```

```
// Message Processing
FUNCTION processMessage(deviceID, message):
    // Parse payload
    parsedData ← parsePayload(message.type, message.payload)
    // Store in database or logs
    STORE parsedData INTO Database
    // Trigger actuator if required
    IF message.type IS linkedToActuator:
        actuatorTopic ← getActuatorTopic(message.type)
        newMessage ← buildActuatorCommand(parsedData)
        Broker.broadcast(actuatorTopic, newMessage)
    ENDIF
END FUNCTION
// Example Scenario: Operator presses button
EVENT buttonPress(operatorID, amount):
    message.type ← "DISPENSE_REQUEST"
    message.payload ← { "amount" : amount }
    publishMessage(operatorID, "water/dispense", message)
END EVENT
END AQUAVENDOR_SOLUTION
```

9.0Appendix 3:

Time Plan

	2018 - Dec 2018	January – April 2019	May – June 2019	June – Dec 2020	2021	2024	2025
Proposal							
Research Design							
Testing and Analysis							
Reporting							
Documentation							
Corrections							
Final Copy							

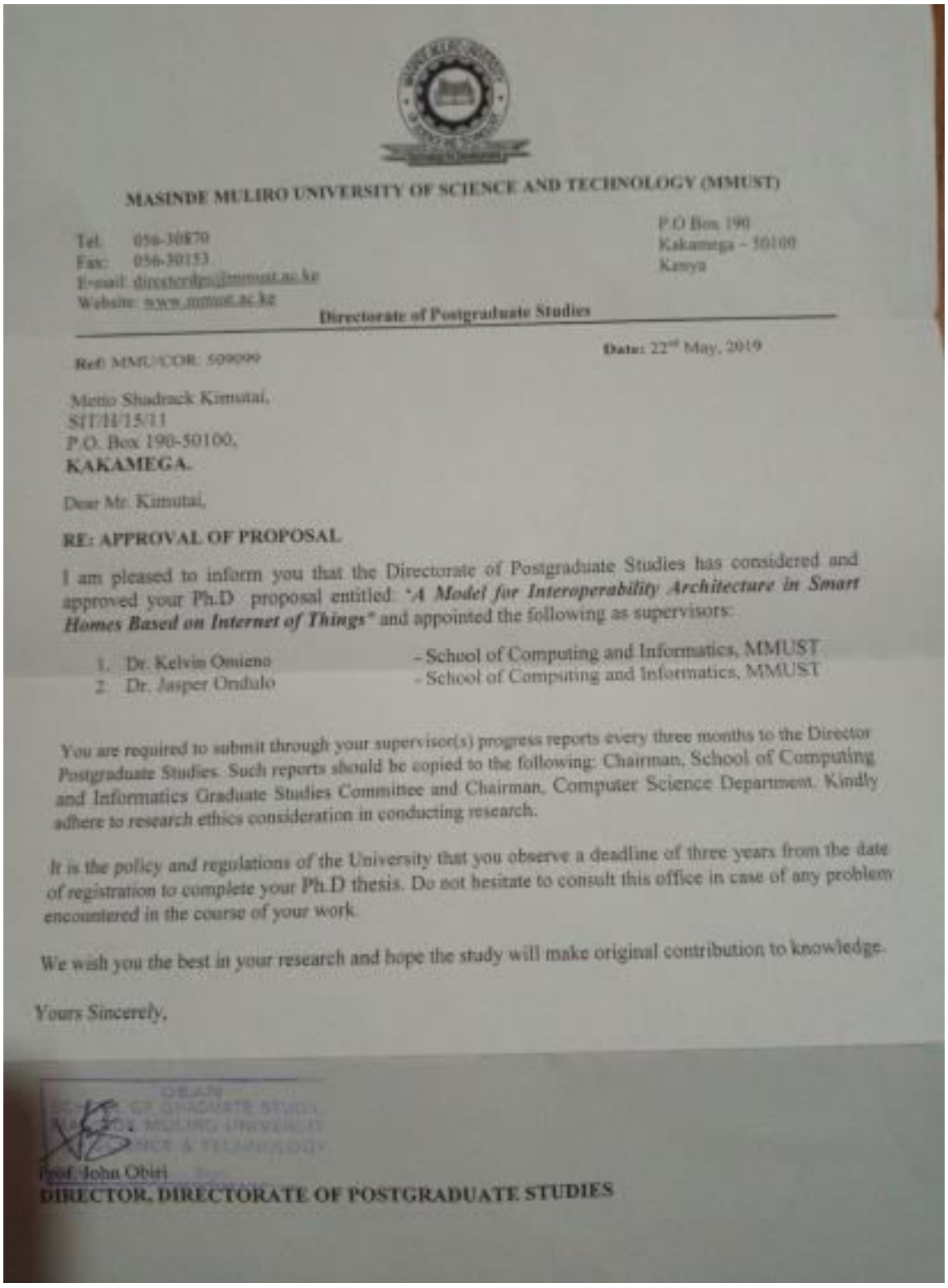
9.1 Research Budget

This section summarizes the major budgetary requirements for the research.

