ADOPTION AND USE OF INTERNET OF THINGS AND THE IMPLICATIONS FOR ADAPTIVE REGULATION

Boipelo Jarvis

Student Number: 2275485

Supervisor: Dr Ntsibane Ntlatlapa

A research report submitted to the Faculty of Humanities, University of the Witwatersrand, in partial fulfilment of the requirements for the degree of Master of Arts in the field of ICT Policy and Regulation.

March 2024

ABSTRACT

Internet of Things (IoT) is evolving, developing and finding use in many industries where it is mainly used for automating, controlling, tracking and monitoring of different assets and processes, and also to digitalise and optimise business processes. One of IoT's main characteristics is the interconnection of physical and virtual objects, the involvement of various stakeholders and the vast amount of data that is collected, communicated, stored and analysed in its ecosystem. IoT is projected to continue on its tremendous growth path for years to come, and to also permeate many more industries. However, IoT has inherent challenges of security and privacy due to its characteristics and therefore requires relevant regulation so as to address the challenges related to it and enable its continued growth, adoption and use.

The study explored the adoption and use of IoT in South Africa, looked into security and privacy challenges for IoT and ways to address them, ways in which current regulatory approaches are affecting IoT and how regulation that is relevant to IoT can be developed. The researcher followed a qualitative research approach, collected data from participants through in-depth interviews and employed thematic analysis to discover themes from data that was collected. The study's findings are categorised according to three themes that emerged from the literature review namely: adoption and use of IoT, security and privacy challenges for IoT and ways to develop adaptive regulation for IoT. The Socio Technical Systems (STS) framework was a theoretical lens that was used to analyse data by mapping the study's findings against STS components to explore the social and technical aspects of IoT. To define and understand the relationship between the social and technical subsystems of STS, an interaction between the elements of these two subsystems namely technology, tasks, structure and people was done.

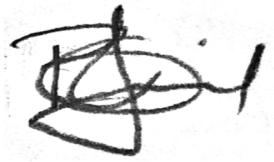
Under the technical subsystem, the findings brought to light the challenge that interoperability, security and privacy has on the adoption and use of IoT and the activities that enable the adoption and use of IoT. The findings under the social subsystem highlighted regulatory measures that are required to enable the adoption and use of IoT, regulatory ways to address the challenges of security and privacy as well as the need for IoT stakeholders to work collaboratively to encourage the growth, adoption and use of IoT and to address challenges related to it. The interaction of the STS elements identified collaborations and collaborative mechanisms as ways to address the challenges of IoT and develop regulation that is adaptive to its development.

Based on the researcher's analysis IoT requires a collaborative approach to address the challenges that its development, adoption and use are confronted with and to also develop regulation that is relevant and encouraging of its adoption and use.

Keywords: Evolving technology, Adoption and use, Security and privacy, Adaptive regulation, Collaboration.

DECLARATION

I declare that this report is my own, unaided work. It is submitted in partial fulfilment of the requirements of the degree of Master of Arts in the field of ICT Policy and Regulation in the University of the Witwatersrand, Johannesburg. It has not been submitted before for any degree or examination in any other University.



_____

Boipelo Jarvis

14 March 2024

DEDICATION

This research is dedicated to my son Mpilonhle Oreokame. Son, as you go about discovering the world may you do so with faith in your heart and always have in your mind that the road to success is paved with hard work, discipline and resilience.

ACKNOWLEDGEMENTS

First and foremost, God my Lord, may to you, be the glory!
I would like to acknowledge Dr Ntsibane Ntlatlapa and Dr Lucienne Abrahams, my supervisors, this would not have been possible without the generosity of your time, guidance and patience. You have not only imparted knowledge, you have also invigorated the love of discovering knowledge in me, I am eternally grateful.
To the participants who took part in this study, a special word of thank you for taking time out of your busy schedules to share your views and experiences.
A special acknowledgment to my parents, you taught me the value of education and instilled the appreciation of discipline in me from a young age. During writing of this research report you were always there supporting, encouraging, and accepting those requests for granny and grandpa visits that bought me time and space to complete this research. To the rest of my family, I would like to express my heartfelt appreciation for your continued love and care that saw me through the longest days and nights during the writing of this research report.

TABLE OF CONTENTS

LIST OF ABBREVIATIONS

4G	4th Generation Networks
4IR	Fourth Industrial Revolution
5G	5th Generation Networks
ANT	Actor Network Theory
C4IR	Centre For The Fourth Industrial Revolution
COVID19	Coronavirus Disease of 2019
DDoS	Distributed Denial of Services
DNS	Domain Name Systems
DOI	Diffusion of Innovation theory
ETSI	European Telecommunications Standards Institute
EU	European Union's
Fintech	Financial Technology
GDPR	General Data Protection Regulation
HIPAA	Health Insurance Portability and Accountability Act of 1996
HIPSSA	Harmonization of ICT Policies in Sub Saharan Africa
ICASA	Independent Communications Authority of South Africa
ICT	Information Communication Technologies
IMT	International Mobile Telecommunications
IoT	Internet of Things
ISO/IEC	International Standards Organisation/International Electrotechnical Commission
IT	information Technology
ITU	International Telecommunications Union
NB-IoT	narrow-band IoT
NIST	National Institute of Standards and Technology
POPIA	Protection of Personal Information Act, 2013
RFID	Radio Frequency Identification
SA	South Africa
SANRAL	South African National Roads Agency Limited
STS	Socio Technical Systems Theory
TDRA	Emirati Telecommunication and Digital Government Regulatory Authority
TVWS	TV Whitespaces
UK	United Kingdom
USA	United States of America

LIST OF FIGURES

LIST OF TABLES

CHAPTER 1: INTRODUCTION TO THE STUDY

1.1 Introduction

The rate of adoption for the Internet of Things (IoT) is accelerating globally; the number of connected things is forecast to reach 41.6 billion in 2025, generating 79.4 zettabytes of data (IDC, 2019). Things are physical and virtual world objects that are identifiable and can be integrated into communication networks (ITU-T, 2012). Unique identifiers make it possible for things to be accessed and to interact in the IoT ecosystem. The IoT ecosystem is characterised by the generation of huge amounts of data, interconnection, interdependence, and the communication of diverse things, all not bound by sector or location.

The term "IoT" was initially used to refer to a technology that tracked goods through the supply chain using radio frequency identification (RFID) tags (Hassan et al., 2017). The term has since evolved to incorporate sensors, actuators, connectivity hardware and software, gateways and processing, and analytics tools, among other components. These components interconnect systems and physical and virtual objects, enabling them to sense, communicate, process, react to triggers, be remotely controlled, and perform data analytics.

IoT is one of the key technologies that enables the Fourth Industrial Revolution (4IR). The term "4IR" describes the use of technology to transform industries through digitalisation, automation, and the creation of digitised value chains (Maisiri et al., 2021). This era is characterised by the seamless integration of the physical and the virtual worlds and will likely bring fundamental changes to most economic sectors (Schiller et al., 2022). The World Economic Forum (WEF) (2019) reports that the success of the 4IR era needs to be guided by adaptive, sustainable, and human-centred regulatory approaches. Current regulatory approaches need to keep up with the fast pace of IoT development to create an enabling environment for its widespread adoption and use. On the other hand, IoT characteristics raise issues of security and privacy, which can also have an effect on its adoption and use. This study explored the ways in which regulatory approaches are affecting the adoption and use of IoT in South Africa, and examined the following:

(1) Issues of security and privacy which affect the adoption and use of IoT

(2) Ways in which adaptive regulatory approaches can be developed and implemented with respect to IoT

This chapter sets out the research problem statement, the study's research objectives, and the research questions that will address the research problem. The chapter also provides the background to the key concepts of the study. An outline of the study's rationale is also presented, as well as its delimitations. This chapter is structured as follows: firstly, the research problem statement, objectives, questions, and background to the study are presented, then the delimitations, significance, and operational terms of the study are

explained. The chapter concludes by outlining the organisation of the remaining chapters of the research report.

1.2 Research problem statement

The regulation of entities in sectors such as manufacturing, agriculture, public services, and logistics that are adopting and using IoT will become more challenging as more physical and virtual things are added to the ecosystem and as they continually communicate and share information.

The research problem in this study is how the existing regulatory approaches are affecting the adoption and use of IoT in South Africa. The increasing rate of adoption and use of IoT requires the connection of a vast number of things to enable communication, and the sending, exchanging, and receiving of information, thus making them interdependent. There exist security and privacy challenges related to cyberattacks aimed at breaching the security of a system or device, as well as incidents of illegitimate access to, or the sharing of, users' personal information; these pose a challenge to the rate of IoT adoption and use. The regulation of IoT is another factor that poses a challenge to its adoption and use, because regulation can either create an enabling environment or create barriers to the adoption and use of IoT, which is dynamic in nature. Regulation plays a major role in protecting consumers and the advancement and growth of innovative solutions and products. For IoT in particular, the absence of or outdated regulatory frameworks create barriers for its long-term growth, and it becomes difficult to address the challenges related to it (Hadzovic, 2021). Therefore, IoT requires the adoption of mechanisms that can make the process of regulation-making flexible and can equip regulators with knowledge about IoT so that they can develop and implement adaptive regulation. Lee (2018) asserts that the huge benefits of IoT will likely be realised by countries whose policymakers create an enabling environment to seize the opportunities, and to help in addressing the challenges.

1.3 Research purpose statement

The purpose of the study is to investigate the ways in which regulatory approaches affect the adoption and use of IoT.

1.4 Research objectives

The objectives of the study are to explore and understand the adoption and use of IoT in South Africa; the ways in which issues of security and privacy and regulatory approaches affect this adoption and use; and how adaptive regulation which is suitable and relevant to the IoT can be developed and implemented.

1.5 Research questions

In line with the research objectives, the main research question is: How are regulatory approaches affecting the adoption and use of IoT in South Africa?

The research sub-questions are:

(1) How do challenges in the areas of security and privacy affect the adoption and use of IoT?
(2) How can adaptive regulation with respect to IoT be developed and implemented in South Africa?

1.6 Background: IoT adoption and use, related challenges, and the regulation of IoT

This section provides the background to IoT adoption and use by first looking at IoT applications that are used globally and in South Africa, with the goal of providing a broad perspective on how the technology is being used, and what it is used for. Regulations and laws specific to IoT as well as those that are relevant to important aspects of IoT are presented to provide an overview of the existing IoT regulation. The security and privacy concerns related to IoT as well as ways to approach regulation-making for IoT are also discussed.

1.6.1 IoT adoption and use globally and in South Africa

The growth of IoT is accelerating globally: Statista (2023a) reports that the IoT global market reached USD75.1 billion in 2022. IoT is being implemented in many sectors: the applications are available in the consumer, enterprise, industrial, and government domains. The uses include wearables, connected cars, utilities management, monitoring, tracking of assets, automation in supply chains, and business processes. The subsections that follow describe some IoT applications in different sectors, both globally and in South Africa.

1.6.1.1 The global picture of IoT applications

In Vietnam, the Da Nang water supply company is using IoT to monitor and analyse water quality in real time by installing sensors at each stage of its water treatment process. This allows the company to track indicators such as the water's pH and salinity, and to send alerts if any of the indicators change suddenly (Kshetri, 2017). In the hospitality industry, major international hotel chains, Hilton and Marriott, use an IoT-based solution to enhance their guest experience and to provide guests with a customised service. The hotel chains implemented the connected room concept to enable their guests to remotely control features in their rooms, such as setting the room temperature, switching lights on and off, and operating blinds or curtains from their smartphones (Tomislav at al., 2019). A smart sensor-based waste management system was enabled by IoT in Kenya with the goal of ensuring that the city's fleet of waste trucks performed their duties in the allocated time. The location and

driving behaviour of waste collection trucks can be monitored, the expected time of waste collection at the various sites can be checked, and whether dumpsites are full or require draining can also be tracked (Vizocom, 2019).

1.6.1.2 IoT In South Africa

Mordor Intelligence (2023) reports that the South African IoT market is growing rapidly and will continue along this path for the coming years with a forecast of 13.28% growth for period 2024 to 2029. The electricity crisis in the country has driven some consumers and innovators to find smarter and innovative solutions to deal with the effects of persistent rolling blackouts, thus conserving electricity, optimising their energy use, and saving costs. IoT-enabled smart geysers is one of these innovative solutions in the electricity sector. This solution places control in consumers' hands by enabling them to remotely choose and control their geysers' heating schedules, switch them on and off, adjust water temperature, and receive alerts when their geysers are faulty (Tech In Africa, 2023). A utilities service provider in Johannesburg has rolled out smart electricity meters in various municipalities; these meters are capable of implementing load limiting measures, which helps to reduce consumption and allows for remote meter reading and accurate billing (ITWeb, 2017). In the insurance sector, Discovery Insure is using IoT to track the driving behaviour of its clients by installing a low power sensor in the vehicle to collect data about driving behaviour (Goldstuck, 2019).

The roads and transport sector also implemented an IoT solution in the electronic tolling (e-toll) system by the South African National Roads Agency Limited (SANRAL) to electronically collect toll fees from motorists without them having to physically stop to pay at a toll plaza. This also has the benefit of reducing traffic congestion. A vehicle owner purchases and fits an electronic tag on their vehicle, and uploads credits. Whenever they pass under an overhead gantry on the highway the tag communicates with a device on the gantry and credits are automatically deducted (Vizocom, 2019).

1.6.2 An approach to regulating IoT In South Africa

Figure 1 below depicts the broad components of IoT: sensors, actuators, connectivity, data processing, analytics, and presentation tools for users. There is a continuous flow of data through the IoT system as data is collected, exchanged, shared, and processed.

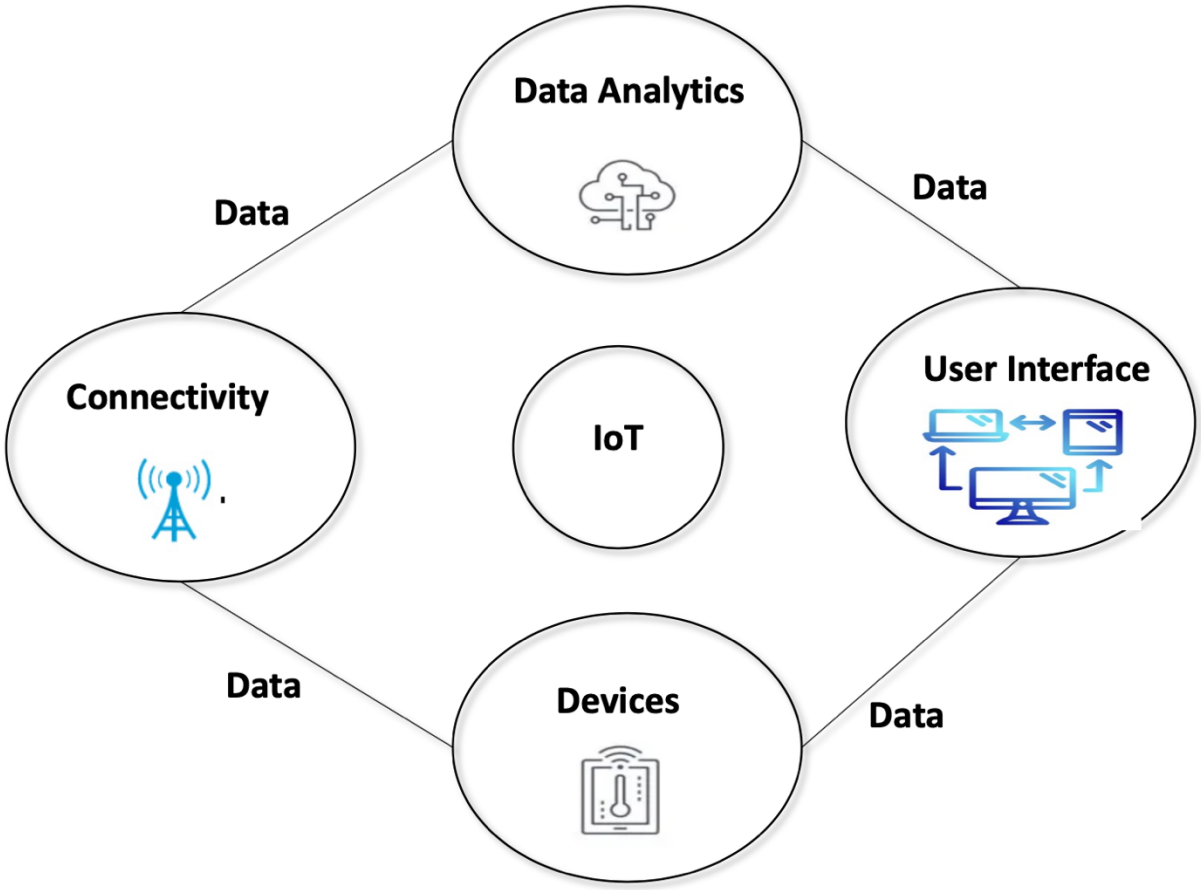


Figure 1: Components of an IoT system

In South Africa, various regulatory authorities govern entities that are involved in the different parts of the IoT ecosystem. The connectivity-providing entities are regulated by the Independent Communications Authority of South Africa (ICASA), which also oversees the type approval process. The information regulator enforces compliance with the provisions of the Protection of Personal Information Act No. 4 of 2013 (POPIA), and different sector-specific regulators regulate entities that are adopting IoT which falls within their scope. In addition, the Cybercrimes Act No. 19 of 2020 aims to reduce and prevent cybercrime in South Africa and criminalises specific acts.

A combined effort by the various stakeholders is needed to address the interoperability, spectrum, security, and privacy challenges facing IoT (Lee, 2018). This coordinated regulatory environment is key to the development of IoT and can support its adoption and widespread use. There is currently no overarching regulatory framework for IoT in South Africa, and an IoT regulatory framework that is specifically tailored to comprehensively address IoT-related issues in South Africa is needed (ITWeb, 2023).

1.6.3 An overview of regulations and laws related to the security and privacy of IoT

The subsections below provide a summary of existing regulations and laws enacted in different countries which are aimed at addressing security and privacy issues. A few of these

are designed specifically for IoT, while most deal with the general protection and security of data and acts of violations in the cyberspace which can be extended to IoT. A consolidation of these distinctive regulations and laws is necessary in order to enact laws which specifically deal with IoT to ensure the protection and security of devices and data (Karale, 2021).

1.6.3.1 Global regulations and laws related to IoT security and privacy

Table 1: Global IoT security and privacy-related regulations and laws

Regulation/Law	Description
California's IoT Law on the Security of Connected Devices – United States of America (USA)	California's IoT Law on the Security of Connected Devices is the first law in the USA to address the security of connected devices. It stipulates requirements for manufacturers of connected devices to equip their devices with reasonable security and features that are proportionate to the nature and function of the device as well as to the information that it collects (Ballon, 2020)
Health Insurance Portability and Accountability Act of 1996 (HIPAA) – USA	HIPAA protects patients' health information. It also ensures that their health information is used and disclosed in accordance with the law while at the same time allowing the flow of information for the purpose of providing and promoting high quality healthcare (United States Department of Health & Human Services, 2005)
General Data Protection Regulation (GDPR) - European Union (EU)	The GDPR ensures the protection of the personal data of EU citizens and gives them more control over their data in terms of how it is processed and stored, and their access to it, and stipulates requirements for entities on how they collect, manage, and store personal data (Official Journal of the European Union, 2016)
Code of Practice for Consumer IoT Security – United Kingdom (UK)	The UK's Code of Practice for Consumer IoT Security provides 13 guidelines to ensure that manufacturers, developers, and retailers of consumer IoT produce and supply IoT products and services with security by design features, and that these products and services are easy for people to use (Department for Digital, Culture, Media & Sport, 2018)
Brazilian General Data Protection Law – Brazil	Brazil's General Data Protection Law (GDPL) provides protection and processing of personal data t also ensures

	privacy of this data (International Association of Privacy Professionals, 2020)
African Union Convention on Cyber Security and Personal Data Protection - African Union (AU)	The AU's Convention on Cyber Security and Personal Data Protection focuses on the promotion of cyber security and combating of cybercrimes among its member states. The member states undertake to implement national cyber security policies and to establish a legal framework in their territories that is aimed at ensuring protection to personal data (African Union, 2014)

1.6.3.2 Regulations and laws related to IoT security and privacy in South Africa

Table 2: IoT security and privacy-related regulations and laws in South Africa

Regulation/Law	Description
Electronic Communications Act No. 36 of 2005	The Electronic Communications Act was passed to provide for the regulation of electronic communication services, communication network services, and broadcasting services, and also to merge these sectors. It provides for the regulation of spectrum and the licensing of market players who deploy electronic communication infrastructure and providers of electronic communication services (ICASA, 2006)
Electronic Communications and Transactions Act No. 25 of 2002	The Electronic Communications and Transactions Act regulates electronic communication and transactions, aims to prevent the misuse of information systems, and supports the use of and access to electronic communications and transactions (ICASA, 2002)
Protection of Personal Information Act No. 4 of 2013 (POPIA)	POPIA is aimed at protecting personal information and the processing of such information i.e. the collection, storage, use, sharing, and retrieval of personal information by public and private entities. It also provides standards on access to personal information as well as how the information flows within the borders of South Africa (Information Regulator South Africa, 2013)
Cybercrimes Act No. 19 of 2020	The Cybercrimes Act provides measures to prevent cybercrimes in South Africa and equips law enforcers with

	the necessary powers to enforce the law. It also criminalises acts such as hacking, the unlawful interception of data, the distribution of malicious communication, and ransomware demands (Cybercrimes Act No. 19 of 2020, 2021)

1.6.4 Issues of security and privacy for IoT

ITU-T (2012) emphasises that security and privacy protection are high-level requirements for IoT. ITU-T (2012) also emphasises the support for high quality and secure collection, communication, and processing of data related to human body services, these are static human features.

In 2016, the Mirai botnet formed a botnet army by recruiting IoT devices and then launched an attack on DYN, a domain name services (DNS) company, which affected many websites, including Twitter, Reddit, PayPal, and the BBC, causing substantial financial losses (Zahra & Chishti, 2019). The Mirai botnet exploited the security vulnerabilities of IoT by using devices with limited security mechanisms deployed in homes. In these settings, the basic but important measures of applying updates and security patches, and resetting default passwords are often neglected, and device manufacturers do not enforce them either (Tanczer et al., 2019).

The exchange and sharing of information between a vast number of things during their interaction in IoT systems creates concerns about the protection of information and the safety of the communication process. Also, the vast amounts of data generated, collected, and analysed in the IoT system are of great concern for privacy. Although this data is understandably necessary for the functioning of systems, privacy needs to be preserved to a certain degree (Sha et al., 2018). The principles of security and privacy need to be supported by a confluence of coordinated standards (Sowell & Brass, 2020).

1.6.5 Ways of adapting regulations for IoT

The IoT ecosystem consists of a variety of players: device, network, platform, and application providers (ITU-T, 2012). In South Africa, device providers are required to have their device type approved, which is a process handled by the telecommunications regulator. Network providers are licensed by the telecommunications regulator and application providers are regulated and licensed in the sector where the IoT application is used. This creates a siloed approach to IoT regulation and leaves open issues of interoperability, cybersecurity, and the privacy of data that flows throughout an IoT system. This data needs to be secured and protected. A collaborative approach ensures that the different regulators can work together to develop regulation that is suitable for IoT.

One way to close the gap between the fast rate of developments in IoT and the current process of regulation-making is to adopt an adaptive approach to regulation, where regulators allow for trial and error and apply co-design tools that have feedback loops through mechanisms like sandboxes (Eggers & Turley, 2018). In this environment, innovators are given the space to develop and test their products without being bound by the regulations that would normally apply (ITU, 2018). This provides regulators with an opportunity to evaluate policies and revise regulations, and stakeholders can collaborate (Eggers & Turley, 2018). The process of regulation-making develops in a flexible, iterative, continually improving, and adjusting manner (Sowell & Brass, 2020).

In South Africa, the Tshimologong Digital Innovation Precinct and Vodacom's narrow-band IoT (NB-IoT) laboratory in Johannesburg are sandboxes for IoT innovation. There are regulatory sandboxes for financial technology (fintech) but regulatory sandboxes for IoT are yet to be established.

1.7 Delimitations of the study

The study used the socio-technical systems (STS) theory to explore the adoption and use of IoT and the effects of regulatory approaches on the adoption and use of IoT in South Africa. The study is therefore delimited to the STS elements, which provide a theoretical lens to guide the understanding of adoption and use of IoT in South Africa, the effect that regulatory approaches, security, and privacy issues have on the adoption and use of IoT, and ways to develop adaptive regulation. Another delimitation is that the study focuses on the security and privacy elements of regulation. Other aspects of regulation are outside the scope of the study.

1.8 Significance of the study

The results of the study will provide a basis for understanding ways in which regulatory approaches, security, and privacy issues affect the adoption and use of IoT, as well as how regulation which is adaptive to the development of IoT can be developed in South Africa.

A study by WEF titled 'State of The Connected World 2023 Edition' (WEF, 2023) focused on the governance gaps in the adoption of IoT globally, Lu (2021) undertook a study on understanding users' acceptance and adoption of IoT in the USA. This study contributes to the increasing body of knowledge on IoT adoption and use in South Africa, security and privacy challenges, and ways of addressing them, as well as how regulation that is relevant to IoT can be developed. It also provides recommendations for future research as well as recommendations for regulators to consider when developing regulations for IoT, and for players in the IoT market to consider when developing IoT devices, products, and systems in South Africa.

1.9 Definitions of terms

The definitions of key concepts and the context in which they are used in the study are provided in this section, to ensure a common understanding of these operational terms within the scope of this study.

1.9.1 Adaptive regulation

Adaptive regulation describes a process of regulation-making which is characterised by flexibility, a focus on continuous improvements, adjustments, and iterations (ITU, 2018). This definition is followed in this study with the additional characteristic of collaboration.

1.9.2 IoT

ISO-IEC (2014) describes IoT as an interconnected configuration of objects, humans and systems with intelligent services that are capable of processing information gathered from the physical and virtual world and are responsive. IoT consists of sensors, actuators, connectivity hardware and software, gateways and processing tools, and analytics tools components. These components interconnect systems and objects of the physical and virtual world, enabling them to sense, communicate, process, react to triggers, be remotely controlled, and perform data analytics.

1.9.3 IoT applications

IoT applications are defined by the following capabilities: the ability to sense the environment, identify and share location information, remote controlling, and the ability to create rapid self-organised networks (Chen et al., 2014). In addition to this definition, the study further defines IoT applications as the way in which technology is used and applied in different domains and industries through products, services, and business processes.

1.9.4 Cybersecurity

Cybersecurity is explained by Stevens (2023) as a type of security whose purpose is to secure computer networks, systems, and data stored or transported between them. Cybersecurity also protects them from incurring damage and being compromised. Further to this definition, cybersecurity is viewed in this study as measures that can be put in place to prevent cyberattacks and other malicious incidents aimed at breaching the security of an IoT system, device, or communication process, or compromising the effective operation of an IoT system or device.

1.9.5 Privacy

Westin (1967) describes the concept of privacy as the ability of an individual to maintain their personal space by restricting physical access by others or limiting others from accessing

information about them. In this study, privacy is used in the context of threats to personal or private information and measures that can be put in place to prevent incidents of illegitimate, unsolicited access to, sharing, and storing of information belonging to an individual, entity, process, or transaction in IoT systems or devices.

1.10 Structure of the research report

This study consists of the following six chapters:

Chapter 1 introduces the report and provides an outline of the research problem statement, the research objectives, and the research questions. This is followed by a description of the background to and context of IoT, its adoption and use, security and privacy challenges relating to IoT, and regulatory approaches in relation to IoT. The significance and limitations of the study and definitions of key terms conclude the chapter.

Chapter 2 reviews the literature on key concepts of IoT, its adoption and use, security and privacy, and regulatory approaches to provide a clear understanding of the problem. Selected theoretical frameworks that are suitable for the study are reviewed and a conceptual framework which explains how the study will be done is introduced and developed.

Chapter 3 defines and discusses the research methodology that was followed for this research. It provides an explanation of the researcher's philosophical assumptions and the research approach and design, as well as the data collection methods employed in the study. It concludes with the ethical considerations that were followed in the study.

Chapter 4 presents the findings from data that was collected from interviews with participants, based on the research methods that were identified and discussed in chapter 3.

Chapter 5 analyses the findings that were presented in chapter 4 using the STS theory as a theoretical lens. The chapter concludes with a presentation of an adapted STS framework.

Chapter 6 concludes the study by evaluating how the research questions have been answered and what the study has contributed. The chapter also examines the limitations, and summarises the study's findings by assessing the research objectives in light of the findings. Finally, recommendations and concluding remarks are made.

1.11 Summary of the chapter

IoT is an evolving technology that is characterised by an interconnection of diverse physical and virtual things, as well as by the collection, exchange, sharing, and analysis of data between these things. Diverse stakeholders are involved in the IoT value chain, namely connectivity providers, device manufacturers, developers, and platform providers. Threats to the security of IoT devices, products, and systems, the security of the processes involved, and threats to the privacy of the data in IoT pose a challenge to its growth as users may distrust

IoT devices, products, and systems, and will be reluctant to adopt and use the technology. Also, an approach to regulation for IoT that is not adaptable to its development poses a challenge for IoT development and adoption as the development and adoption of IoT relies on an enabling regulatory environment.

This chapter introduced and provided the background to the adoption and use of IoT and the effects of regulatory approaches, security, and privacy on IoT in South Africa. The problem statement then laid the basis for the research objectives and research questions and the context of the study was provided. The factors that limit the study were discussed. The significance of the study was explained to justify the need for and relevance of the study. The operational terms that are used in the study were defined to ensure a common understanding of them in the context of this study. The chapter concluded by explaining how the chapters of the study are organised.

CHAPTER 2: LITERATURE REVIEW ON THE ADOPTION AND USE OF THE INTERNET OF THINGS, THE CHALLENGES, AND RELATED REGULATORY FRAMEWORKS

2.1 Introduction

The Internet of Things (IoT) is a dynamic technology that is being developed and implemented in a wide variety of industries. Its ecosystem is characterised by heterogeneous components and stakeholders. It is important to further explore the technology itself, the ways in which it is adopted, the security and privacy issues affecting it, the regulatory issues relating to it, as well as a regulatory environment that is conducive to its adoption and use.

A literature review provides the researcher with a means by which they can express their knowledge about the subject matter, vocabulary, and theories about a field of study (Justus, 2009). In this chapter, the literature is reviewed to provide information on the following themes: the adoption and use of IoT, security and privacy challenges relating to IoT, and the regulatory approaches relating to IoT, and how to develop an adaptive regulatory approach to IoT. Gall et al. (1996) assert that the purpose of reviewing literature is to make recommendations for future research, to lay the groundwork for the theory, and to obtain insights related to the methodology. A review of literature on selected theoretical frameworks relating to the nature of IoT and also to the adoption of technologies such as IoT is also conducted. This is done to inform the selection of a theory and the development of a conceptual framework which will provide the researcher with a lens with which to analyse the data that was collected and to guide the process of making recommendations.

2.2 The Internet of Things and its architecture

ITU-T (2012, p. 1) defines IoT as "[a] global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies". The sharing and exchange of information between IoT components facilitates seamless computing and makes it possible to achieve interoperability. Seamless computing is also enabled by an IoT assemblage that comprises sensors, actuators and communication hardware, storage, tools that enable data analytics, and visualisation and presentation tools (Gubbi et al., 2013). These technical artefacts and processes, and the actors, including connectivity service providers, device manufacturers, platform providers, IoT service providers, and users, comprise the aspects of an IoT ecosystem.

The above-mentioned technical artefacts need to be organised and connected in a way that will enable communication in an IoT system. An IoT architecture is made up of layers and each one of these layers has its own set of tasks. Interoperability between the layers is key to ensuring the large-scale interconnection of heterogeneous devices (Sha et al., 2018). There

is, however, no uniform IoT architecture. ITU-T (2012) refers to application, service support and application, network, and device layers while Mena et al. (2018) state that the architecture consists of perception, network, and application layers. The architecture depends on the type of IoT implementation and functionality required from a system. Figure 2 below shows a typical IoT architecture with the basic layers that enable an IoT system.

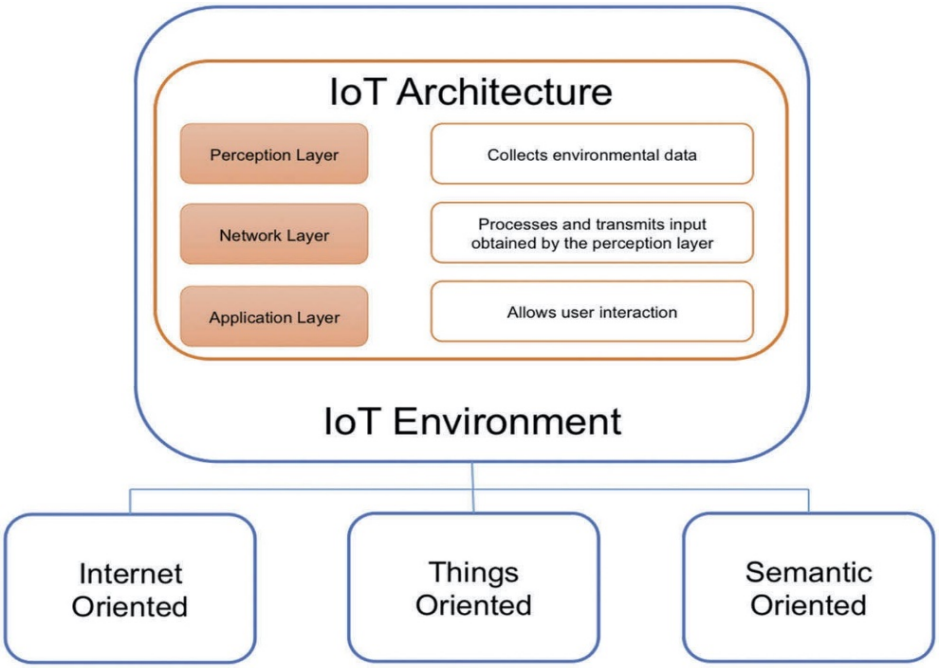


Figure 2: IoT architecture Source: Mena et al. (2018)

2.3 Applications driving the adoption and use of IoT

IoT applications are implemented in a broad range of industries. IoT Analytics (2023) reports that in 2022 the number of connected IoT devices reached 14.3 billion worldwide. Agriculture is reported to have had 36.2 million connected IoT devices in 2022 (Statista, 2023b): IoT enables precision agriculture by digitising the irrigation processes. Nutrition pumps for soil and water respond to data received from actuators such as water sprinklers and ventilation devices and crop data is collected by temperature and soil condition sensors (Lynn, Mooney, Lee & Endo, 2020). IoT also enables smart energy in the energy sector. Smart energy products such as intelligent battery storage and smart meters allow for the real-time monitoring of energy consumption and provide remote controlling capability to help users to manage their consumption and optimise their energy use (Paukstadt & Beker, 2019). IoT has enabled the digitalisation of the manufacturing process by transforming the traditional manufacturing process which consisted of independent, standalone applications to one where machines and products interact with each other, with or without humans as intermediaries (Kalsoom et al., 2020). With IoT, the monitoring and controlling of processes is automated, leading to efficiencies in production and operations. Also, the different elements of the production value chain such as product development, production, operations, and planning are integrated,

leading to operations, monitoring, and control processes that are quicker, and more effective and efficient (Kalsoom et al., 2020).

Additionally, in South Africa various sectors are implementing IoT applications, section 1.6.1.2 in chapter 1 highlighted some of these application from the electricity, insurance and roads and transport sectors.

2.4 The adoption and use of IoT and the challenge of standardisation

Lee (2018) states that the advancement of IoT partly depends on how policymakers respond to the opportunities and challenges associated with it. The diverse players involved in the IoT value chain use different policies, protocols, and security standards. They, together with the wide-ranging components and systems used, show the complex nature of the technology. The diverse and broad nature of IoT means that it defies regulatory classification and requires soft-law mechanisms such as standards, guidelines, interpretive rules, and guidance documents (Hagemann et al., 2018). Standards are a major contributing factor to technology development and adoption, and, once commonly accepted, they also influence IoT and related technologies' development and adoption (Krotov, 2017). Standards also provide a necessary structure to the way in which IoT technologies are designed, developed, and implemented (Karie et al., 2021). Additionally, standards are important to encourage the adoption of new technologies and to help manufacturers achieve economies of scale.

There are, however, no uniform IoT standards. A lack of dominant standards in IoT can be seen in the manufacturing of devices where various competing standards and new standards are being developed (Saint & Garba, 2016). Standardisation is a process that needs to be implemented at the design phase of the application (Hadzovic et al., 2021). Jakobs (2018) asserts that there were more than 900 IoT-related standards in 2016, citing the complex nature of IoT as the main reason for this. These disparate standards need to be harmonised. The harmonisation of existing standards and industry-specific privacy laws is needed to put in place new IoT-specific laws so that data can be secured and risks can be minimised (Karale, 2021). Table 3 and Table 4 illustrate some of the IoT-related security and privacy standards.

Table 3: IoT-related cybersecurity standards

Organization	Cybersecurity Standard
National Institute of Standards and Technology (NIST)	NIST is developing a cybersecurity labelling program for consumer IoT products leveraging its existing work on IoT cybersecurity, existing standards, and recent available information on threats, and by engaging with communities. Part of the work includes educating consumers, informing the certification scheme owners of the

	conformity assessment, and making recommendations on the criteria for labelling consumer IoT products and the label design (NIST, 2022)
Foundational Cybersecurity Activities for IoT Device Manufacturers	It aims to make recommendations for manufacturers on ways to improve the security of their IoT devices in terms of the features or functionalities; it also aims to help customers to manage cybersecurity risks and maintain the cybersecurity of their devices and systems (Fagan et al., 2020)
International Standards Organisation/International Electrotechnical Commission (ISO/IEC)	The ISO/IEC 27400: 2022 Cybersecurity IoT Security and Privacy Guidelines are a standard for security and privacy of IoT solutions, providing guidelines on risks, principles, and controls (ISO, 2022)
International Telecommunications Union (ITU)	The ITU-T Y.4810: Requirements for data security of heterogeneous Internet of Things devices helps to ensure IoT data safety by defining the requirements for various IoT devices, taking into account the context in which IoT is deployed and IoT resource limitations (ITU, 2021)
European Telecommunications Standards Institute (ETSI)	The ETSI TS 103 645 V2.1.2 (2020-06): CYBER; Cyber Security for Consumer Internet of Things: Baseline Requirements provide guidelines for the development and manufacturing of secure consumer IoT products (ETSI, 2020)

Table 4: IoT-related privacy standards

Organisation	Privacy Standard
ISO/IEC	The ISO/IEC 27400:2022: Cybersecurity – IoT security and privacy – Guidelines outline security and privacy controls for various stakeholders in the development of IoT solutions, as well as risks pertaining to the security and privacy of IoT solutions (ISO, 2022)
ITU	The ITU-T X.1369 Security requirements for IoT service platform outline assessment principles on security threats and challenges for the IoT service platform and provide ways to mitigate them. Data security,

	which is fundamental in solving privacy leakage issues, is a requirement in the architecture of an IoT service platform (ITU, 2022)
NIST	The NIST Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management, Version 1.0 is suitable for any organisation regardless of size, applicable in any context, and not specific to any technology, sector, law, or jurisdiction. It is aimed at addressing different privacy needs, helps in the management of privacy risks, and is directed at evolving technologies such as IoT (NIST, 2020)

A lack of standardised cybersecurity regulation leads to fragmentation, which results in IoT manufacturers and developers being compelled to adhere to different requirements in different countries and regions (WEF, 2023). Also, the lack of clear standards stifles innovation and creates a problem for implementing best practices and guidelines (WEF, 2023). A collaborative approach to establishing technology standards by forming an industry association comprising different stakeholders with the objective of encouraging the development and adoption of technology is needed (Krotov, 2017).

2.5 Issues raised by IoT: Security and privacy

IoT is one of the technologies responsible for the increased occurrence of cyberattacks. According to Cisco (2020), distributed denial of services (DDoS) attacks would double from 7.9 million in 2018 to 15.4 million by 2023. An IoT network consists of interconnected and heterogeneous devices which continuously exchange data among them; these open connections are potential access points for potential attacks. These streams of collected data are characterised by quantity, specificity, and continuity (Cichy et al., 2021). The interdependence of IoT systems makes the scale of attacks worse as disruption of one of the components can affect many other components. Each layer in the IoT architecture presents security issues of their own, but a holistic approach to IoT security is required. The perception layer is vulnerable to resource availability attacks such as DoS, while the network and application layers have issues of authentication, data integrity, and privacy (Mena et al., 2018).

Manufacturers may fail to include security features in IoT devices due to constraints of power, processing, and storage capability as well as capacity; these overheads also limit the security that can be incorporated into the device (Brown, 2015; Schiller et al., 2022). Other components of the IoT system with high processing power also suffer from security challenges (Conti et al., 2018). Jaspers and Pearson (2022) explain that there is a need to balance functionality with simple controls that allow users to define their preferred privacy settings

in the design of IoT products and devices without overloading the users with excessive information. In addition, users' understanding of privacy can be facilitated by educating them about their rights and responsibilities.

The concepts of privacy by design and security by design need to be implemented. This results in a successful implementation, with security and privacy built into the IoT system (Mena et al., 2018). Solutions should not make trade-offs between privacy and security (Weber, 2010), but should rather aim to involve all stakeholders in the IoT ecosystem in developing secure applications and services. The principles of security and privacy by design need to be addressed and included together with basic functionality and design at the initial stages of development, rather than being treated as modifications to a finalised product or even as an after-market solution (Lee, 2018). Also, the WEF (2023) asserts that industry and governments should ensure that a robust cybersecurity infrastructure is developed at the design phase of IoT products as this will result in products that are resilient and as free from vulnerabilities as possible.

The results of a WEF survey (2023) showed that the majority of experts from the IT and electronics sector that were surveyed were not confident that users of connected devices are protected against cyberattacks. They referred to underdeveloped regulatory frameworks and standardisation as some of the main reasons for their lack of confidence (WEF, 2023). In the same study, the experts also expressed their lack of confidence about the level of protection afforded to users of connected devices with regard to the unethical and irresponsible use of technology. They referred to insufficient data regulation, insufficient user education and awareness, as well as industry players, users, and regulators being disproportionately informed as contributing factors (WEF, 2023).

A transparent and predictable regulatory framework is required to develop trust in IoT for users, to stimulate innovation, to create an even playing field for industry players, and to address challenges associated with the technology (Vermesan & Bacquet, 2020). These frameworks play an important role in providing guidelines which enable users of IoT to gain an understanding of the security and privacy of their data. However, given the pace of regulation-making, uncertainty is created among manufacturers of IoT devices as the speed at which regulation is implemented is much slower than the pace of IoT deployments (Access Partnerships, 2021).

2.6 Adaptive regulation and mechanisms to develop it

IoT requires adaptive regulation, which means that regulation is reviewed, updated from time to time, and incorporates the latest available knowledge (Hagemann et al., 2018). IoT is one of the technologies which enables the 4IR and one of its key features is the fast pace at which it develops, leaving regulations intended to regulate its use lagging behind. Regulation needs to be flexible, agile, and coordinated to respond effectively and to be resilient to

developments and challenges brought by 4IR technologies in order to take advantage of the opportunities that they bring (OECD, 2020). IoT also requires a collaborative approach which involves various stakeholders, including innovators and regulators, and is agile in its posture. This means that regulation has the distinct qualities of adaptiveness, inclusivity, and sustainability, and is human-centred, placing an emphasis on faster policy-making and being responsive (WEF, 2018).