	ITEM	UNIT COST		TOTAL
1	Literature review (Journals subscription, books)			120,000
2	Research Assistant Allowance	10,000	3 Months	30,000
3	Stationery			70,000
4	Software Tools			300,000
5	Travel and Subsistence			200,000
6	Model Design and Testing			100,000
Total				**820,000**

APPENDICES

APPENDIX 1 RESEARCH AUTHORIZATION LETTER FROM THE UNIVERSITY



MASINDE MULIRO UNIVERSITY OF SCIENCE AND TECHNOLOGY (MMUST)

Tel: 056-30870
Fax: 056-30153
E-mail: directordgs@mmust.ac.ke
Website: www.mmust.ac.ke

P.O Box 190
Kakamega – 50100
Kenya

Directorate of Postgraduate Studies

Ref: MMU/COR: 509099

Date: 22nd May, 2019

Metto Shadrack Kimutai,
SIT/H/15/11
P.O. Box 190-50100,
KAKAMEGA.

Dear Mr. Kimutai,

RE: APPROVAL OF PROPOSAL

I am pleased to inform you that the Directorate of Postgraduate Studies has considered and approved your Ph.D proposal entitled: "***A Model for Interoperability Architecture in Smart Homes Based on Internet of Things***" and appointed the following as supervisors:

1. Dr. Kelvin Omieno - School of Computing and Informatics, MMUST
2. Dr. Jasper Ondulo - School of Computing and Informatics, MMUST

You are required to submit through your supervisor(s) progress reports every three months to the Director Postgraduate Studies. Such reports should be copied to the following: Chairman, School of Computing and Informatics Graduate Studies Committee and Chairman, Computer Science Department. Kindly adhere to research ethics consideration in conducting research.

It is the policy and regulations of the University that you observe a deadline of three years from the date of registration to complete your Ph.D thesis. Do not hesitate to consult this office in case of any problem encountered in the course of your work.

We wish you the best in your research and hope the study will make original contribution to knowledge.

Yours Sincerely,

Prof. John Obiri
DIRECTOR, DIRECTORATE OF POSTGRADUATE STUDIES

APPENDIX 2 NATIONAL COUNCIL FOR SCIENCE AND TECHNOLOGY CLEARENCE LETTER

REPUBLIC OF KENYA

NATIONAL COMMISSION FOR SCIENCE,TECHNOLOGY & INNOVATION

Ref No: 637728

Date of Issue: 29/May/2020

RESEARCH LICENSE

This is to Certify that Mr.. METTO KIMUTAI SHADRACK of Masinde Muliro University of Science and Technology, has been licensed to conduct research in Kisumu, Nairobi, Nandi, Uasin-Gishu on the topic: A Model for Interoperability Architecture in Smart Homes Based on Internet of Things for the period ending : 29/May/2021.

License No: NACOSTI/P/20/5063

637728

Applicant Identification Number

Director General
NATIONAL COMMISSION FOR SCIENCE,TECHNOLOGY & INNOVATION

Verification QR Code

NOTE: This is a computer generated License. To verify the authenticity of this document, Scan the QR Code using QR scanner application.