As part of their regulatory processes, regulators can adopt mechanisms such as sandboxes and accelerators where regulators partner with innovators to build and test innovative products and services (ITU, 2018). This helps to increase the regulator's knowledge and further assists them in developing suitable and relevant regulations (Eggers & Turley, 2018). Regulatory sandboxes offer a space for learning for both regulators and innovators and are appropriate for new technologies, because they offer flexibility, adaptability, and innovation friendliness, and can be used to adapt regulation to technology as it develops and to develop evidence-based regulation (Ranchordás, 2021). They can benefit innovators by reducing regulation uncertainty. Also, incorporating sunsetting into regulation can ensure automatic reviews to regulation (Eggers & Turley, 2018) and help to put in place the re-evaluation of regulation for effectiveness (Hagemann et al., 2018). Ranchordás (2015) asserts that sunsetting allows for an adaptable, flexible, and innovation-friendly approach to regulation.

Another method that can used by regulators is to employ proof of concept approaches on policies, using iterations with feedback loops to test out the effects of new policies on new technologies and using lessons from the iterative stages to improve upon and make the required changes before implementing policy (WEF, 2018). This achieves sustainability and inclusivity, capacitating regulators by gaining skills in the use of technologies (OECD, 2020) and establishing ways to get feedback from users of the technology in order to keep policies relevant (WEF, 2018).

2.7 A discussion of theoretical frameworks

A theoretical framework is a vital part of the research process. It provides a clear vision for the study and a theoretical basis for the analysis of data and the interpretation of the study's findings (Grant & Osanloo, 2015; Kivunja, 2018). As such, it serves as a foundation and underpins knowledge that is constructed for a research study. The guiding structure provided by a theoretical framework encompasses and depends on a formal theory (Grant & Osanloo, 2015)**.** Theories describe the key drivers and outcomes of a phenomenon, and the reasons and the kinds of underlying processes that propel that phenomenon (Bhattacherjee, 2012). Additionally, Kivunja (2018) describes a theoretical framework as a structure that synthesises ideas and concepts from the literature review, which helps the researcher to develop an informed lens that enables them to analyse their data, interpret the results, and make recommendations.

Three theories are identified for this study, namely the diffusion of innovation (DOI) theory, the actor network theory (ANT), and the socio-technical systems (STS) theory. These theories are discussed below, and the most appropriate one is selected in line with the objectives of this research.

2.7.1 Diffusion of innovation theory

DOI theory describes the ways in which innovation spreads as well the rate at which it disseminates. One of the main ideas is to describe individuals' and organisations' behaviour towards innovation; it also defines a process of diffusion which progresses through five stages and specifies key elements which influence the spread of new ideas (Sharma & Mishra, 2014). These elements are: (1) innovation which is seen as new by a prospective adopter – this can be an idea, object, or practice; (2) communication which describes channels through which supporters and potential adopters communicate; (3) time, which is a key element that describes the rate of adoption and an individual or an organisation's tendency to innovate; and (4) social systems which are interrelated units in which an innovation diffuses – these units can be individuals or organisations (Rogers, 1982). The process results in categories of adopters, namely innovators, early adopters, early majority, late majority, and laggards (Dissanayake et al., 2022). These adopters are categorised according to the degree to which the one group is relatively earlier in adopting a new idea as compared to the other group (Sahin, 2006).

DOI theory has been widely used to study adoption, innovation, implementation, and diffusion of technology (Prescott, 1995). Sahin (2006) states that this theory is widely used as a theoretical framework in the area of technology diffusion and adoption. DOI theory is also applicable to emerging technologies such as IoT. Saarikko et al. (2020) used DOI theory to better understand the diffusion of IoT within the public sector in Swedish municipalities.

For the purpose of this study, DOI theory does not go far enough beyond its focus on the adoption and diffusion of technology and will therefore not be suitable for the study. The study also seeks to explore ways in which aspects of regulation, security, and privacy affect the adoption and use of IoT.

2.7.2 Actor network theory

ANT was derived from science and technology studies. ANT explains mutual, evolving interactions and the building of heterogeneous networks among humans and non-human actors which happen over a period of time (Yuan, 2023). Law (1992) refers to the actor network as saying that society, organisations and machines are results of a patterned network. An actor is defined as a human being, a group, and non-humans, and a network is an interactive, heterogeneous group of actors comprising humans, machines etc (Dolwick, 2009).

ANT does not allow for the superiority of either technical or social aspects, meaning that it disregards the idea of technical and social determinism (Hald & Spring, 2023). ANT is used to describe the process of technology adoption, and also defines technology adoption as an outcome of a build-up of smooth flowing networks of diverse relationships between actors who are human and inanimate objects (McBride, 2003). ANT is suitable for technology studies as it comprises both social and technical elements. Al Isma'ili et al. (2017) applied ANT to study the potential that IoT has to relieve societal challenges in Africa.

Although ANT focuses on the technical and social elements of technology it does not sufficiently describe the system that is defined by the interrelationship and interaction of the two elements. Accordingly, it will not be suitable for the study, which seeks to delve deeper into that system.

2.7.3 Socio-technical systems

The main thrust of STS theory is to effectively bring together an organisation's social and technical aspects (Maguire, 2014)**.** The traditional focus on technical aspects is described as narrow when looking into systems, as the focus needs to be on technology, users of technology, and the context in which it exists (Shin, 2014). The main idea of STS theory is that social and technical aspects are considered together as interdependent aspects of a complex system (Ghaffari et al., 2019). STS theory comprises two subsystems: technical and social subsystems, which in turn consist of four interacting elements, namely technology and tasks, which are categorised under the technical subsystem, and structure and people, which are categorised under the social subsystem (Bostrom & Heinen, 1977). Technology aspects cover technical elements including hardware, software, and infrastructure, while tasks describe efforts to develop the technology and activities to get it adopted. People include users and developers, and structure describes systems of authority (Kapoor et al., 2021).

The success of an STS is an outcome of interactions between the technical and social subsystems. STS theory has been applied to a wide range of disciplines, including information systems, production systems, sustainability studies, business, and engineering, employing both qualitative and quantitative methodologies (Abbas & Michael, 2023). Shin (2014) explains that STS theory is a valuable tool when investigating how evolving technologies are advancing. It also provides a comprehensive approach to explaining interactions between humans and technology in the development of IoT. Brass and Sowell (2020) refer to IoT as a dynamic, evolving STS.

Ghaffari et al. (2019) applied STS theory to evaluate and to gain an understanding of how IoT will develop and evolve in Korea, as well as to investigate how Korea will approach the challenges of designing and implementing the various IoT components. Also, Shin and Park (2016) analysed the development of IoT by employing STS theory to provide insights into the socio-technical issues related to IoT with the aim of helping stakeholders in IoT, such as

governments, industries, and business owners, to align their strategies and efforts better in order to achieve a balance between the technical and social aspects of IoT.

The study adopts STS theory as suitable for exploring the adoption and use of IoT in South Africa, the regulatory, security, and privacy issues affecting it, and ways to develop adaptive regulation for IoT, as well as to analyse the findings of the study. STS theory will provide the study with a focus on the technical and social components of IoT as well as on the interaction of these components. Additionally, the elements of STS theory, namely technology, tasks, structure, and people, will help the researcher to explore adoption, use, regulation, security, and privacy in relation to IoT.

2.8 Conceptual framework

The conceptual framework explains how the research problem will be explored. It also helps to explain how the phenomena will be studied. Dickson, Emad and Joe (2018) posit that a conceptual framework is a logical structure which provides a presentation of how ideas in a study are related; it also identifies and links concepts which emanate from the problem that is being studied. Additionally, a conceptual framework explains the relationships among key constructs of the study, is rooted in the study's literature, and is also set in relation to a viable theory (Crawford, 2020).

IoT is not merely a technical phenomenon; it has an effect on the people who adopt and use it, and its development is also affected by structures of authority such as regulators. IoT has the potential to transform how society operates and interacts (Lynn et al., 2020). This study views IoT not only as a technical phenomenon, but also incorporates its social aspects, thereby adopting a socio-technical approach to IoT. In the previous section STS theory was adopted as a suitable theory for the study, because STS theory considers both social and technological aspects, as well as the system which is defined by their interactions. The framework in Figure 3 below shows concepts that have been identified from the literature reviewed and the relationships between them, and it will be used to analyse the findings of the study. The framework is derived from Bostrom and Heinen (1977).

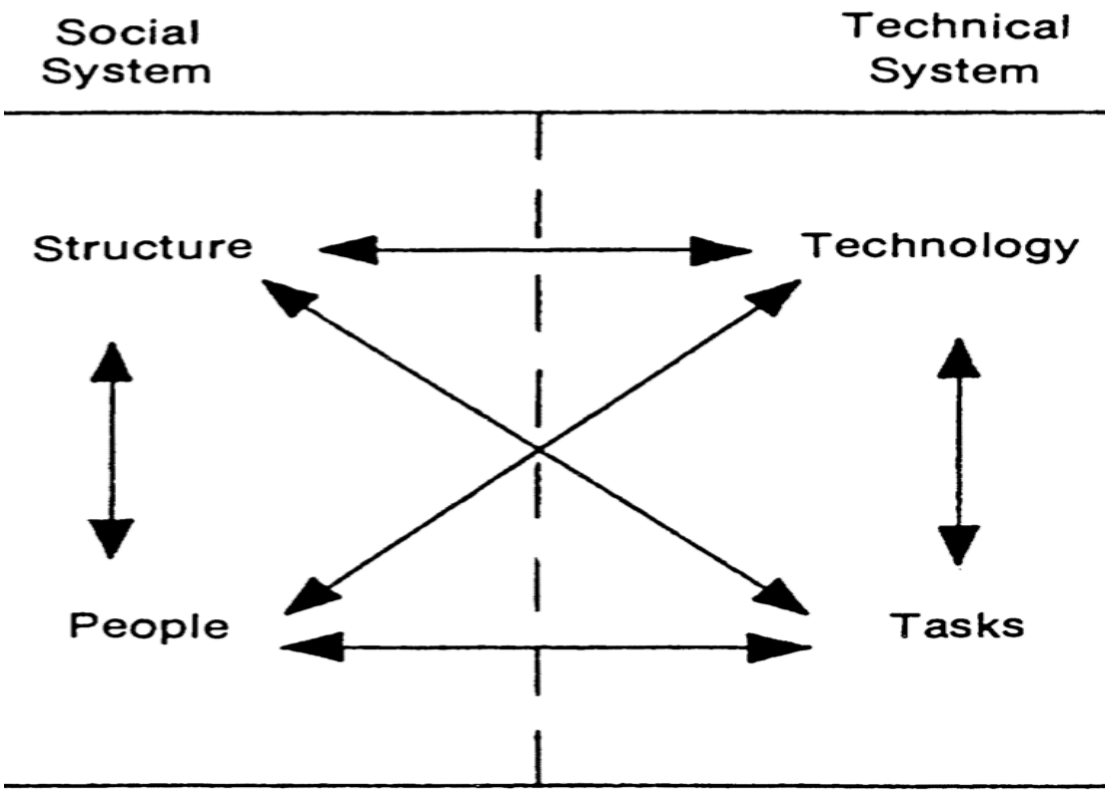


Figure 3: Socio-technical systems framework Source: Adapted from Bostrom and Heinen (1977)

2.9 Summary of the chapter

Three themes were employed to explore literature for this study. The first theme described the adoption and use of IoT by first looking into the technical components of IoT with the aim of laying a foundation, to create a reference, and to better explain the point of origin for some IoT-related issues. It also described some implemented IoT applications and outlined the challenge of standardisation which affects the adoption and use of IoT. The second theme described the security and privacy challenges for IoT, and the third theme looked at adaptive regulation and the mechanisms that regulators can adopt in order to develop adaptive regulation for IoT. The chapter then turned to the literature on theoretical frameworks that are applicable to IoT before selecting the STS framework. This framework is the appropriate theory and conceptual framework to explore the adoption and use of IoT in South Africa, the regulatory, security, and privacy issues affecting it, and ways to develop adaptive regulation for IoT, and also to analyse the study's findings.

CHAPTER 3: QUALITATIVE METHODOLOGICAL APPROACH

3.1 Introduction

Research is a systematic way of enquiring into or investigating something with the primary goal of creating and expanding knowledge (Hussain et al., 2013). A key requirement for this process is to design and undertake it in a manner that is methodologically sound (Saunders, Lewis & Thornhill, 2009).

This chapter explains the methodology followed in this study that enabled the researcher to answer the research questions and fulfil the purpose of the research that was identified in chapter 1. It outlines the research paradigm that served as the philosophical underpinning for the study, the research approach that allowed the researcher to seek a deeper understanding of a phenomenon, a detailed plan for the collection of data through research design, as well as the data collection methods employed in the study. The chapter also outlines the process of data analysis and concludes with a discussion on the ethical considerations that were followed for the study.

3.2 Research paradigm

A paradigm, also referred to as a philosophical worldview, is defined by Ernest (1994) as a set of beliefs and a theoretical framework which makes assumptions about ontology, epistemology, methodology, and methods. It is a means by which reality can be understood and studied. These components are interlinked, meaning that from a researcher's ontological stance, research methods can be traced through epistemology and methodology (Scotland, 2012). Moreover, a researcher's ontological assumptions inform their epistemological assumptions which inform their methodology, and these all give rise to the methods employed to collect data (Mack, 2010). They act as philosophical underpinnings for elements of the research paradigm. An approach to research is underpinned by philosophical assumptions which guide and inform the choice of research questions, methodology, methods, and intentions (Mack, 2010). These elements are positivism, interpretivism, and critical theory (Kivunja & Kuyini, 2017).

The following sections define the components and elements that have been outlined above, and also specify the ones that were selected for the study.

3.2.1 Ontological assumptions

Scotland (2012) defines ontological assumptions as being concerned with what constitutes reality and goes further to say that researchers need to take a position about their perception of how things are. The experiences that the researcher gains from interactions, in different contexts, and the meaning that they attach to things and situations shape how they view reality. Therefore, there are multiple realities. The ontological view that this study adopted

was relativism. The researcher participated in the research to uncover reality and bring meaning to the topics that were under study. Furthermore, the researcher viewed reality as unique, evolving depending on the context and experience of people; it cannot be generalised or uncovered objectively.

3.2.2 Epistemological assumption

An epistemological assumption is concerned with how knowledge is uncovered. Scotland (2012) defines epistemology as how the knowledge can be created, acquired, and communicated. Knowledge is gained by examining reality to uncover meaning, to understand it, and to interpret it. The epistemological view that this study adopted was interpretivism, which seeks to understand (Scotland, 2012). Data was gathered from interaction with participants and then interpreted to uncover meaning, which helped to understand the area of interest. The interpretive paradigm regards understanding and interpretation as inseparable (Hussain et al., 2013). It also regards the interaction of the researcher with participants as a principle where research is not observed from the outside (Mack, 2010). Additionally, the study employed a deductive approach to reasoning guided by the STS framework. A deductive approach is one of the modes of reasoning which moves from general principles to particular observations. Babbie (2010) explains this process as transitioning from a theoretically expected pattern to observations that test the existence of that pattern, while an inductive approach moves from specific observations to general principles.

3.2.3 Methodology

Kothari (2004) defines methodology as a systematic way of solving a problem. The approach helps to construct knowledge, understand it, and interpret it for meaning. It also provides guidance to the researcher on the kind of data and the data collection tools that are required for the study (Rehman & Khalid, 2016). Further, research methodology is the path by which researchers need to conduct their research (Sileyew, 2019). This study employed a case study methodology. Case studies delve deep into the investigation of any social phenomenon (Hussain et al., 2013). Merriam (2010) describes a case study as a carefully considered examination and description of a bounded system. A bounded system is explained as an entity with boundaries around it. The case is a phenomenon to be studied, such as a thing, group, institution or specific policy (Merriam, 2010). In the context of this study the case is IoT and it is bounded by looking at the process of adoption and use, as well as at South Africa as the location. In addition, interviews, observations, and documents are relevant data collection methods for case studies (Creswell & Creswell, 2018).

3.2.4 Research methods

Yohannan (2010) defines a research method as a step-by-step process of enquiry which begins with underlying assumptions and moves to research design and data collection. Data that is collected and analysed helps to answer the research questions posed and also

addresses the research objectives. The study adopted a qualitative data method for its research. A detailed discussion of this research method is provided in the section that follows.

3.3 Research approach

The three research approaches are the qualitative approach, the quantitative approach, and the mixed methods research approach (Creswell, 2013). Kothari (2004) describes the quantitative approach as research that is focused on measurements of quantity and numbers. It uses statistical techniques such as regression to analyse the data, with the aim of generalising results. On the other hand, researchers using qualitative methods aim to understand the way in which people make sense, give meaning to their experiences and how they shape their worlds (Merriam, 2010). It emphasises processes and meaning and uses interviews, focus groups, and observations as data collection techniques (Kivunja & Kuyini, 2017). Qualitative data that is generated from interaction with participants is analysed to discover patterns, concepts, themes, and meanings, and the results are presented as descriptive narrative using words (Yohannan, 2010). Mixed methods research uses both the quantitative and qualitative approaches, and is perceived to use strengths from both approaches and to provide the researcher with deeper insights into the research problem (Creswell, 2013).

This study employed a qualitative research approach. The researcher gained an understanding and meaning, and through the use of words produced a rich description of what was learnt from the study of the adoption and use of IoT and the implications for adaptive regulation (Merriam, 2010).

3.4 Research design

Research design is the framework of the study. Bhattacherjee (2012) refers to it as a blueprint which specifies a comprehensive plan for the process of data collection and answering research questions; it needs to detail the data collection, instrument development, and sampling processes. The sections below provide details on the sampling strategy, data collection, and data analysis methods.

3.4.1 Sampling strategy

The sampling strategy defines the target population, the sample, and the sampling technique that is used to select the representative number from the population.

3.4.1.1 Population

A population refers all individuals including things and events that have common characteristics that are of interest to the researcher (Sileyew, 2019). The target population for the study was individuals who are knowledgeable about IoT and those who are

knowledgeable about the regulation of technology as well as information communication technologies (ICTs).

3.4.1.2 Sample

A sample is a subset of the population selected for the purpose of providing in-depth information about phenomena. Furthermore, Babbie (2010) explains that the degree to which the sample is representative is determined by it having a combined set of characteristics that approximately match the same combined characteristics in the population from which it was selected. A total of 13 participants who are knowledgeable about IoT and regulations related to it were interviewed for this study. Guest et al. (2006) describes saturation as a concept that describes a stage at which new themes are no longer emerging from the data, and posits that this stage is reached within the first 12 interviews for a qualitative research.

3.4.1.3 Sampling technique

Probability and non-probability sampling techniques are two broad techniques of sampling. These techniques are differentiated by the chance that a unit has to be selected in the sample. In probability sampling a unit has a chance to be selected, while in non-probability sampling a unit has zero chance of being selected (Bhattacherjee, 2012). The participants in this study were determined by a purposive sampling method which is a non-probability method. In purposive sampling the inclusion of a participant in the sample is not pre-determined and the selection is based on the researcher's judgment (Kothari, 2004). The selected sample was one from which the researcher wanted to learn and purposive sampling was the most suitable method as it is based on the premise that it allows for discovering, understanding, and gaining insights (Merriam, 2010).

3.4.1.4 The study's participants

The study had 13 participants from the automotive, telecommunications, technology, research, consulting, academic, and technology original equipment manufacturer (OEM) industries. They hold executive, managerial, architecture, and practitioner positions. Figure 4 below shows the industry profile of the participants.

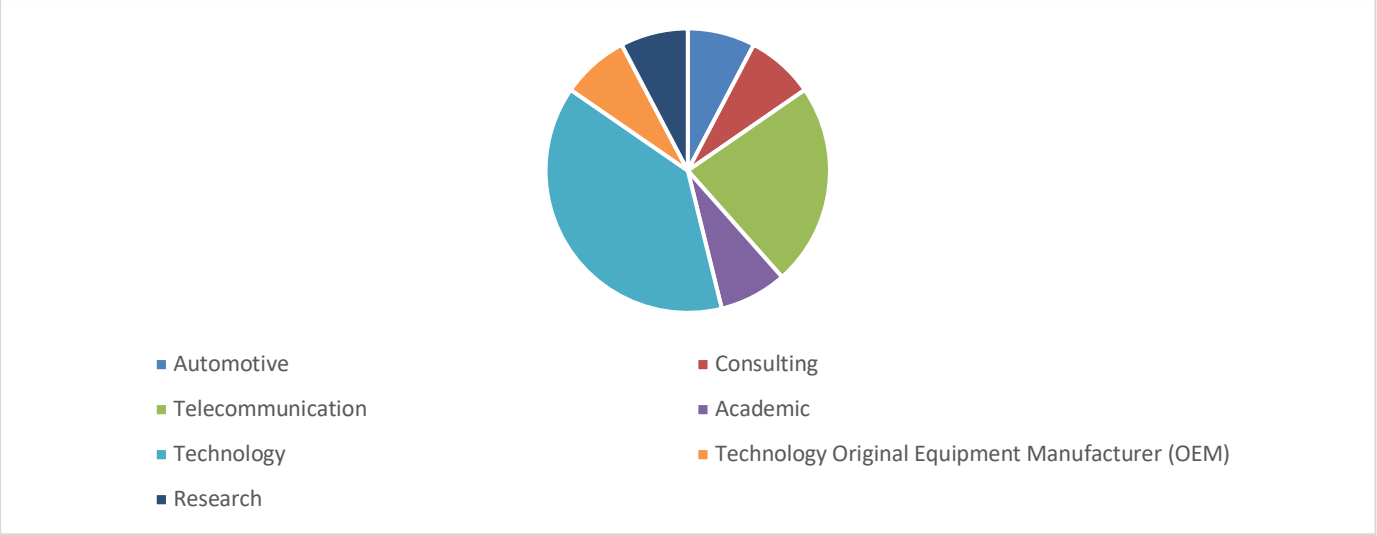


Figure 4: Participants in the study

3.5 Data collection method

Data was collected using qualitative data sources, namely in-depth interviews, which provided the primary data for the study. Primary data is data that is collected for the first time (Kothari, 2004) from the original source. Additionally, interviews are the most used data collection method for interpretive research studies (Bhattacherjee, 2012). Sileyew (2019) refers to interviews as having the advantage of allowing respondents to raise issues that the interviewer may not have expected. Another advantage of interviews is that the rate of non-responses is low and researchers can obtain in-depth information (Kothari, 2004). Interviews also allow the researcher to probe so as to get as much information as possible from the participant, which helps to enrich the data. The study employed semi-structured interviews as the data collection method; this method has a pre-planned set of core questions for consistency among interviewees, and also allows them to further elaborate or provide more relevant information as the interview progresses (Yohannan, 2010). The interviews were conducted on digital meeting platforms, namely Microsoft Teams and Zoom.

3.6 Data analysis

The researcher plays an important role in the analysis of qualitative data as it relies on their ability to analyse and integrate the information and on their personal knowledge of the field of study (Bhattacherjee, 2012). Furthermore, the researcher needs to understand, make sense of, and interpret the data that was collected.

Data that was collected in the study was analysed deductively using the thematic analysis method to systematically discover themes that emerged from the data. Thematic analysis is a qualitative data analysis method that serves to identify, analyse, and organise data into themes (Braun & Clarke, 2006). It also produces unanticipated insights drawn from different

participants' varying perspectives as well as a summary of key attributes of a set of data (Nowell et al., 2017).

Braun and Clarke (2006) outline the phases of conducting thematic analysis, and the analysis of data in this study followed these steps. Braun and Clarke (2006) assert that the researcher is not compelled to follow the steps in a linear fashion but can traverse between them backwards and forwards as needed. The sections below detail how thematic analysis was conducted in the study by following the thematic analysis phases of Braun and Clarke (2006).

3.6.1 Immersion in the data

This step entails engaging, transcribing, and reading the data. Data that was collected through semi-structured interviews was recorded with the permission of the participants and transcribed using Otter.ai, which is voice-to-text transcription software (Otter.ai, 2023). The transcripts were checked for accuracy by listening to the interview recording while reading through the transcribed text. Additional active re-reading sessions were done to familiarise the researcher with the text and gain an understanding of the data.

3.6.2 Generating initial codes

Coding essentially categorises data items into concepts and is a key process in qualitative data research (Babbie, 2010). It also allows the researcher to systematically arrange and group data with similar codes which have common characteristics into categories (Saldaña, 2013). The researcher systematically identified and organised meaningful data into codes by using descriptive codes which were a summary of the subject of the excerpt, as well as In Vivo coding, which uses interesting words from participants verbatim. Figure 5 below illustrates a part of the coding process from the study.

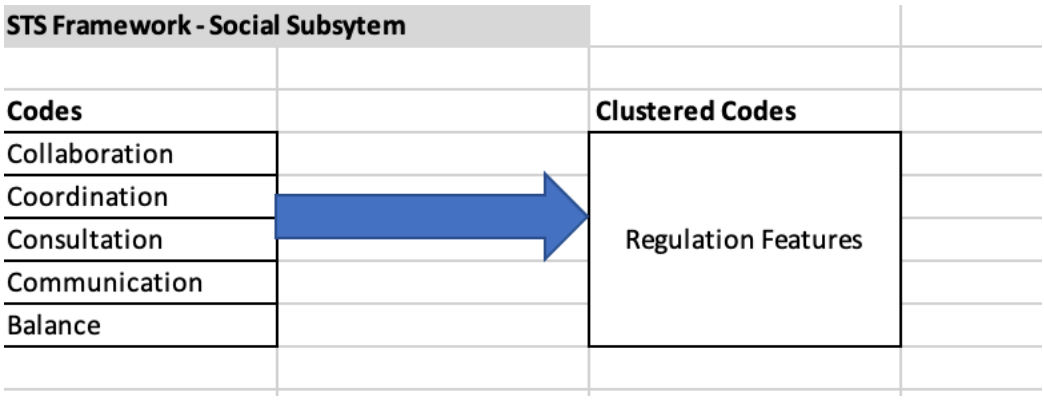


Figure 5: Data coding process

3.6.3 Searching for themes

Codes that were generated from the data were allocated to potential themes that were identified. The researcher also took note of similar themes to be condensed into a broader theme at a later stage.

3.6.4 A review of themes

At this stage potential themes that were developed in the previous stage were re-considered to assess if they were relevant and relatable to the study. This entailed discarding irrelevant themes, condensing similar themes, and breaking down compact themes into meaningful, more specific, focused themes.

3.6.5 Defining and naming themes

The themes were now clearly defined and given descriptive names and could provide a clear interpretation of the data.

3.6.6 Writing of the report

At this final stage the fully developed themes allowed for analysis in relation to the STS framework and for narrative reflection on the data in the writing of the report.

3.7 Ethical considerations

Saunders et al. (2009) explain that research ethics refer to designing the research, collecting, processing, storing, and analysing data, and writing the report in a moral and responsible way. In accordance with this and the compliance procedures of the University of the Witwatersrand, the researcher applied for and obtained ethical clearance from the human research ethics committee (non-medical) of the university. This permitted the researcher to carry out the process of data collection through interviews with the study participants. The researcher upheld the requirements and compliance procedures throughout the process of conducting interviews and other consequent research processes. Table 5 provides a summary of some key ethical considerations followed by the researcher.

Table 5: Ethical considerations followed

Ethical consideration	Process undertaken
Seeking permission to conduct interviews with human participants as part of the data collection process	Applied and obtained an ethical clearance certificate from the university's human research ethics committee (non-medical). Certificate Protocol Number: SLLM-M21-02 (see annexure A)

Participation in the study	All participants were sent requests to participate in the study and informed consent forms. An explanation of the purpose of the study, the details of the study, and the interviewing process were also provided
Anonymity and confidentiality issues	The participants' confidential information was not shared and pseudonyms (e.g. Participant 1) were used in the report
Protection and safe-keeping of data	Data was stored in a password-protected computer belonging to the researcher and backed up on the researcher's cloud storage for safekeeping

3.8 Summary of the chapter

This chapter began by defining the philosophical orientation of the study through a discussion of the ontology, epistemology, methodology, and research methods components in the research paradigm section. A qualitative research approach that helped the researcher to develop an understanding of the meaning of the phenomenon was then explained, together with the other research approach methods, as well as the research design, which detailed a plan for the process of data collection. Lastly, the process of analysing the qualitative data that was collected and the ethical considerations that the researcher adhered to were also explained. A summary of the research methodology for this study, as presented in this chapter, is illustrated in Figure 6 below.

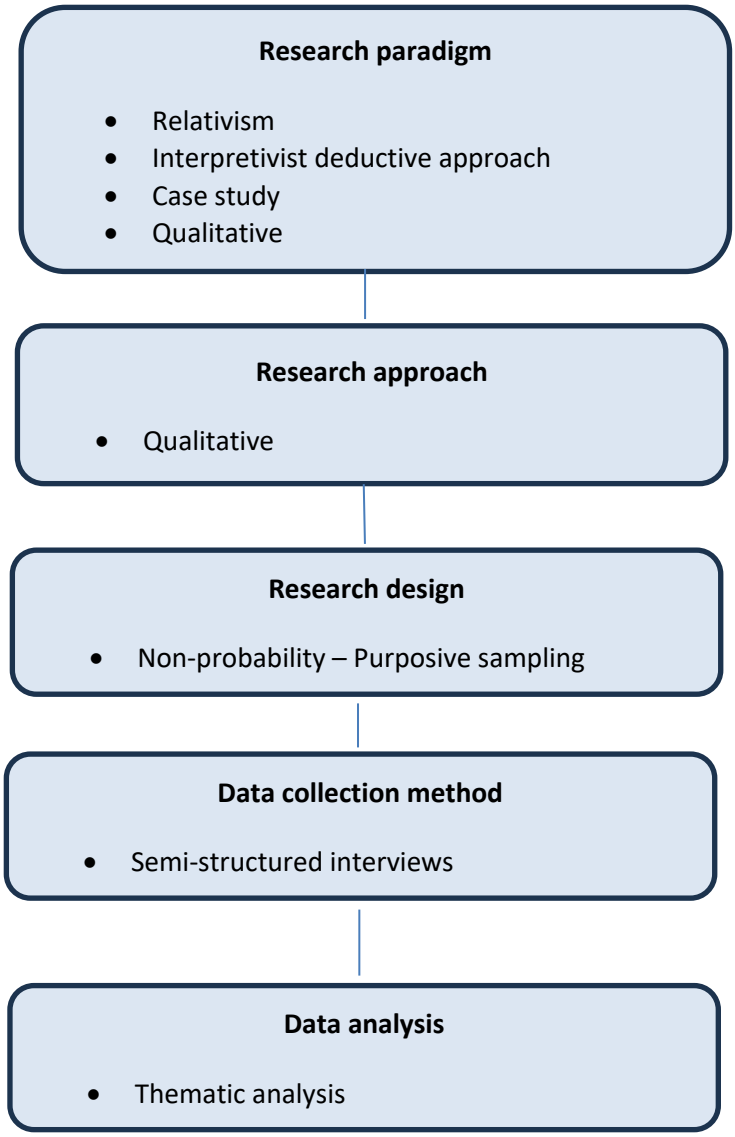


Figure 6: Summary of the research methodology

CHAPTER 4: PERSPECTIVES ON THE ADOPTION AND USE OF THE INTERNET OF THINGS AND THE REGULATORY ASPECTS AFFECTING IT

4.1 Introduction

The purpose of this chapter is to present the findings of the study. This is done by discussing data according to the themes that were outlined in the literature review in chapter 2, sections 2.4, 2.5 and 2.6 respectively.

The findings are derived from the data that was collected from interviews with participants who are involved in the IoT industry in South Africa, and who are knowledgeable about IoT and regulation. Alshenqeeti (2014) explains that interviews are an interactive, powerful means that is used to obtain in-depth narrative data about the topic where interviewees can express their views in more detail.

The findings are presented by categorising them according to the themes that were identified in the literature review: the adoption and use of IoT, security and privacy, and adaptive regulation. Under each theme, details which expand on the responses from the participants are discussed.

4.2 The adoption and use of IoT

This theme explores the adoption and use of IoT in South Africa by looking into the rate at which IoT is advancing. It also looks at the industries in which IoT is being adopted and used to gain an understanding of who is adopting and using IoT, and the kinds of applications for which IoT is being used. Emerging technologies are characterised by being distinctive, radical, fast-growing, having a great impact, and being ambiguous (Rotolo et al., 2015).

IoT is the kind of technology that can be implemented in the form of new products and solutions. IoT can also be adapted and added onto existing products, processes, and services. This theme also looks at which of these implementations is more prevalent in South Africa to understand which one of them is driving the uptake of IoT. Current and ongoing challenges that affect IoT adoption and use are also examined to gain an understanding of the issues that need to be addressed to create the kind of environment that can encourage its growth.

4.2.1 Varying perspectives on the rate of IoT adoption and use in South Africa

The way in which IoT as a technology and its applications are seen to be maturing in South Africa has an impact on the pace of its adoption and use. The study participants described the pace of IoT adoption and use in South Africa as slow where the rate is low, moderate where it is progressing steadily, or fast where the rate is rapid. Figure 7 summarises the responses according to these three categories.

4.2.1.1 Slow adoption

A slow pace of IoT adoption and use in South Africa was observed by a number of participants, who noted that IoT applications are still in the early developmental stages and have not yet reached a stage of maturity. Participant 2 remarked:

> So, rate of adoption, I think it is relatively slower than one might expect given the potential for the application in the South African market. And the reason I say that is I think a lot of the application for me seems to be in the research space where people are exploring, but I don't think there's enough mainstreaming of IoT.

Some people also seem to adopt a "wait and see" approach where they wait for the technology to mature first and then adopt it when it is much safer to do so. Also, the lack of digitised processes is seen to be affecting IoT adoption in small- to medium-sized enterprises.

4.2.1.2 Moderate adoption

Measures that were put in place to combat the spread of the COVID-19 virus during the pandemic years have had an effect on the use of digital technologies. IoT is one of the technologies that made moderate progress in its adoption and use during that period. A steady growth was noted by some of the participants, with one of them alluding to the fact that IoT has not been adopted in great numbers worldwide, as was projected in various publications. With regard to this point, Participant 11 commented:

> It's not been the absolute disrupter, the absolute massive influx of IoT adoption that we expected.

4.2.1.3 Fast adoption

The majority of participants reported a fast rate of IoT adoption and use in South Africa. One contributing factor that was identified is connectivity, which is seen to have improved through 4th generation networks (4G) and the ongoing rollout of 5th generation networks (5G). Also, the transition from fixed to wireless connectivity seems to have been less onerous for the country and this enabled a fast uptake. Participant 10 remarked:

> We probably had a stronger uptake than a lot of developed markets because we were wireless first in a lot of cases, we didn't have a strong legacy of a fixed line. So, when Vodacom and MTN started innovating around IoT we were probably leaders in that space.

Government support for smart city projects such as City Power's Smart Meter Implementation Programme also points to the adoption of IoT. Another participant added that in the last 12 to 18 months there has been an increase in the adoption of IoT, noting that in their industry they have witnessed lots of discussions, proof of concepts, proof of value, and projects related to IoT. They attributed this to a level of maturity that has come into the

IoT market, and also to the efforts and projects that have been put in place by some companies to reduce their carbon footprint.

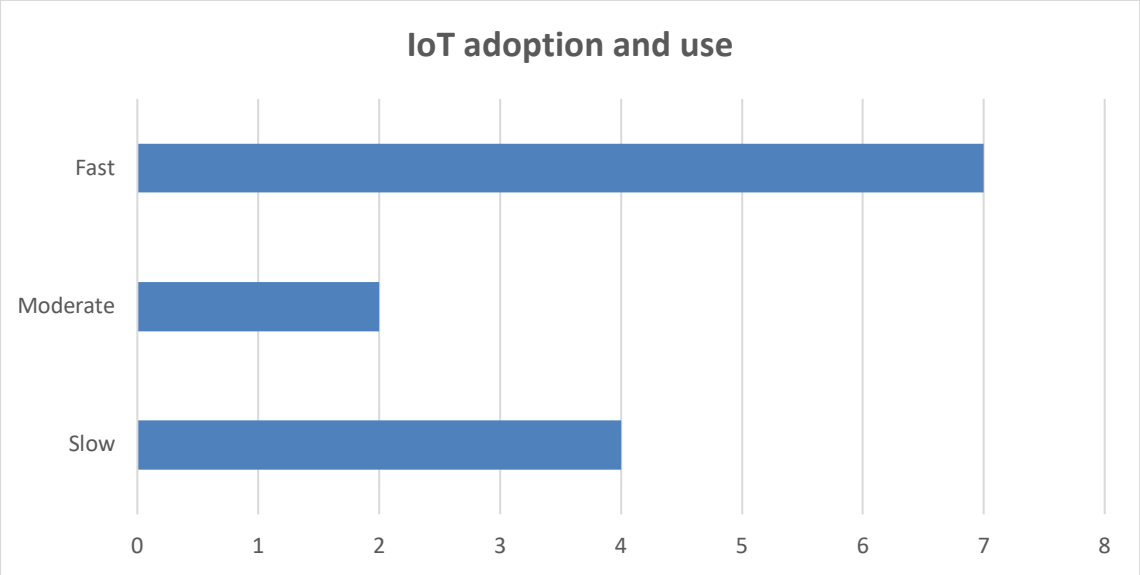


Figure 7: Rate of adoption and use of IoT in South Africa

4.2.2 Implementations that are driving IoT adoption and use

IoT can be implemented by acquiring a completely new solution or product, by digitalising some elements of the business process, or by equipping existing products, processes, and services with new features and efficiencies. The participants responded on which implementation is more prevalent in South Africa and also indicated the factors that influence the decision to choose a specific implementation.

4.2.2.1 New solutions and products

Rogers (1982) describes innovation as an idea or project that is seen as new by an individual or an organisation. The costs associated with upgrading or replacing existing equipment and systems are driving some companies to seek and implement new IoT solutions and products, as noted by one participant. The need for companies to differentiate themselves was noted by Participant 4, who said:

> So I find that the biggest drivers really are the innovations, there are companies that are just trying to differentiate themselves using technology. So I find that innovations are what is really driving IoT currently.

Additionally, the issue of compatibility between the legacy system and IoT is discouraging for some, so they prefer this way of implementing IoT in their environments.

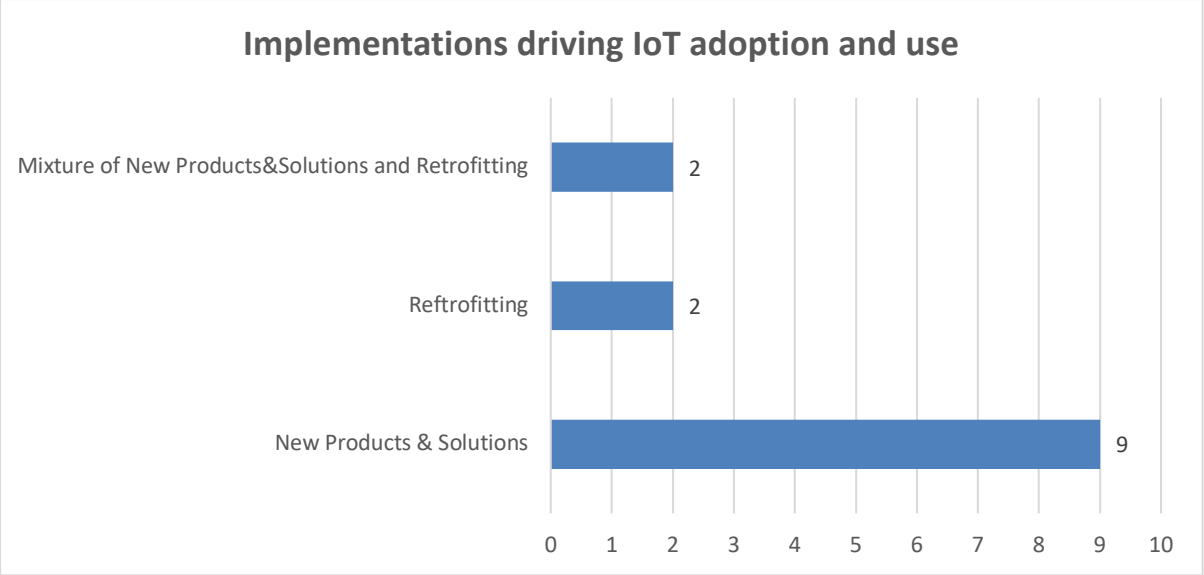


Figure 8: Types of IoT implementations driving IoT adoption and use in South Africa

4.2.2.2 Retrofitting

The majority of participants said that they are witnessing implementations of IoT in existing environments, using existing infrastructure, where IoT is added on to equipment and systems that were not initially designed and built with IoT in mind. These companies want to optimise and to better manage the use of resources in order to save costs. Another reason for this, according to one participant, is that South Africa is faced with economic challenges.

Another participant noted that they have observed more incremental innovation, where legacy systems are enabled to interoperate with new, smarter systems. Participant 13 commented:

> The highest adoption is mostly seen in the manufacturing industry, as a means to optimise processes, reduce costs and streamline efficiencies. We see this mostly taking place within a retrofitting context due to the high costs and operational disruption associated with overhauling the production line and installing new technologies.

4.2.2.3 A mixture of new solutions and products and retrofitting

A mixture of both new products and solutions and retrofitted implementations was noted by a few participants.

4.2.3 Industries where IoT is being adopted

The adoption and use of IoT is significant in a number of industries. The majority of participants identified the top three industries where IoT applications are being implemented. Other industries that were identified are listed in Table 6 below.

4.2.3.1 Top three industries with the most observed IoT adoption in South Africa

Manufacturing

The participants reported having observed a significant number of IoT adoptions in the manufacturing industry. IoT is used in maintenance management systems to enable predictive and preventative maintenance, and also to streamline production lines in order to achieve efficiencies and save costs.

Logistics

Another industry that leads in the use of IoT is logistics: IoT is used for fleet management, and for tracking vehicles, parcels, assets, and wildlife. Vehicles are equipped with sensors and can send information about the condition, movement, and load of the vehicle back to the company or the original equipment manufacturer (OEM), and can also collect information to enhance the driver's driving experience. Insurance and car tracking companies also use sensors to monitor the driving behaviour of their clients and to track vehicles so as to inform their clients when they enter a dangerous area, to track the movement of their vehicles, or in instances where the vehicle is stolen. Parcels can also be tracked throughout the supply chain.

Security services

The security services industry is also a big adopter of IoT, partly due to the high levels of crime in the country. Service providers use IoT in early warning detection systems, smart cameras, and for monitoring intrusion, tampering, and breaches on properties. These systems also allow homeowners to monitor their properties remotely, using applications on their smartphones. IoT is also used to detect gunshot sounds. Additionally, a prominent security services provider in South Africa is a supplier of IoT solutions to the retail industry. One solution is a system equipped with sensors which helps retailers to manage inventory and track stock items to mitigate loss.

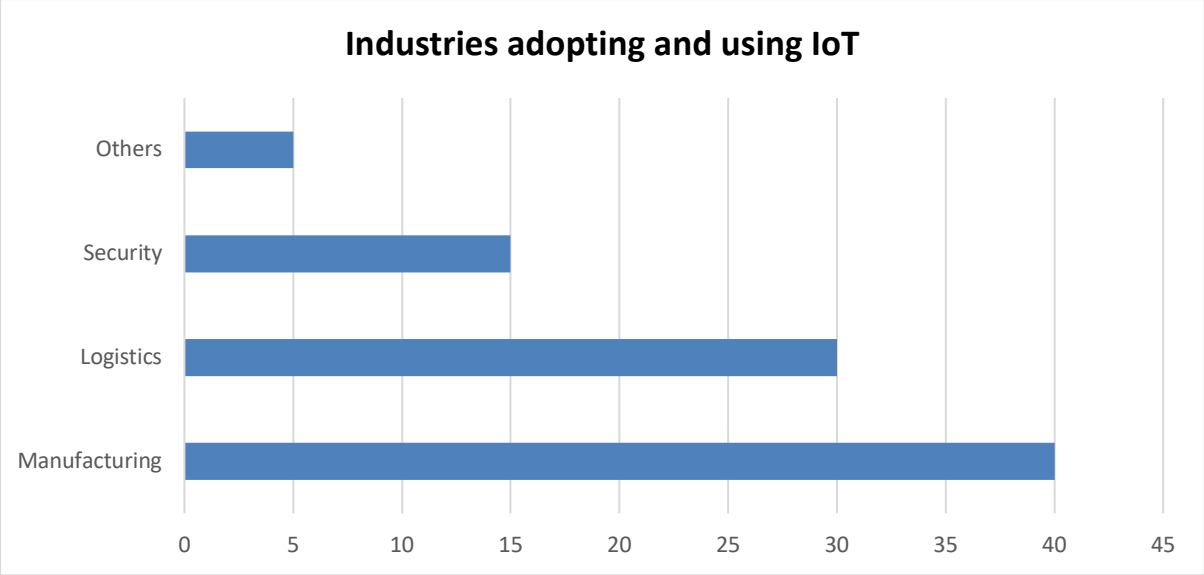


Figure 9: Industries adopting and using IoT in South Africa

4.2.3.2 Other industries that are adopting and using IoT in South Africa

Table 6 lists other industries with IoT applications that were noted by participants.

Table 6: Other industries adopting and using IoT in South Africa

Industry	In what way is IoT being applied?
Agriculture	• Sensors monitor soil moisture to inform irrigation schedules • Sensors monitor the levels of grain in silos
Automotive	• IoT is used for preventative maintenance: sensors gather information about the vehicle's tyre pressure, oil level, condition of the brakes etc. The information is then sent to an onboard diagnostics system which alerts the driver to a potential problem
Financial	• IoT is used for contactless payments
Energy	• IoT helps to balance the use of different sources of energy, including solar, batteries, grid, and generator power, to ensure the efficient mix of power sources and to optimise the way in which these sources are used
Healthcare	• Heart rate monitors and blood pressure monitors
ICTs	• Assets such as mobile operators' cellular base stations and data centres are monitored for predictive maintenance

	• Mobile operators adopt IoT, make sure they understand it, and then repackage it and sell it to their customers
Insurance	• Clients use smart geysers where they can turn their geysers on and off remotely, set and adjust the water temperature remotely, and receive alerts when the geyser is faulty
Mining	• IoT is used to monitor temperature level and air quality to assess if it is safe for workers to go underground
Public sector	• Municipalities use smart electricity meters to automate meter readings, to monitor demand and use in real time, and to deal with meter tampering • Parking management in the inner cities
Retail	• Monitoring foot traffic in shopping centres • Monitoring customer behaviour as they interact with the products on the shelves, and their movement in the store as they go from aisle to aisle • Yard management where forklifts are equipped with sensors to optimise packing and the routes that the forklift is taking • Attaching sensors to high-value stock items to mitigate loss
Building management	• Sensors are used to monitor and control air conditioners and lights for efficiency, and motion sensors are used to check building occupation

4.2.4 Challenges facing the widespread adoption and use of IoT

Several challenges will need to be addressed in order for IoT to reach widespread adoption and use. The findings from the study revealed four categories of challenges.

4.2.4.1 Challenges affecting enterprises

Long-term value realisation

In order for companies to adopt IoT they must have a business case to introduce IoT and must also understand its value and the value that it will bring them in the long term. Participant 1 remarked:

> Communicating the value is another aspect, so obviously having the value well defined and a roadmap to achieve that value at the lowest cost is important.

Another participant noted that business value for IoT is not yet entirely proven because the technology is still new and has not yet had a chance to prove a return on investment or show long-term savings.

Costs and budgets

Some companies and governments do not have traditional IoT budgets and they also lack a proper system-wide digitalisation strategy, and therefore IoT becomes more like an add-on. Another cost-related challenge that was observed is the cost of deploying IoT in terms of acquiring infrastructure, hardware, software, and the cloud. A key benefit of IoT implementation is the capability of analysing data that is collected by sensors and IoT devices; this makes it possible to derive insights from the collected data which helps to inform business decisions, and to optimise and streamline processes.

The business environment

A participant noted that South Africa is a difficult environment in which to get IoT adopted because one needs a strong business case for introducing an IoT service. The participant commented:

> I mean, it's sort of a tough environment out there when it comes to getting IoT adopted. I mean, you won't find a mobile operator like Vodacom just going out and rolling out an IoT service without partnering with another industry.

4.2.4.2 General challenges

Availability of digital skills

The availability of digital skills is one of the challenges that has an impact on IoT adoption and use. In addition to this, there is a notable lack of skills necessary for the maintenance of IoT hardware in agriculture and wildlife, which are sometimes based in remote areas.

4.2.4.3 Technology-related challenges

Cybersecurity challenges

The security of data that is collected, transmitted, and processed by IoT applications is a concern and does affect the uptake of IoT. Some IoT applications are reported to have weak architecture and weak security protocols, which render them vulnerable to cybersecurity breaches. The participants emphasised the importance of using IoT devices and cloud services that meet cybersecurity standards in IoT deployments as well as adopting a security by design approach. With regards to this approach, Participant 4 noted:

> There is this slogan for many of the cloud providers, they'll always say that security is our zero job, meaning before we do anything, the underlying security is the starting point. We need to

> be thinking the same for IoT security so that security is embedded in every layer of an IoT development process.

Privacy challenges

Privacy of data is a challenge for users because they are concerned about what the collected data is used for. It was also noted that South Africa's approach to cybersecurity and privacy-related matters is not sufficiently resourced and coordinated.

Another privacy challenge that emerged from the findings is that users are sometimes compelled to lower their privacy settings in order to obtain some services, especially those that are offered free of charge. In order to have access to these services a trade-off is required, which sees users having to lower their privacy and security settings so that they can obtain these services.

Interoperability challenges

Issues of compatibility across the technologies that interface with IoT applications have been raised; sometimes proven use cases are presented to a market as a product which offers functionality, features, and insights, but problems arise when they have to be integrated with another system.

Adoption is also reported to be limited by some developers of systems who do not share, or do not make it easy for others to use their application programming interfaces (APIs); if they do share their APIs, this comes at a high cost.

4.2.4.4 Regulation-related challenges

The participants noted that the lack of IoT-specific regulation which can serve as a guide affects the adoption of IoT. The type approval process is another regulatory challenge that was identified. This is a process whereby devices that use electronic communication must be certified: they must comply with standards and must fulfil certain regulatory requirements (ICASA, 2013). This process needs to be made flexible so as not to slow down innovation. It was also noted that a harmonised universal standard will help with the adoption of IoT. Participant 6 commented:

> A universal standard will help to deal with unharmonised regulations and requirements across different countries and regions with regard to the approval of devices. In this way, devices will not need to be tested and approved in every country.

Additionally, it is necessary to have a consistent IoT solution in order to achieve scaling across different countries. Unharmonised regulations across different countries where an IoT solution will be offered poses a challenge to scaling, because a customised solution for every country might be required.

Access to the spectrum required to operate IoT devices is another key regulatory challenge that was noted. Real-time and low-latency connectivity that is always available is necessary to operate some IoT applications. One participant stated that the regulator needs to ensure that small players in the IoT market are allocated a portion of the spectrum to increase competition in the market and to encourage the adoption of IoT.

4.3 Security and privacy

This theme explores the security and privacy of IoT by looking at the ways in which regulatory measures can be put in place to ensure that developers of IoT incorporate security into the design of their products and services. The Emirati Telecommunication and Digital Government Regulatory Authority (TDRA) has made it a requirement for the type approval of equipment to include security as part of the design of IoT equipment to ensure the implementation of security (Access Partnerships, 2021). This section also looks at the privacy-related frameworks that are in place in South Africa and the ways in which these frameworks can be adapted to address the privacy issues that are raised by IoT.

4.3.1 Security

An appropriate approach is needed to ensure that security measures are adopted and put in place by IoT manufacturers, vendors, and service providers. This approach needs to be acceptable to these stakeholders so that the goal of securing IoT devices, communication, processes, and data is achieved.

The study identified two modes by which regulatory measures can be put in place for IoT manufacturers, vendors, and service providers to adopt. The first mode is voluntary security measures comprising standards, an industry code of conduct, certifications, and guidelines, which are not compulsory to adopt. The second mode is formal regulation which is prescribed by the regulator. The responses from the participants with regard to which mode is more appropriate for IoT are presented next.

4.3.1.1 Voluntary baseline security measures

One participant suggested that the adoption of voluntary security measures, in particular the ISO2700 series of standards, has been helpful in many countries that did not have cybersecurity regulation. This was when the industry was developing and these standards could be applied in the absence of cybersecurity regulation.

The participants identified the following as the benefits of this approach: firstly, the voluntary security measures help to get buy-in from industry players; secondly, they encourage the adoption of security measures; thirdly, they provide players in the IoT market with product differentiation, as they can use the certificates to earn and build trust with users; and lastly, they help to maintain the reputation of the industry.

4.3.1.2 Formal regulation

Participants stated that formal regulation does not go as far, compared to the adoption of voluntary security measures, because it is seen as cumbersome and could create barriers for entry into the market for new entrants, thus discouraging innovation and limiting competition. Participant 7 commented:

> Formal regulation, they take long to develop and to implement, and by the time they get implemented, they're almost irrelevant.

4.3.2 Privacy

Data that is collected and transmitted throughout the IoT value chain needs to be protected from the point of collection to the point of storage. The data protection frameworks that are in place in South Africa offer provisions that protect data. The study examined whether these provisions have adequate controls, and also considered the ways in which the provisions can be adapted to IoT so that they can address the data protection issues posed by IoT.

4.3.2.1 Privacy protection frameworks

The participants' responses as to whether the current privacy protection frameworks have adequate controls were categorised as follows: (1) adequate for satisfied participants; (2) uncertain for participants who could not conclusively declare whether the controls are adequate or not; and (3) inadequate for dissatisfied participants. Figure 10 summarises the responses according to these categories.

Adequate

Some participants noted that privacy protection provisions in South Africa have adequate, relevant controls. Some likened the provisions to the General Data Protection Regulation (GDPR), saying that they are of the same standard and cover similar topics.

Uncertain

Most participants noted that privacy protection legislation is relatively new in South Africa. They therefore asserted that they cannot evaluate whether the privacy protection provisions are adequate, stating that their adequacy can only be tested in court in instances where there have been violations. They went on to say that the privacy protection frameworks need to be enforceable and that there must be consequences for transgressions. Participant 8 commented:

> I'm saying if a customer's data gets compromised or there is an issue between two competitors and then this goes to court, and then the courts have to deal with it, only then will we see how good it stands up.

Inadequate

Some participants reported that they found privacy protection provisions in South Africa to have inadequate controls. One reason provided was that the provisions lack enforceability, with one participant noting that since POPIA was introduced, the number of spam calls, SMSes, and emails has not decreased. This kind of communication is unsolicited. Participant 4 commented:

> I'm thinking, since POPIA was introduced there's more spam calling than any other time.

Another reason provided was that enforcement will be very difficult because some companies exist solely to sell people's data; for them to do this, they need to obtain access to as much data as possible. Also, some companies operate by giving their platforms to users free of charge, and in exchange users pay them with their data.

One participant said that the privacy protection provisions are not adequate because their scope is limited and they do not address issues for technologies such as IoT from a multilayered perspective.

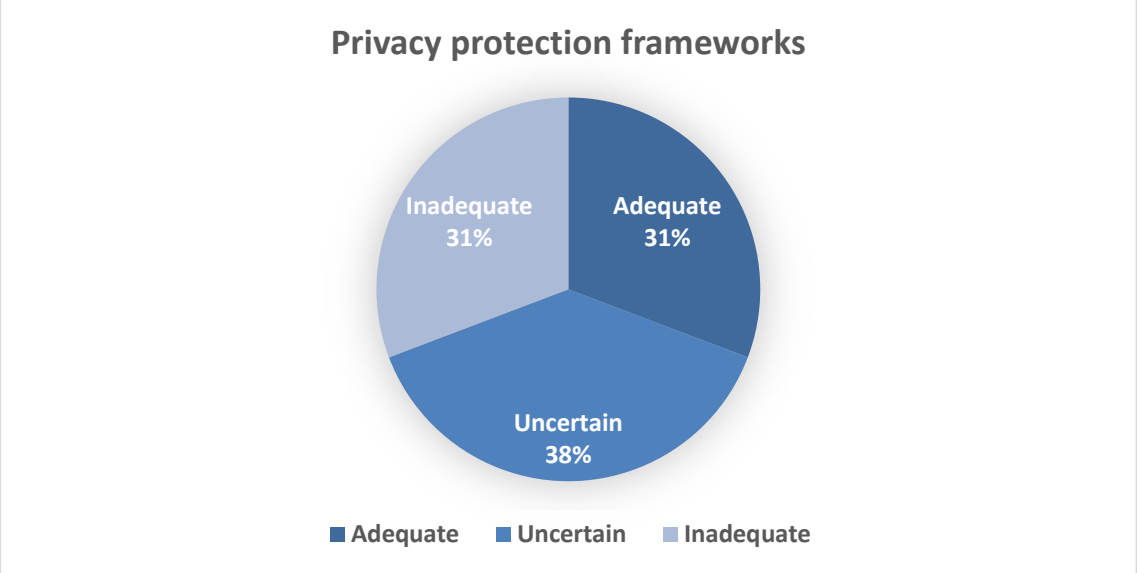


Figure 10: Adequacy of privacy protection frameworks in South Africa

4.3.2.2 Adapting existing privacy protection frameworks to IoT

The participants identified the ways in which the current privacy protection frameworks can be adapted to IoT. These included adding to the scope of data fields and the types of data that need to be protected, and going beyond protecting only personal identifying data. This will ensure that some IoT applications that do not deal with personal data are also covered.

One participant added that the design of the privacy protection frameworks should also include the review of data retention policies and that they must be clearly defined for the specific data collected.

4.4 Adaptive regulation

IoT is a dynamic technology and needs to be matched with regulation that can easily adapt to change. A clear and efficient regulation-making process is required to achieve the widespread adoption of IoT (Lee, 2018). This theme explores ways in which current regulatory approaches affect the adoption and use of IoT. It also looks at mechanisms and features that can be incorporated into regulation development and regulatory approaches to encourage the adoption and use of IoT.

4.4.1 Regulatory approaches affecting adoption

The responses from the participants can be classified into two categories that describe ways in which the current regulatory approaches are affecting the adoption and use of IoT. Some participants stated that they are limiting, and some participants said that they have no effect. Figure 11 shows the responses according to these two categories.

4.4.1.1 Limiting

Access to spectrum was identified by the participants as one of the ways in which regulation is seen to be limiting the adoption and use of IoT. This is because spectrum is needed to maximise the use of IoT devices as well as to reduce the costs of connectivity.

One of the other ways that was identified is the slow pace of regulation-making, which means that regulation lags too far behind technology, thus affecting the adoption of the technology. Participant 9 commented as follows:

> The problem is that from the point where technology capability becomes available to where regulation is being formulated and discussed to where regulation is actually implemented, that gap is so wide. By the time we get here, this technology might be superseded by another technology already.

Also, the failure to harmonise standards and regulations across different countries is affecting adoption. This harmonisation is necessary so that a product is not subjected to testing in every country before it is adopted. The testing can be done once and then any country can adopt the product.

Participants noted that the levels of understanding and knowledge of emerging technology by regulators is another way in which regulatory approaches are limiting the adoption of IoT. The learning curve becomes too great for regulators as they might not understand IoT, so ultimately they are unsure about what regulatory measures need to be put in place. They

then try to retrofit existing regulations onto IoT and thus stifle the benefits of the technology. Participant 4 commented:

> So I feel like regulators need to also have in their teams and incorporate people that understand technology as well, so that it's kind of aligned. While you're protecting people and protecting people's data and protecting organisational data as well, you need not be stifling innovation.

Regulation always lags behind technology, but the gap can be narrowed by ensuring that regulators understand the technology.

4.4.1.2 No effect

One participant noted that there is no specific IoT regulation in South Africa so it is impossible to say whether regulation is affecting the adoption of IoT. The participant stated that there are no specific restrictions on IoT compared to other technologies or even general information technology. When designing an IoT solution one needs to ensure that one has the correct required safeguards in place to secure the data, and one must incorporate internal policies about preventing security breaches. These must be designed into the solution. Participant 11 commented:

> IoT doesn't have its own rulebook. So I wouldn't say there's any specific legal aspects that are driving or preventing its adoption more than any other technology, per se.

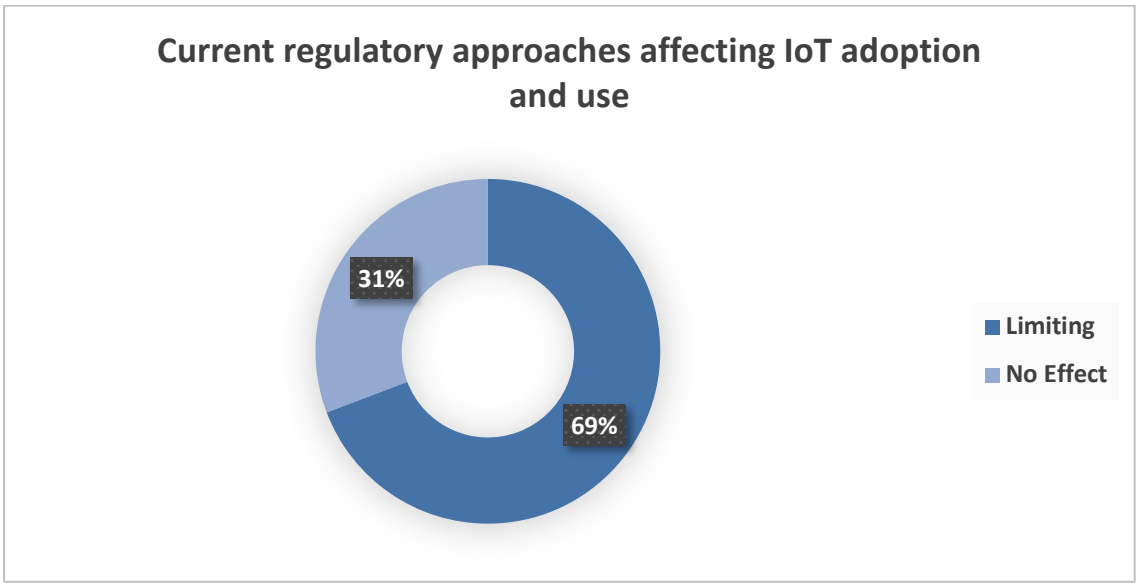


Figure 11: Effect of current regulatory approaches on IoT adoption and use in South Africa

4.4.2 Making regulation more adaptive

The participants identified certain features that need to be incorporated into regulations and the process of regulation-making, as well as mechanisms that need to be employed to achieve the kind of regulations that are relevant and that can easily adapt to changes. These features and mechanisms are seen as creating an enabling environment for the uptake of IoT.

4.4.2.1 Collaboration and consultation

One participant described the regulatory approach of the telecommunications sector regulator which regulates some of the entities involved with IoT in South Africa as lacking collaboration and having minimal consultation processes. Participant 6 asserted:

> I know that there is some kind of consultation, but that consultation only happens when the regulator is intending to publish new regulations. And then after that, the industry is left to deal with the regulation, whether it is right or wrong. If the industry is not happy with certain regulation, then it's impacting your business. That process gets handled through the courts.

The participants identified consultation and collaboration among stakeholders, which include regulators, manufacturers, developers, and vendors of IoT, as some of the ways that can enable regulation to be more adaptive to the changes and advancements in technology. It was noted that because technologies such as IoT cannot be pre-regulated, regulators need to work alongside the industry to monitor how the technology develops. This process needs to be iterative, where the products are developed and tested, and regulations are being updated at the same time. The benefit of such collaboration will lead to standardisation and a common understanding, especially in IoT that cuts across different industries. It will also lead to data-driven regulation which will be better received by the regulated entities. The other benefit of consultation that was noted was that it will create a space for IoT industry players to propose what they need to improve the adoption of IoT.

4.4.2.2 Apportioning of responsibilities

A need to determine sets of responsibilities for the industry and regulators was noted. One participant stated that there is a misconception that regulation is a function of government, and the IoT industry needs to enable itself through self-regulation.

Having mechanisms in place whereby a regulatory body takes responsibility for the regulation of IoT while being guided by an industry council of subject-matter experts was identified as one way in which the apportioning of responsibilities can be achieved. This proposed industry council could develop standards and specifications and those recommendations could be implemented by the regulatory body.

4.4.2.3 Prototyping mechanisms

One way of making regulation more adaptive is for regulators to adopt principles of rapid prototyping and agile development for the regulatory environment so that the process of regulation-making is speeded up. Rapid prototyping will ensure that the regulatory process is fast and irrelevant regulations can be retired and new ones put in place so as not to hinder the uptake of IoT. This will also help to close the gap between the pace of technology and regulation. It was also noted that regulators need to work closely with industry as products are being prototyped. This will facilitate the adoption of a soft-touch regulatory approach which will be a result of them having worked closely with industry as a stakeholder. This will also reduce the time that it takes to develop regulations and will enable businesses to take their products to market on time. A soft-touch regulatory approach is described by Sowell and Brass (2020) as a type of approach that allows regulated entities to put in place their own means of achieving regulatory goals.

4.4.2.4 Regulatory sandboxes for IoT

One participant pointed out that having a mechanism such as regulatory sandboxes for IoT will give regulators the opportunity to see how the development process of products unfolds so that when they draft regulations they will know and understand the technology better. It was added that this mechanism will help the regulators to develop fit-for-purpose regulations as the people who develop the technology will be working alongside them. Learnings from sandboxing will ensure that the approach to regulating technologies such as IoT comes from a place of understanding them. It will also ensure that regulation is not just copied from other developed nations, and that it considers the context of the country for which it is developed. Participant 13 commented:

> Regulators should actually be involved in innovation hubs that have been set up around South Africa. The regulators should have its presence in product development so that they understand how these things work.

4.5 Summary of the chapter

The chapter presented findings from data that was collected through interviews with the study participants. The findings revealed that IoT is seeing a fast rate of adoption and use in South Africa, mainly due to improved levels of internet connectivity. The uptake is reported to be driven by environments where IoT is being incorporated in a retrofitting way onto existing environments, and also onto legacy equipment and systems, with the aim of achieving efficiencies, the optimisation of processes, and costs savings in some instances. One participant described this phenomenon as “incremental innovation”. The leading industries where IoT adoption and use are witnessed are the manufacturing, logistics, and security industries. The participants also identified and described challenges related to IoT users, technology, and regulation that are affecting the widespread adoption and use of IoT.

The need for a security by design approach in order to secure IoT products, systems, processes, and data was identified. The participants could not evaluate the adequacy of the data protection provisions that are contained in the current privacy frameworks in South Africa with certainty. They opined, however, that they can be adapted to IoT and highlighted the ways in which they can be adapted to address privacy issues that are raised by IoT.

Lastly, the data revealed that the current regulatory approaches have a limiting effect on the adoption and use of IoT. The participants pointed to a wide gap between the pace of regulation-making and the pace of developments in IoT and outlined the factors contributing to this gap. The features and mechanisms that need to be incorporated, employed, and designed into regulations and the process of regulation-making to make it more adaptive were also identified and discussed.

CHAPTER 5: A SOCIO-TECHNICAL ANALYSIS OF THE ADOPTION AND USE OF THE INTERNET OF THINGS IN SOUTH AFRICA AND THE IMPLICATIONS FOR ADAPTIVE REGULATION

5.1 Introduction

This chapter provides an analysis of the data that was presented in chapter 4. Saldana (2013) explains data analysis as the steps taken to search for the meanings of phenomena and to provide an explanation for the causes thereof. The study's findings are analysed by mapping them against the components of the STS theoretical framework. The interdependent components of the STS theoretical framework are used as theoretical lenses to guide the understanding of the adoption and use of IoT in South Africa and the implications for adaptive regulation. The major components of the STS theoretical framework comprise the social and technical subsystems, which in turn have four interactive elements i.e. technology, tasks, structure, and people (Bostrom & Heinen, 1977), as depicted in Figure 12.

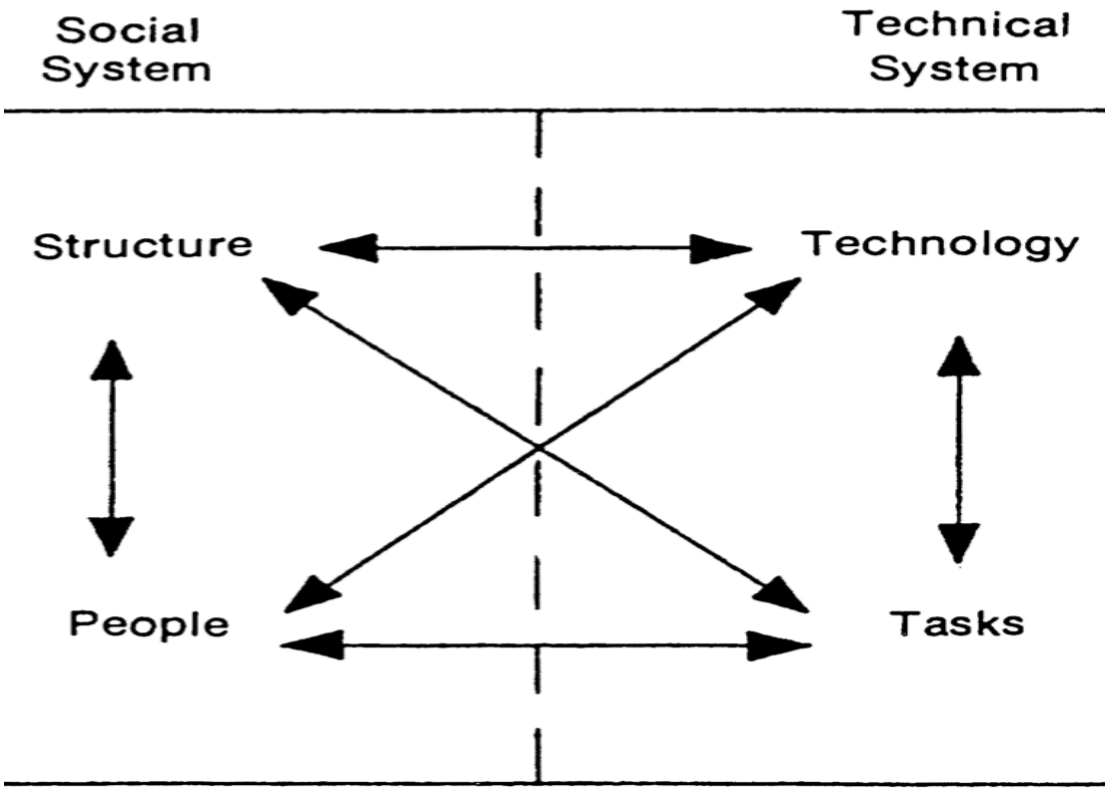


Figure 12: Socio-technical framework Source: Adapted from Bostrom and Heinen (1977)

A technological system is not only shaped by the technical artefacts such as hardware, software, and processes, but it is also shaped and given meaning by the diversity of social interactions (Bijker, 1995). The process of developing a technology is not an independent

occurrence; it is carried by the relevant social groups that are affected by it and who interact with it (Bijker, 1995). By analysing the study's findings through the STS theoretical framework, this study not only considers the technical aspects IoT, but also considers the social aspects of IoT, where a system of rules and regulations determine its development, adoption, and use. The study also takes into account the different social groups that are affecting and are affected by the development, adoption, and use of IoT. Shin (2012) explains that a socio-technical view can offer a comprehensive and consolidative framework to capture and show the relationship between humans and technology in IoT. Additionally, the STS framework is appropriate for exploring issues that encompass social and technical elements and the reciprocal relationship between them (Mumford, 2006).

This chapter presents the analysis of data by first discussing the socio-technical subsystems with each of its relevant elements, and then the elements are related to each other to reflect and elucidate the interaction between the social and technical subsystems. The conceptual framework that was initially postulated in chapter 2 is then revisited to reflect on its components and to develop an adapted framework taking into consideration the themes that emerged from the data analysis.

5.2 The technical subsystem

The study will explain the technical subsystem through the elements of technology and tasks.

5.2.1 A perspective on IoT technological elements and technology-related challenges in South Africa

The technology element captures the technical elements that are required to enable the adoption and use of IoT as well as technology-related issues that need to be addressed in order to achieve the widespread adoption and use of IoT.

5.2.1.1 Connectivity required for IoT

Spectrum is an important enabler of IoT and is necessary to enable the diverse and wide-ranging IoT use cases (Access Partnerships, 2021). The findings point to the need to allocate a portion of the spectrum to the smaller players involved in IoT to increase competition in the IoT market and to encourage the widespread adoption and use of IoT. An increase in participation by various players in IoT will provide users with competitive prices, thus making IoT more accessible.

There are notable ongoing initiatives by the telecommunications regulator ICASA through the International Mobile Telecommunications (IMT) spectrum auction to increase competition in the telecommunications sector and to reduce the costs of communication (ICASA, 2021). ICASA also published the final Radio Frequency Spectrum Assignment Plan for the frequency

band 410 MHz to 430 MHz in 2023, which declared that this spectrum band would be made available for emerging applications, including IoT (ICASA, 2023).

5.2.1.2 Addressing interoperability concerns for connected devices

The ease of integrating IoT into an existing environment is important to ensure communication, the exchange and sharing of data, and the effective performance of the overall system. The end goal of an IoT deployment is to have a seamless environment which is interoperable, with objects integrating and working effectively with others (Gubbi et al., 2013).

It emerged from the findings that the interoperability of IoT with other systems and technologies poses a challenge to the adoption and use of IoT. The use of different communication tools, security protocols, and closed solutions makes the sharing and integration of resources with other devices or services difficult. Weber and Zarko (2019) note that the protocols used in some of the IoT deployments are proprietary and do not use open standards or open interfaces.

To address this concern, ICASA issued the Equipment Authorisation Regulations 2022 which are aimed at ensuring the interoperability and interconnectability of electronic communication equipment (ICASA, 2022). ICASA's 5G forum has a working group that is focused on standards and plans to address interoperability issues as one of its objectives. Furthermore, the adoption and application of standards that are developed by international standards organisations such as the ITU and ISO, and international standards-developing organisations such as ETSI and the NIST by device manufacturers, developers, platform, and solutions providers can ensure the seamless integration of devices and systems in an IoT system.

5.2.1.3 Issues of cybersecurity and the impact of privacy on the adoption and use of IoT

The lack of and insufficient security and privacy protection measures in IoT devices, products, and systems pose challenges for the adoption and use of IoT. The findings revealed that cybersecurity and privacy pose a challenge to the adoption and use of IoT because the security of data that is collected, transmitted, and stored by IoT applications and the privacy of that data is a factor that contributes to the development and adoption of the technology. The concerns of security and privacy have an impact on users' adoption of IoT; moreover, inadequate privacy controls expose users to risks (Cichy et al., 2021).

POPIA is the data protection law in South Africa that provides for the protection of personal data. The Cybercrimes Act provides measures to prevent cybercrimes in South Africa and to equip law enforcers with the necessary powers to enforce the law. To address this from an IoT perspective, the findings showed that regulatory frameworks that are specific to IoT need to be developed to put measures in place to deal with security and privacy challenges. The

security and privacy measures need to be incorporated into the design of IoT devices, products, and systems at the outset by the device manufacturers and the developers of IoT. By applying the security by design approach, manufacturers and developers can ensure that IoT products and systems are resilient to cyberattacks and as free as possible from vulnerabilities (WEF, 2023).

5.2.2 Tasks for fostering the adoption and use of IoT

This element refers to activities that enable IoT to be adopted and used. The activities include the development of different applications and the implementation of IoT in various industries and user environments. IoT is adopted and used in a variety of industries, mainly for tracking, monitoring, controlling, automating, optimising, and streamlining business processes with implementations realised either by adding and incorporating it onto existing systems or by implementing new IoT solutions and services.

The findings showed that the manufacturing, logistics, and security industries are the top adopters of IoT in South Africa. Other industries such as agriculture, energy, insurance, and retail, to name a few, are also adopting and using IoT. The most prevalent implementation of IoT is incremental innovation where it is added onto existing systems and environments.

The availability of IoT networks such as Sigfox, NB-IoT, and 5G in South Africa, which can be used for most IoT applications in any industry, will enable the adoption and use of IoT. Also, the Centre for the Fourth Industrial Revolution (C4IR) in South Africa ran a project in 2022 whose aim was to accelerate the adoption of IoT by small- and medium-sized enterprises in the automotive sector (Centre for the Fourth Industrial Revolution South Africa, 2023).

5.3 The social subsystem

The social subsystem describes people, the relationship between them, and the structures of authority (Bostrom & Heinen, 1977). The elements of structure and people will be explored to assist with understanding the social subsystem for this study.

5.3.1 A take on structures regulating IoT in South Africa

The structure element covers the systems of authority with regard to the regulations and rules associated with IoT. It also covers issues of standardisation relating to IoT.

5.3.1.1 The type approval process

The compliance of devices with technical standards is key to ensuring interoperability and safety in an IoT ensemble. The principal aim of subjecting devices to the type approval process is to certify that they comply with technical standards and that they fulfil certain regulatory requirements.

The findings showed that this process, which is overseen by ICASA in South Africa, needs to be more flexible than it is currently. This will help to encourage participation by many more IoT manufacturers and developers, and will also help them to take their products to market on time. The findings further showed that this process needs to be harmonised across different countries and regions, so as not to subject the devices to testing and approval in the different countries where IoT manufacturers, developers, and solutions providers may wish to participate and scale their IoT offerings. This also applies to IoT that straddles country or regional boundaries.

As a measure to address the harmonisation of the type approval process, a project named "Support for Harmonization of ICT Policies in Sub-Saharan Africa" (HIPSSA) has as its main goal the development and promotion of the harmonisation of telecommunications and ICT regulations and legal frameworks in sub-Saharan Africa. One of its initiatives is harmonisation of the type approval procedures across sub-Saharan countries and regions (ITU, 2009).

5.3.1.2 The regulatory aspects of security and privacy

The incorporation of security measures in IoT products and systems by manufacturers and developers is necessary to secure data that is collected, exchanged, and shared in an IoT system, and also to prevent malicious attacks on the system and any of its components.

The study's findings identified the adoption of security measures on a voluntary basis as a way to encourage manufacturers and developers of IoT to adopt and implement security measures for their products and systems. The findings further highlighted that incentives such as certifications can be used to encourage and promote the application of standards and the adoption and implementation of security and privacy measures. In addition to issues pertaining to security, it also emerged from the findings that the existing privacy protection frameworks only provide protection for personal identifying data and do not provide for the other types of data.

According to the OECD (2022), there are insufficient incentives for IoT manufacturers and developers to incorporate security into the design of their products. One way to promote the adoption of security measures is by using certifications for IoT devices and systems. This is also necessary to earn the trust of users (Cirne et al., 2022). Furthermore, one measure to address the incorporation of non-personal data into the privacy protection frameworks in South Africa is the draft Data and Cloud Policy of the Department of Communications and Digital Technologies, which aims to extend some provisions of POPIA to include non-personal identifying data.

5.3.1.3 Employing collaborations to facilitate regulation development

Collaborations play the key role of facilitating an effective response to new technologies. Regulators also need to aim for collaborative, consultative policies and regulation, which

includes the participation of the various stakeholders as well as other cross-sectoral regulators (ITU, 2018).

The study's findings revealed that collaboration between manufacturers, developers of IoT, and regulators will facilitate the development of regulations that are well received by regulated entities and that can easily adapt to changes. The findings also revealed that regulators need to be knowledgeable about IoT, and that a mechanism such as regulatory sandboxes for IoT can help them to better understand it. One key role of regulatory sandboxes is to keep regulators informed and updated about innovative solutions. Regulatory sandboxes also promote and increase collaboration between regulators and the industry (Pygma Consulting, 2022).

There have been some notable successes in the use of regulatory sandboxes in South Africa. One success was in the telecommunications sector for the development of a regulatory framework for TV Whitespaces (TVWS) technology, and another was in the fintech industry which enabled an innovative business to launch its blockchain technology to the market (Pygma Consulting, 2022). Currently, no regulatory sandboxes have been set up for IoT.

5.3.2 The element of people affected by and affecting IoT

The people element describes people as users of IoT and regulated entities. These parties are stakeholders in IoT, they can affect or be affected by this technology, and they are an integral part of IoT.

5.3.2.1 Users of IoT

Users of IoT are important to its development, and they have a direct effect on its adoption and use. It emerged from the findings that one of the ways for IoT to reach widespread adoption and use is for users to see value in IoT and for users who use IoT for business to see long-term value and the savings created by IoT. IoT offers users smart and connected products, new functionalities for business, and increased reliability, more product use, and capabilities that go beyond the traditional product limitations (Molling & Klein, 2022).

IoT tools that are available for users to deal with the effects of the electricity crisis in South Africa are providing value. People are using these tools to monitor their back-up batteries, generators, and consumption, providing them with costs savings and business continuity (Tech in Africa, 2023).

5.3.2.2 Regulated entities involved in IoT

The entities that manufacture, develop, and provide IoT solutions and products form part of the regulated entities in an IoT market. In South Africa, these entities are regulated by the telecommunications regulator, the information regulator, and the specific sector regulator whose scope covers the industry in which an entity operates.

The findings articulated a need for the regulated entities and regulators to work in collaboration to facilitate the development of regulation for IoT that is informed by those who are affected by it, while offering consumer protection. Key stakeholders in IoT need to develop IoT in close collaboration, with the aim of integrating the legal and technological issues (Ghaffari et al., 2019).

The ICASA 5G Forum Use Case Working Group is a collaboration between different stakeholders from the regulator, research organisations, and manufacturers from different industries and network operators, among others. It is looking at use cases for 5G and aims to promote the adoption of 4IR technologies such as IoT (ICASA, 2021).

5.4 Socio-technical system – An interaction between social and technical subsystems

To understand the essence of a technological phenomenon involves comprehending the interaction between social structures, industry, policy, and technology (Shin, 2014). This section frames the system as a space within which the two subsystems of the STS, namely the technical and social subsystems, interact. It describes and presents the interrelationships between these two subsystems through their respective elements, namely the technological element, which is aimed at addressing IoT challenges and increasing IoT adoption and use; the structure element, which covers systems of authority, rules, and technical standards for IoT; the tasks element, which comprises the required activities to enable IoT adoption and use; and lastly, the people element, which includes people who have an effect on IoT and those who are adopting IoT and are affected by it. Song, Cai, Chahine and Li (2017) explain that the development of an IoT implementation such as smart cities needs people and institutions of authority such as regulators and policymakers as much as it needs technical infrastructure such as hardware and software.

The interactions are described by first illustrating the STS elements in tables and then explaining them further in the subsections below. The technology element is focused on the security and privacy subcomponents as these fall within the scope of this study.

5.4.1 Technology and structure

Table 7: Interaction between the technology and structure elements

Technology	Structure
Interoperability	Type approval process
Cybersecurity and privacy	Adoption of security and privacy measures
	Adapting privacy protection frameworks

	Collaboration

Regulation and standards related to IoT are required to deal with the interoperability, security, and privacy challenges of IoT that were identified in the findings. Also, a collaborative approach through the use of regulatory sandboxes can provide a space where IoT-related regulation that is aimed at addressing issues of interoperability, security, and privacy can be tested and developed.

5.4.2 Technology and tasks

Table 8: Interaction between the technology and tasks elements

Technology	Tasks
Interoperability Cybersecurity and privacy	IoT applications and implementations

The technological elements of IoT are necessary building blocks that enable the development of IoT applications. The adoption of these applications and their use in various industries can be enhanced by the development of IoT that has security and privacy protection measures and can integrate with other devices and systems with ease.

5.4.3 Tasks and people

Table 9: Interaction between the tasks and people elements

Tasks	People
IoT applications and implementations	Regulated entities Users

IoT market-players play a role in the development and enabling of IoT adoption and use in different industries because they are the manufacturers, developers, and solution providers of IoT devices, products, and systems. Also, they are in a position to encourage the further adoption and use of IoT by gaining the trust of users by dealing with the security, privacy, and interoperability challenges related to IoT.

5.4.4 Structure and people

Table 10: Interaction between the structure and people elements

Structure	People
Type approval process Adoption of security and privacy measures Adapting privacy protection frameworks Regulatory sandboxes	Regulated entities Users

Regulation puts in place measures for the development of secure, privacy-protecting IoT devices, products, and systems by regulated entities who are involved in the IoT market. Collaboration between regulators and players in the IoT market is one of the ways to ensure that the development of IoT regulation involves stakeholders who can affect the development of IoT.

5.4.5 Technology and people

Table 11: Interaction between the technology and people elements

Technology	People
Cybersecurity and privacy Interoperability	Regulated entities Users

The manufacturers, developers, and solutions providers who are players in IoT need to ensure that they develop devices, products, and systems that are resilient to attacks, secure, provide privacy protection to data, and are interoperable in order to encourage users to adopt and use IoT.

5.4.6 Structure and tasks

Table 12: Interaction between the structure and tasks elements

Structure	Tasks
Type approval process Adoption of privacy and security measures Adapting privacy protection frameworks Regulatory sandboxes	IoT applications and implementations

Regulation plays a key role in creating an enabling environment for IoT to be adopted and used by ensuring that IoT devices, products, and systems are safe for users. The collaborative environment that regulatory sandboxes offer can benefit the development of IoT applications that are market-ready as they will be developed in an environment that allows for regulation to be adapted and adjusted to suit the development of the technology.

5.5 Developing a socio-technical framework for the adoption and use of IoT in South Africa

This section presents an adaptation of the STS framework to establish the required collaborations for the adoption and use of IoT in South Africa. The interactions between the elements of the STS that were explained in section 5.4 exposed the need to incorporate the element of collaboration which emanated from the interactions between the technology, tasks, structure, and people elements.

Collaborations and engagements that foster collaboration emerged from the study as an important factor that is present in the interactions of the technical and social subsystems. Accordingly, they need to be incorporated into these interactions. Various organisations have had to seek collaborative innovative approaches to and collaborative ways of structuring themselves as a result of experiences related to the COVID-19 pandemic (Mahdad et al., 2021).

Table 13 below explains the role that collaboration plays in the interfacing process of the elements of the STS framework as described by the study's findings.

Table 13: Collaboration factor in the interaction of the STS elements

STS elements		**Collaboration factor**
Technology	**Structure**	

Connectivity Interoperability Cybersecurity and privacy	Type approval process Adoption of privacy and security measures Adapting privacy protection frameworks Regulatory sandboxes	Collaboration can be used to test the adaptation of privacy frameworks to include non-personal identifying data for IoT by regulators, IoT manufacturers, and developers
Technology	**Tasks**	Interoperability, security, and privacy challenges that affect the adoption and use of IoT can be addressed by regulators, manufacturers, and developers of IoT devices, products, and systems working collaboratively to test a regulatory approach that will ensure that IoT is designed with security and privacy protection measures and is interoperable
Connectivity Interoperability Cybersecurity and privacy	IoT applications and implementations	
Tasks	**People**	Collaborations offer manufacturers, developers, and solution providers of IoT an opportunity to gain the trust of users by addressing security, privacy, and interoperability challenges related to IoT devices, products, and systems by working with regulators to develop regulation that is specific to IoT and deals with IoT-related issues
IoT applications and implementations	Users and regulated entities	
Structure	**People**	Collaborations can be used as a tool by regulators to ensure that regulation is informed by people who are affected by IoT. To achieve this, they will need to look at issues that affect users such as extending the scope of privacy frameworks to include non-personal data and ensuring that IoT devices, products, and systems have security and privacy protection measures designed into them
Type approval process Adoption of privacy and security measures Adapting privacy protection frameworks Regulatory sandboxes	Users and regulated entities	
Technology	**People**	

Connectivity Interoperability Cybersecurity and privacy	Users and regulated entities	Collaborations can be used by regulators and regulated entities to test the provisions of regulations that are developed to ensure the interoperability and interconnectability of electronic communication equipment by regulators to evaluate whether they are relevant and suitable for IoT
Structure	**Tasks**	Manufacturers, developers, and solutions providers of IoT can leverage the absence of regulation that normally applies in a market and the presence of regulators in a collaborative space such as a regulatory sandbox to develop innovative IoT applications that are market-ready to boost the adoption and use of IoT in different industries
Type approval process Adoption of privacy and security measures Adapting privacy protection frameworks Regulatory sandboxes	IoT applications and implementations	

It is clear that collaboration is a key factor, and the synthesis of the elements above highlights the collaborative elements that need to be looked at. Based on this synthesis of the STS framework elements, namely technology, structure, tasks, and people with the element of collaboration, the adapted STS framework is illustrated in Figure 13 below. This adapted framework emerged from the interactions of the STS elements which led to the incorporation of collaboration with the four elements of the STS. This is how the researcher views the STS framework. It is not intended to replace the STS framework by Bostrom and Heinen (1977), but rather to reflect the findings of the study based in South Africa on the adoption and use of IoT and the implications for adaptive regulation.

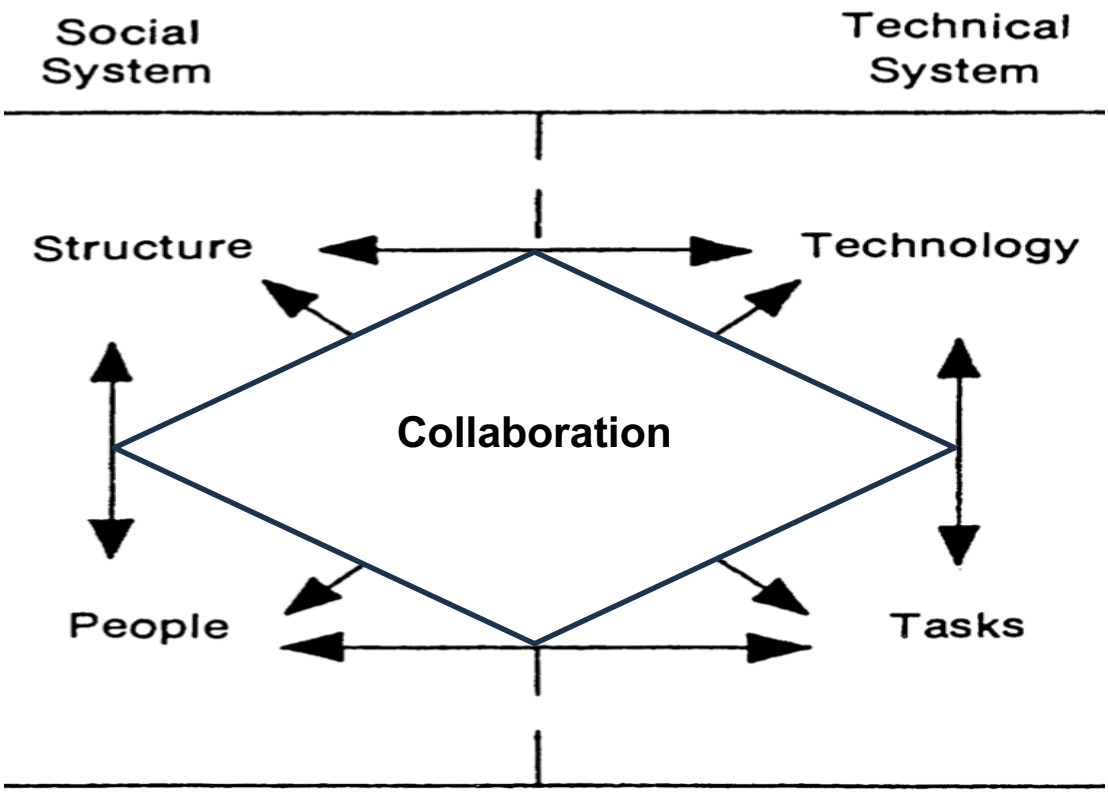


Figure 13: Adapted STS framework Source: Adapted from Bostrom and Heinen (1977)

5.6 Summary of the chapter

This chapter provided an analysis of the study's findings in line with the STS theoretical framework. The social and technical subsystems of the STS framework were defined by categorising data as corresponding to them, and the system was then determined by describing the relationships between the elements of the technical and social subsystems. Finally, an adapted STS framework was developed by incorporating the element of collaborations so that these are involved in the process of interactions by the elements of the STS framework. This adapted framework is suitable for exploring the adoption and use of IoT in South Africa, the regulatory, security and privacy issues affecting it, and the ways to develop adaptive regulation for IoT.

CHAPTER 6: AN APPROACH TO ADVANCING THE ADOPTION AND USE OF THE INTERNET OF THINGS AND THE WAY FORWARD

6.1 Introduction

The advancement of IoT thrives in an enabling, adaptive regulatory environment and the development of secure devices, products, and systems for users. To provide an understanding of this, the study adopted a qualitative approach and used thematic analysis to analyse data that was collected through interviews.

This chapter concludes the study by first revisiting the research objectives that were defined in chapter 1 to assess what the findings have achieved. Concluding remarks about the major themes from the study are made, followed by the key contributions, limitations, evaluation of the study, and recommendations. Lastly, the way forward is presented by discussing recommendations for future research.

6.2 Evaluation and contributions of the study

This section presents an evaluation of the study by looking at how the analysis of data helped to answer the research questions posed in chapter 1, and also outlines the contributions made by the study.

6.2.1 Evaluation of the study

The main research question was to establish how regulatory approaches are affecting the adoption and use of IoT in South Africa. The two sub-questions looked at the way in which challenges of security and privacy affect the adoption and use of IoT, as well as ways in which adaptive regulations in relation to IoT can be developed and implemented in South Africa. By employing a thematic analysis method, the social and technical aspects of IoT as well as the interaction between them was discussed using the STS framework by Bostrom and Heinen (1977). It emerged that this format of the STS framework needed to be adapted to explore the adoption and use of IoT in South Africa and the regulatory, security, and privacy factors affecting it. This led the researcher to develop an adapted STS framework which has the element of collaborations present in the interactions between the STS elements. This framework ensures that collaborations are used to develop regulations that are relevant and adaptable to IoT, and it also ensures that the solutions to the challenges of security and privacy are facilitated by collaboration between regulators and IoT manufacturers, developers, and solutions providers. It ultimately furthers the development of IoT and promotes its adoption and use.

6.2.2 The study's contributions

The sections below discuss the contributions made by the study to existing literature and practice.

6.2.2.1 Contributions to the body of knowledge

The study took a different approach to developing an understanding of how the adoption and use of IoT as an evolving technology is affected by regulatory approaches, thus adding to the existing body of knowledge on the adoption and use of evolving technologies in developing countries. The study also brought to the fore an understanding of the importance and implications of security and privacy on IoT, and ways to address these issues and to develop relevant and adaptable regulations for IoT in South Africa. IoT is still developing and is being used in many industries, therefore understanding that its adoption and use are affected by regulations, security, and privacy and that it needs regulation that is adaptable to it benefits the body of knowledge.

6.2.2.2 Practical contributions

The study employed an STS theory as an analytical lens through which the interplay between the technical and social aspects of IoT helped to develop an understanding of how to address the challenges of regulation, security, and privacy that are affecting the adoption and use of IoT, as well as ways to develop relevant regulations for IoT. The insights derived from this study are applicable to addressing issues of regulation, security, and privacy for IoT and the development of relevant regulations for IoT in South Africa.

6.3 Challenges of the study

The researcher experienced difficulties in accessing a number of potential participants from the regulators and other industries because the researcher did not have relationships with the potential participants; this affected the sample size and the breadth of representation of the industries. Although a perspective is missing from interviewing regulators, it was supplemeted from literature by looking at reports from the telecommunications regulator. The research also encountered some delays due to slow response rates and the slow securing of interview appointments. Also, the process of obtaining permission letters to interview participants from the relevant government departments was long, and in most cases the researcher did not obtain access to those participants.

6.4 Summary of findings

A summary of the study's findings is presented below by discussing how the research objectives that were outlined in chapter 1 were addressed in light of the findings.

6.4.1 Research Objective 1: To explore how regulatory approaches to IoT affect its adoption and use

This research objective sought to explore ways in which the adoption and use of IoT in South Africa is affected by the regulatory approaches related to IoT. The approaches concerning regulatory aspects of type approval process, spectrum, security, privacy, and interoperability as well as the collaborative regulatory approach are discussed in the subsections below.

6.4.1.1 Spectrum and type approval regulatory elements

Aspects of regulation that deal with type approval of equipment and spectrum are key for the development of IoT and the subsequent levels of IoT adoption and use. They are both fundamental requirements for IoT devices, products, and systems to be operational, to enter the market, and to advance the growth of IoT. The notable needs for the allocation of spectrum to smaller players in IoT and the need for the harmonisation of the type approval process across different countries and regions are being addressed by the relevant regulatory authorities and regulatory agencies. In addition to the auctioning of IMT spectrum aimed at increasing competition in the telecommunications sector, among other things, ICASA published the final Radio Frequency Spectrum Assignment Plan for the frequency band 410 MHz to 430 MHz in 2023, which stated that this spectrum band will be made available for emerging applications, including IoT (ICASA, 2023). Also, the HIPSSA project has as one of its initiatives the harmonisation of the type approval procedures across the sub-Saharan countries and regions (ITU, 2009).

6.4.1.2 Security, privacy, and interoperability of IoT

The security, privacy, and interoperability of IoT devices and systems are important requirements for IoT. Employing measures to ensure their implementation in IoT serves to ultimately encourage users to adopt the technology and provides them with the knowledge that the devices and systems are secure from vulnerabilities and can be integrated seamlessly into an environment. Through the adoption of standards, device manufacturers, developers, platforms, and solutions providers are enabled to provide IoT that is secure and interoperable. The adoption of these standards needs to be done on a voluntary basis so that regulated entities are willing to adopt them. To promote and support the adoption of standards, incentives such as certifications can be used to empower and motivate IoT device manufacturers, developers, and solutions providers. Additionally, certifications will help them to differentiate their devices and products in the market, earn the trust of users, and demonstrate accountability for their devices and products.

6.4.1.3 A collaborative approach to regulating IoT

Collaboration between regulators, manufacturers, developers, and solutions providers of IoT in developing regulations leads to regulations that are relevant to IoT, adaptable to change,

well-received by regulated entities, and informed by the people who are involved in IoT. Collaboration can also be used in developing regulations specific to IoT which will help to address the challenges of interoperability, security, and privacy. Dealing with these challenges will boost the value that is derived from IoT for users and business users and in turn provide an advantage for the widespread adoption and use of IoT.

6.4.2 Research Objective 2: To identify and explore ways in which the challenges of security and privacy can affect the adoption and use of IoT

Factors such as the inherent vulnerability of IoT due to the interconnectedness and heterogeneity of devices and stakeholders, as well as inadequately secured IoT devices, products, and systems, affect security and the privacy of data that is collected, exchanged, and shared in IoT. These have a negative impact on the adoption and use of IoT, mainly because users are not confident that their data, devices, and systems are secure. To address this, IoT manufacturers, developers, and solution providers need to adopt the security and privacy by design approach. With this approach security and privacy-protecting measures are embedded into IoT devices, products, and systems from the outset. Additionally, the adoption of IoT that does not use personal identifying data needs to be enhanced by adapting existing privacy protection frameworks to include and cover other types of data.

6.4.3 Research Objective 3: To explore and understand the ways in which adaptive regulation can be developed and implemented with respect to IoT

An environment which fosters collaboration between regulators and IoT manufacturers, developers, and regulators helps to adapt regulation to technology as it develops. Regulatory sandboxes for IoT are an environment which offers regulators a space to increase their knowledge about IoT while working alongside manufacturers and developers in the development of their products. Regulators are then in a better position to develop relevant and informed regulation for IoT that takes the context of the country into account.

6.5 Recommendations

The following recommendations are presented for consideration by regulatory authorities and the manufacturers, developers, and solutions providers of IoT in South Africa.

6.5.1 Recommendations for regulators

The following subsections outline recommendations for consideration by regulatory authorities.

6.5.1.1 Addressing the adoption and implementation of security and privacy protection measures

Regulators need to use incentives to encourage and empower IoT manufacturers and developers to adopt and implement the security and privacy by design approach to ensure that IoT devices, products, and systems are secure and offer privacy protection. Incentives in the form of certifications which offer product differentiation, demonstrate accountability, and help to gain trust from the users can be applied to motivate and promote the adoption and implementation of the security and privacy by design approach.

6.5.1.2 Establishing regulatory sandboxes for IoT

Regulators need to leverage the collaborative quality of regulatory sandboxes to develop a better understanding of IoT and the risks related to it, to evaluate existing regulations, and to develop regulations that are data-driven, relevant, and adaptable to IoT as an evolving technology.

The scope of the privacy protection frameworks needs to be extended to go beyond the protection of personal data and to provide protection for non-personal identifying data that is collected, exchanged, shared, and stored in the IoT ecosystem. Some IoT applications deal with non-personal identifying data that is sensitive and critical to the users of those applications, and this data also needs to be protected by the provisions of POPIA. An IoT regulatory sandbox can be established with different regulators, IoT manufacturers, and developers involved to test this proposed regulatory change.

The issue of adopting and implementing the security and privacy by design approach for IoT can also be put as a subject in an IoT regulatory sandbox for regulators to work collaboratively with manufacturers and developers of IoT devices, products, and systems to test and develop a regulatory approach that will enable the adoption and implementation of security and privacy by design. This will help to ensure that IoT devices, products, and systems that are developed are safe and secure, and that users can trust the technology. This will in turn advance the adoption and use of IoT.

6.5.1.3 Regulators to take a socio-technical view of IoT

Although IoT is a digital technology, it is not only a technical phenomenon; it has both technical and social aspects. In as much as it constitutes technical components, its development is also sustained and affected by its application in other sectors outside the ICT sector such as health, energy, agriculture, and manufacturing, as found by this study. By recognising the equal importance of both the technical and social aspects of IoT and the relationship between them, the issues that affect the technology and people for whom the technology is designed and those who affect its development can be better explored. By taking this view, regulators are placed in a better position to develop regulations and create

a regulatory environment that is relevant to the technology and influences the development and subsequent adoption and use of IoT.

6.5.2 Recommendations for regulated entities

The subsections below outline recommendations for consideration by IoT manufacturers and developers.

6.5.2.1 Addressing the adoption and implementation of security and privacy protection measures

IoT manufacturers and developers need to adopt and implement a security and privacy by design approach by incorporating security and privacy protection measures at the design phase of their products and systems' development life cycle to ensure that these devices, products, and systems have security and privacy protection measures designed and embedded into them from the outset.

6.5.2.2 Participation in IoT regulatory sandboxes

In a regulatory sandbox IoT manufacturers, developers, and solutions providers will be able to learn and develop an understanding of regulations pertaining to their market and enhance the development, adoption, and use of IoT with new products and solutions that have fulfilled regulatory requirements.

6.5.3 Recommendations for future research

Semi-structured interviews provided an in-depth understanding of how regulatory approaches, security, and privacy affects the adoption and use of IoT. One recommendation for future research is research that uses other types of research methods to explore the subject. Future researchers could also explore other regulatory aspects of IoT, for example connectivity. The scope of this study was limited to the regulatory aspects of security and privacy. Lastly, the STS framework with its technical and social subsystems was employed as a theoretical lens to analyse the data collected for the study. Other theoretical frameworks can be applied to analyse data looking at aspects of IoT other than the technical and social aspects.

6.6 Conclusion

IoT is a growing phenomenon that is progressively being adopted and used in more industries in South Africa. Its growth, adoption, and varied use is further propelled by the fact that it is one of the key technologies that enables the 4IR. The adoption and use of IoT is, however, confronted by regulation, security, and privacy challenges; these issues need to be addressed to further enable the widespread adoption of IoT and to earn the trust of users.

Taking a socio-technical view of IoT, the study revealed that the adoption and use of IoT needs to be facilitated by a collaborative and adaptable regulatory approach. Also, the security and privacy challenges of IoT are hampering its adoption and use and need to be addressed by ensuring that IoT devices, products, and systems are designed with security and privacy protection measures. The study further revealed that the development of IoT regulation requires the involvement of regulators, IoT manufacturers, developers, and solutions providers working alongside each other in an environment that fosters collaboration, such as regulatory sandboxes. Thus, reaching even higher levels of adoption and use of IoT must be a joint effort between regulators, IoT manufacturers, developers, and solutions providers.

REFERENCES

Abbas, R., & Michael, K. (2023) Socio-Technical Theory: A review. https://open.ncl.ac.uk/theory-library/socio-technical-theory.pdf

Access Partnerships. (2021). *Regulating the IoT: 2020s and beyond*. https://cdn.accesspartnership.com/wp-content/uploads/2021/08/Regulating-IoT-2020s-and-beyond.pdf

African Union (AU). (2014). *African Union Convention on Cyber Security and Personal Data Protection*. https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection

Al Isma'ili, S., Li, M., Shen, J., He, Q., & Alghazi, A. (2017). African Societal Challenges Transformation through IoT. https://aisel.aisnet.org/pacis2017/162

Alshenqeeti, H. (2014). Interviewing as a Data Collection Method: A Critical Review. *English Linguistics Research, 3*(1). https://doi.org/10.5430/elr.v3n1p39

Babbie, E. (2010). *The practice of social research* (12th ed.). Wadsworth Publishers.

Ballon, I. C. (2020). California's IoT Law On The Security Of Connected Devices. *E-Commerce & Internet Law – Treaties with Forms* (2nd ed.), *3*. Thomas Reuters.

Bhattacherjee, A. (2012). *Social Science Research: Principles, Methods, And Practices* (2nd ed.). Creative Commons.

Bijker, W. E. (1995). *Of Bicycles Bakelites and Bulbs: Toward a Theory of Sociotechnical Change*. MIT Press.

Bostrom, R, P., & Heinen, S, J. (1977). MIS Problems and Failures: A Socio-Technical Perspective. Part I: The Causes. *MIS Quarterly, 1*(3), 17-32. https://doi.org/10.2307/248710

Brass, I. & Sowell, J. H. (2020). Adaptive governance for the Internet of Things: Coping with emerging security risks. *Regulation & Governance*. https://doi:10.1111/rego.12343

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology, 3*(2), 77-101. https://doi.org/10.1191/1478088706qp063oa

Brown, I. (2015). *Regulation and the Internet of Things*. GSR-2015 Discussion Paper, Geneva, Switzerland: International Telecommunication Union. https://www.itu.int/en/ITU-D/Conferences/GSR/Documents/GSR2015/Discussion_papers_and_Presentations/GSR_DiscussionPaper_IoT.pdf

Centre for the Fourth Industrial Revolution South Africa. (2023). *Accelerating The Adoption of Industrial IoT By Small, Medium and Macro Enterprises*. https://c4ir.co.za/all_projects/accelerating-the-adoption-of-industrial-iot-by-small-medium-and-macro-enterprises/

Chen, S., Xu, H., Liu, D., Hu, B., & Wang, H. (2014). A Vision of IoT: Applications, Challenges, and Opportunities With China Perspective. *IEEE Internet of Things Journal. 1(4), 349–359.* https://doi,org: 10.1109/JIOT.2014.2337336

Cichy, P., Salge, T. O., & Kohli, R. (2021). Privacy Concerns And Data Sharing In The Internet Of Things: Mixed Methods Evidence From Connected Cars. *MIS Quarterly, 45*(4), 1863-1892. https://doi.org/10.25300/MISQ/2021/14165

Cirne, A., Sousa, P. R., Resende, J. S., & Antunes, L. (2022). IoT security certifications: Challenges and Potential Approaches. *Computers & Security*, *116*. https://doi.org/10.1016/j.cose.2022.102669

Cisco. (2020). *Cisco annual internet report (2018-2023)* [White Paper]. https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html

Conti, M., Dehghantanha, A., Franke, K., & Watson, F. (2018). Internet of Things security and forensics: Challenges and opportunities. *Future Generation Computer Systems, 78*(2), 544-546. http://dx.doi.org/10.1016/j.future.2017.07.060

Crawford, L. M. (2020). *Conceptual And Theoretical Frameworks In Research*. Sage Publications. https://uk.sagepub.com/sites/default/files/upm-assets/105274_book_item_105274.pdf

Creswell, J. W. (2013). *Research Design: Qualitative, Quantitative And Methods Approaches* (3rd ed.). Sage Publications.

Creswell, J. W., & Creswell, J. D. (2018). *Research Design: Qualitative, Quantitative And Methods Approaches* (5th ed.). Sage Publications.

Cybercrimes Act No. 19 of 2020. (2021). Cybercrimes Act No. 19 of 2020. *Government Gazette,* 44651.

Department for Digital, Culture, Media & Sport. (2018). Code of Practice for Consumer IoT Security. https://assets.publishing.service.gov.uk/media/60576f54e90e0724c0df4631/Code_of_Practice_for_Consumer_IoT_Security_October_2018_V2.pdf

Dickson, A., Emad, H. & Joe, A. (2018). Theoretical And Conceptual Framework: Mandatory Ingredients Of A Quality Research. *International Journal of Scientific Research,* 7, 438–441.

https://www.researchgate.net/publication/322204158_THEORETICAL_AND_CONCEPTUAL_FRAMEWORK_MANDATORY_INGREDIENTS_OF_A_QUALITY_RESEARCH

Dissanayake, C. A. K., Jayathilake, W., Wickramasuriya, H. V. A., Dissanayake, U., Kopiyawattage, K. P. P., & Wasala, W. C. M. B. (2022). Theories and Models of Technology Adoption in Agricultural Sector. *Hindawi Human Behavior and Emerging Technologies, (2022)*. https://doi.org/10.1155/2022/9258317

Dolwick, J. S. (2009). 'The Social' and Beyond: Introducing Actor-Network Theory. *Journal of Maritime Archaeology, 4*(1). 21–49. https://doi.org/10.1007/s11457-009-9044-3

Eggers, W., & Turley, M. (2018). The future of regulation: Principles for regulating emerging technologies. Deloitte Center for Government Insights. https://www2.deloitte.com/us/en/insights/industry/public-sector/future-of-regulation/regulating-emerging-technology.html#

Ernest, P. (1994). *An Introduction To Research Methodology And Paradigms*. University of Exeter.

European Telecommunications Standards Institute (ETSI). (2020). *ETSI TS 103 645 V2.1.2 CYBER; Cyber Security for Consumer Internet of Things: Baseline Requirements*. https://www.etsi.org/deliver/etsi_ts/103600_103699/103645/02.01.02_60/ts_103645v020102p.pdf

Fagan, M., Megas, K. N., Scarfone, K., Smith, M. (2020) . *Foundational Cybersecurity Activities for IoT Device Manufacturers*. NIST. https://doi.org/10.6028/NIST.IR.8259

Gall, M. D., Borg, W. R., & Gall, J. P. (1996). *Education research: An introduction* (6th ed). Longman Publishing.

Ghaffari, K., Lagzian, M., Kazemi, M., & Malekzadeh, G. (2019). A Socio-Technical Analysis of Internet of Things Development: An Interplay of Technologies, Tasks, Structures and Actors, *Foresight*, *21*(6). 640 – 653. https://doi.org/10.1108/FS-05-2019-0037

Goldstuck, A. (2019, June 26). How your smartphone can make you a safer driver. *Citizen*. https://citizen.co.za/lifestyle/technology/2147350/how-your-smartphone-can-make-you-a-safer-driver/

Grant, C., & Osanloo, A. (2015). Understanding, Selecting, And Integrating A Theoretical Framework In Dissertation Research: Creating The Blueprint For Your "House". *Administrative Issues Journal: Connecting Education, Practice and Research, 4*(2). https//doi.org/10.5929/2014.4.2.9

Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Generation Computer Systems, 29*(7), 1645-1660. http://dx.doi.org/10.1016/j.future.2013.01.010

Guest, G., Bunce, A., & Johnson, L. (2006). How Many Interviews Are Enough?: An Experiment with Data Saturation and Variability. *Field Methods*, *18*(1), 59-82. https://doi.org/10.1177/1525822X05279903

Hadzovic, S., Mrdovic, S., & Randonjic, M. (2021). Identification of IoT Actors. *Sensors 2021, 21*(6). https://doi.org/10.3390/s21062093

Hadzovic, S. (2021). Internet of Things from a regulatory point of view. *2021 20th International Symposium INFOTEH-JAHORINA (INFOTEH)*, East Sarajevo, Bosnia and Herzegovina, 1–4. https://doi.org: 10.1109/INFOTEH51037.2021.9400654

Hagemann, R., Skees, J., & Thierer, A. (2018). Soft law for hard problems: The governance of emerging technologies in an uncertain future. *Colorado Technology Law Journal*, *17*(1), 37-130. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3118539

Hald, K., & Spring, M. (2023). Actor-Network Theory – A Novel Approach to Supply Chain Management Theory Development. *Journal of Supply Chain Management*. https://doi.org/10.1111/jscm.12296

Hassan, Q. F., Khan, A. R., & Madani, S. A. (2017). *Internet of things: Challenges, advances, and applications*. CRC Press. https://books.google.co.za/books?hl=en&lr=&id=iGpQDwAAQBAJ&oi=fnd&pg=PP1&dq=history+of+iot&ots=bnj7pDUBr4&sig=jowZdlYDEHIsa41YExGoO16YYsc&redir_esc=y#v=onepage&q=history%20of%20iot&f=false

Hussain, M. A., Elyas, T., & Nasseef, O. A. (2013). Research paradigms: A slippery slope for fresh researchers. *Life Science Journal*, *10*(4), 2374-2381. http://www.lifesciencesite.com/lsj/life1004/317_B02518life1004_2374_2381.pdf

International Association of Privacy Professionals (IAAP). (2020). *Brazilian General Data Protection Law.* https://iapp.org/media/pdf/resource_center/Brazilian_General_Data_Protection_Law.pdf

International Communications Authority of South Africa (ICASA). (2002). Electronic Communications and Transactions Act, 2002. *Government Gazette*, 23708

ICASA. (2006). Electronic Communications Act, 2005. *Government Gazette*, 28743

ICASA. (2013). Type Approval Regulations, 2013*. Government Gazette*, 36785

ICASA. (2021). *The State of 5G In South Africa*. https://www.icasa.org.za/uploads/files/ICASA-2021-5G-Annual-Report.pdf

ICASA. (2022). Equipment Authorisation Regulations, 2022. *Government Gazette*, 46146

ICASA. (2023). Radio Frequency Spectrum Assignment Plan For The Frequency Band 440 MHz To 40MHz. *Government Gazette*, 49079

IDC. (2019). How You Contribute to Today's Growing DataSphere and Its Enterprise Impact. https://blogs.idc.com/2019/11/04/how-you-contribute-to-todays-growing-datasphere-and-its-enterprise-impact/

Information Regulator South Africa. (2013). Protection of Personal Information Act, 2013. *Government Gazette,* 37067.

IoT Analytics. (2023). *State of IoT 2023: Number of Connected IoT Devices Growing 16% to 16.0 billion Globally – Wi-Fi, Bluetooth, and Cellular Driving The Market*. https://iot-analytics.com/wp/wp-content/uploads/2023/05/Insights-Release-State-of-IoT-2023-Number-of-connected-IoT-devices-growing-16-to-16.0-billion-globally.pdf

International Organization for Standardization (ISO). (2022). *ISO/IEC 27400:2022. Cybersecurity - IoT security and privacy – Guidelines*. https://www.iso.org/standard/44373.html

International Standards Organisation/International Electrotechnical Commission (ISO/IEC). (2014). *Internet of Things (IoT)*. https://www.iso.org/files/live/sites/isoorg/files/developing_standards/docs/en/internet_of_things_report-jtc1.pdf

ITWeb. (2017, March 2). *City power intensifies smart meter roll-out in Joburg*. https://www.itweb.co.za/content/lP3gQ2MGXkYqnRD1

ITWeb. (2023, November 17). *Mitigating IoT Hurdles Can Unlock Billions for SA*. https://www.itweb.co.za/article/mitigating-iot-hurdles-can-unlock-billions-for-sa/xA9PO7NELgxvo4J8

International Telecommunication Union (ITU). (2009). *ICT Regulatory Harmonization: A Comparative Study of Regional Initiatives*. https://www.itu.int/ITU-D/projects/ITU_EC_ACP/hipssa/docs/D_REG_HIPSSA_2010_PDF_E.pdf

ITU-T. (2012). *Series Y: Global information infrastructure internet protocol aspects and next generation networks*. https://www.itu.int/rec/T-REC-Y.2060/en

ITU. (2018). *Global ICT regulatory outlook 2018*. https://www.itu.int/en/ITU-D/Regulatory-Market/Documents/Publications/Document-Summary_English.pdf

ITU. (2021). *Y.4810: Requirements for data security of heterogeneous Internet of things devices***.** https://www.itu.int/rec/T-REC-Y.4810-202111-I/en

ITU. (2022). X.1369: *Security requirements for IoT service platform.* https://www.itu.int/rec/T-REC-X.1369-202201-I

Jakobs, K. (2018). *On Standardizing the Internet of Things and its Applications*. John Wiley & Sons. https://doi.org/10.1002/9781119456735.ch7

Jaspers, E.D.T., & Pearson, E. (2022). Consumers' acceptance of domestic Internet-of-Things: The role of trust and privacy concerns. *Journal of Business Research, 142*, 255–265. https://doi.org/10.1016/j.jbusres.2021.12.043

Justus, J. R. (2019). A Guide to Writing the Dissertation Literature Review. *Practical Assessment, Research, and Evaluation*, *14*(13). https://doi.org/10.7275/b0az-8t74

Kalsoom, T., Ramzan, N., Ahmed, S., & Ur-Rehman, M. (2020). Advances in Sensor Technologies in the Era of Smart Factory and Industry 4.0. *Sensors 2020*, *20*(23). https://doi.org/10.3390/s20236783

Kapoor, K., Bigdeli, A. Z., Dwivedi, Y. K., Schroeder, A., Beltagui, A., & Baines, T. (2021). A Socio-Technical View of Platform Ecosystems: Systematic Review and Research Agenda. *Journal of Business Research*, *128*, 94–108. https://doi.org/10.1016/j.jbusres.2021.01.060

Karale, A. (2021). The Challenges of IoT Addressing Security, Ethics, Privacy, and Laws. *Internet of Things, 15*. https://doi.org/10.1016/j.iot.2021.100420

Karie, N., Sahri, N., Yang, W., Valli, C., & Kebande, V. R. (2021). A Review of Security Standards and Frameworks for IoT-Based Smart Environments. *IEEE Access*, *9*, 121975–121995. https://doi.org/10.1109/ACCESS.2021.3109886

Kim, J. H. (2021). 6G and Internet of Things: A Survey. *Journal of Management Analytics*. 8(2), 316 – 332. https://doi.org/10.1080/23270012.2021.1882350

Kivunja, C., & Kuyini, A. B. (2017). Understanding and Applying Research Paradigms in Educational Contexts. *International Journal of Higher Education*, *6*(5), 26-41. https://doi.org/10.5430/ijhe.v6n5p26

Kivunja, C. (2018). Distinguishing between Theory, Theoretical Framework, and Conceptual Framework: A Systematic Review of Lessons from the Field. *International Journal of Higher Education*, *7*(6). https://doi.org/10.5430/ijhe.v7n6p44

Kothari, C. R. (2004). *Research Methodology: Methods and Techniques* (2nd ed.). New Age International Publishers.

Krotov, V. (2017). The Internet of Things and new business opportunities. *Business Horizons, 60*(6), 831-841. https://dx.doi.org/10.1016/j.bushor.2017.07.009

Kshetri, N. (2017). The economics of the Internet of Things in the Global South. *Third World Quarterly*, *38*(2), 311-339. http://dx.doi.org/10.1080/01436597.2016.1191942

Law, J. (1992). Notes on the theory of the actor-network: Ordering, strategy, and heterogeneity. *Systems Practice* 5, 379–393. https://doi.org/10.1007/BF01059830

Lee, G. (2018). What roles should the government play in fostering the advancement of Internet of Things? *Telecommunications Policy*, *43*(5), 434-444. https://doi.org/10.1016/j.telpol.2018.12.002

Lu, Y. (2021). Examining user acceptance and adoption of the internet of things. *International Journal of Business Science & Applied Management (IJBSAM)*, *16*(3), 1-17. https://hdl.handle.net/10419/261656

Lynn, T., Mooney, J. G., Lee, B., & Endo, P. T. (2020). The Cloud-to-Thing Continuum: Opportunities and Challenges in Cloud, Fog and Edge Computing. *Palgrave Studies in Digital Business & Enabling Technologies*. https://doi.org/10.1007/978-3-030-41110-7

Mack, L. (2010). The philosophical underpinnings of educational research. https://en.apu.ac.jp/rcaps/uploads/fckeditor/publications/polyglossia/Polyglossia_V19_Lindsay.pdf

Maguire, M. (2014). Socio-Technical Systems and Interaction Design - 21st Century Relevance. *Applied Ergonomics*, *45*(2), 162-170. https://doi.org/10.1016/j.apergo.2013.05.011

Mahdad, M., Hasanov, M., Isakhanyan, G., & Dolfsma, W. (2022). A smart web of firms, farms and internet of things (IOT): Enabling collaboration-based business models in the agri-food industry. *British Food Journal, 124*(6), 1857-1874. https://doi.org/10.1108/BFJ-07-2021-0756

Maisiri, W., Van Dyk, L., & Coetzee, R. (2021). Factors that Inhibit Sustainable Adoption of Industry 4.0 in the South African Manufacturing Industry. *Sustainability*. *13*(1013). https://doi.org/10.3390/su13031013

Mcbride, N. (2003). Actor-network theory and the adoption of mobile communications. *Geography, 88*(4), 266-276. https://www.jstor.org/stable/40573881

Mena, D. M., Papapanagiotou, I., & Yang, B. (2018). Internet of things: Survey on security. *Information Security Journal: A Global Perspective*, *27*(3), 162-182. https://doi.org/10.1080/19393555.2018.1458258

Merriam, S. B. (2010). *Qualitative Case Studies A Guide To Design And Implementation*. Jossey-Bass Publishers

Mordor Intelligence. (2023). *South Africa IoT Market Size & Share Analysis – Growth Trends & Forecasts (2024 - 2029)*. https://www.mordorintelligence.com/industry-reports/south-africa-iot-market

Molling, G., & Klein, A. Z. (2022). Value Proposition of IoT-Based Products and Services: A Framework Proposal. *Electronic Markets, 32*, 899–926. https://doi.org/10.1007/s12525-022-00548-w

Mumford, E. (2006), The story of socio-technical design: reflections on its successes, failures and potential. *Information Systems Journal, 16*(4), 317-342. https://doi.org/10.1111/j.1365-2575.2006.00221.x

National Institute of Standards and Technology (NIST). (2020). *NIST Privacy Framework: A Tool For Improving Privacy Through Enterprise Risk Management, Version 1.0*. https://www.nist.gov/system/files/documents/2020/01/16/NIST%20Privacy%20Framework_V1.0.pdf

NIST. (2022). *Recommended Criteria for Cybersecurity Labeling for Consumer Internet of Things (IoT) Products*. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.02042022-2.pdf

Nowell, L. S., Norris, J. M., White, D. E., & Moules, N. J. (2017). Thematic Analysis: Striving to Meet the Trustworthiness Criteria. *International Journal of Qualitative, 16*, 1-13. https://doi.org/10.1177/1609406917733847

Organisation for Economic Co-operation and Development (OECD). (2022). *Building Cyber Resilience In A Post COVID-19 World: Local Challenges, Global Solutions*. https://one.oecd.org/document/DSTI/CDEP/SDE(2022)5/FINAL/en/pdf

OECD. (2020). *Shaping The Future of Regulators: The Impact of Emerging Technologies on Economic Regulators*. OECD Publishing. https://doi.org/10.1787/db481aa3-en

Official Journal of the European Union. (2016). *Regulation (EU) 2016/679 of The European Parliament and ff The Council of 27 April 2016*. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

Otter.ai. (2023). AI Meeting Note Taker & Real-time AI Transcription. https://otter.ai

Paukstadt, U., & Beker, J. (2019). Uncovering the business value of the internet of things in the energy domain – a review of smart energy business models. *Electronics Market 2021, 31*, 51-66. https://doi.org/10.1007/s12525-019-00381-8

Prescott, M. B. (1995). Diffusion of Innovation Theory: Borrowings, Extensions, and Modifications from IT Researchers. *ACM SIGMIS Database: the DATABASE for Advances in Information Systems, 26*(2-3), 16-19. https://doi.org/10.1145/217278.217283

Pygma Consulting. (2022). *A Proposed Regulatory Sandbox Framework For Africa*. https://pygmaconsulting.com/a-proposed-regulatory-sandbox-framework-for-africa/

Ranchordas, S. (2015). Innovation-friendly regulation: the sunset of regulation, the sunrise of innovation. *Jurimetrics*. *55*(2), 201-224. www.jstor.org/stable/24395571

Ranchordás, S. (2021). Experimental Lawmaking in the EU: Regulatory Sandboxes. http://dx.doi.org/10.2139/ssrn.3963810

Rehman, A. A., & Khalid, A. (2016). An introduction to research paradigms. *International Journal of Educational Investigations, 3*(8), 51–59. http://www.ijeionline.com/attachments/article/57/IJEI.Vol.3.No.8.05.pdf

Rogers, E. M. (1982). *Diffusion Of Innovations* (3rd ed.). The Free Press

Rotolo, D., Hicks, D., & Martin, B. R. (2015). What Is an Emerging Technology?. *Research Policy, 44*(10), 1827-1843. https://doi.org/10.1016/j.respol.2015.06.006

Saarikko, T., Westergren, U., & Jonsson, K. (2020). Here, there, but not everywhere: Adoption and Diffusion of IoT in Swedish Municipalities. https://doi.org/10.24251/HICSS.2020.248

Sahin, I. (2006). Detailed Review Of Rogers' Diffusion Of Innovations Theory And Educational Technology-Related Studies Based On Rogers' Theory. *The Turkish Online Journal of Educational Technology*, *5*(2). https://files.eric.ed.gov/fulltext/ED501453.pdf

Saint, M., & Garba, A. (2016). *Technology and policy for the Internet of Things in Africa*. TPRC 44: The 44th Research Conference on Communication, Information and Internet Policy 2016. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2757220

Saldaña, J. (2013). *The Coding Manual for Qualitative Researchers* (2nd ed.). Sage Publications

Saunders, M., Lewis, P., & Thornhill, A. (2009). *Research Methods For Business Students* (5th ed.). Pearson Education

Schiller, E., Aidoo, A., Fuhrer, J., Stahl, J., Ziörjen, M,. & Stiller, B. (2022). Landscape of IoT security. *Computer Science Review, 44*. https://doi.org/10.1016/j.cosrev.2022.100467

Scotland, J. (2012). Exploring the philosophical underpinnings of research: Relating ontology and epistemology to the methodology and methods of the scientific, interpretive, and critical

research paradigms. *English Language Teaching, 5*(9). https://files.eric.ed.gov/fulltext/EJ1080001.pdf

Sha, K., Wei W., Yang, T. A., Wang, Z., & Shi, W. (2018). On security challenges and open issues in Internet of Things. *Future Generation Computer Systems*, *83*, 326-337. https://doi.org/10.1016/j.future.2018.01.059

Sharma, R., & Mishra, R. (2014). A Review of Evolution of Theories and Models of Technology Adoption. *6*(2). https://www.researchgate.net/publication/295461133_A_Review_of_Evolution_of_Theories_and_Models_of_Technology_Adoption

Shin, D., & Jung, J. (2012). Socio-technical analysis of Korea's broadband convergence network: Big plans, big projects, big prospects?. *Telecommunications Policy, 36(*7), 579-593. https://doi.org/10.1016/j.telpol.2012.03.003

Shin, D. (2014). A Socio-Technical Framework for Internet-of-Things Design: A Human-Centered Design for The Internet of Things. *Telematics and Informatics*, *31*(4), 519-531. https://doi.org/10.1016/j.tele.2014.02.003

Shin, D., & Park, Y. J. (2016). Understanding the Internet of Things Ecosystem: Multi-Level Analysis of users, society, and ecology. *Digital Policy, Regulation And Governance, 19*(1), 77 - 100. https://doi.org/10.1108/DPRG-07-2016-0035

Sileyew, K. J. (2019). Research design and methodology. https://doi.org/10.5772/intechopen.85731

Song, T., Cai, J., Chahine, T., & Li, L. (2021). Towards Smart Cities by Internet of Things (IoT)—a Silent Revolution in China. *Journal of The Knowledge Economy, 12*(2), 1–17. https://doi.org/10.1007/s13132-017-0493-x

Song, T., Cai, J., Chahine, T., & Li, L. (2017). Towards Smart Cities by Internet of Things (IoT)—a Silent Revolution in China. *Journal of the Knowledge Economy.* 12. https://doi:10.1007/s13132-017-0493-x

Sowell, J. H., & Brass, I. (2020). Adaptive governance for the Internet of Things: Coping with emerging security risks. *Regulation & Governance*. https://doi.org:10.1111/rego.12343

Statista. (2023a). Global consumer IoT market size from 2020 to 2022, with a forecast up to 2030. https://www.statista.com/statistics/1409175/global-consumer-iot-market-value/

Statista. (2023b). Number of Internet of Things (IoT) connected devices worldwide from 2019 to 2030, by vertical. https://www.statista.com/statistics/1194682/iot-connected-devices-vertically/

Stevens, T. (2023). *What Is Cybersecurity For?* (1st ed.). Bristol University Press

Tanczer, L. M., Brass, I., Elsden, M., Carr, M., & Blackstock, J. (2019). The United Kingdom's emerging Internet of Things (IoT) policy landscape. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3385548

Tech In Africa. (2023). *Smart Geyser Devices: A High-Tech Solution for South Africa's Energy Crisis.* https://www.techinafrica.com/smart-geyser-devices-a-high-tech-solution-for-south-africas-energy-crisis/

Tomislav, C., Stifanich, P. L., & Šimunić, M. (2019). Internet Of Things (IoT) In Tourism And Hospitality: Opportunities And Challenges. *Tourism in Southern and Eastern Europe, 5*, 163-175. https://doi.org/10.20867/tosee.05.42

United States Department of Health & Human Services. (2005). *Summary of the HIPAA Privacy Rule. Office For Civil Rights.* https://www.hhs.gov/sites/default/files/privacysummary.pdf

Vermesan, O., & Bacquet, J. (2020). *Internet of Things – The Call of the Edge Everything Intelligent Everywhere*. River Publishers Series in Communication. https://library.oapen.org/handle/20.500.12657/59760

Vizocom. (2019). *6 IoT Applications that Improved People's Lives in Africa – A Story of 6 Countries*. https://www.vizocom.com/ict/6-iot-applications-that-improved-peoples-lives-in-africa-a-story-of-6-countries/

Weber, R. H. (2010). Internet of Things – New security and privacy challenges. *Computer Law & Security Review*, *26*(1), 23-30. https://doi.org/10.1016/j.clsr.2009.11.008

Weber, M., & Zarko, I. P. (2019). Regulatory View on Smart City Services. *Sensors, 19*(2). https://doi.org/10.3390/s19020415

WEF. (2018). *Agile Governance Reimagining Policy-making in the Fourth Industrial Revolution*. https://www3.weforum.org/docs/WEF_Agile_Governance_Reimagining_Policy-making_4IR_report.pdf

WEF. (2019). *Agile Governance for The Creative Economy 4.0*. https://www3.weforum.org/docs/WEF_Agile%20Governance_for_Creative_Economy_4.0_Report.pdf

WEF. (2023). *State of the Connected World 2023 Edition*. https://www.weforum.org/publications/state-of-the-connected-world-2023-edition/

Westin, A. F. (1967). Privacy and Freedom. https://scholarlycommons.law.wlu.edu/wlulr/vol25/iss1/20/

Yohannan, T. P. (2010). Towards developing a web-based blended learning environment at the University of Botswana. http://uir.unisa.ac.za/handle/10500/4245

Yuan, B. (2023). Understanding digital information production in virtual communities from the perspective of Actor-Network Theory. *Journal of Hospitality and Tourism Management*. *56*, 495 – 502. https://doi.org/10.1016/j.jhtm.2023.08.003

Zahra, S. R., & Chishti, M. A. (2019). Assessing the services, security threats, challenges and solutions of the Internet of Things. *Scalable Computing: Practice and Experience*, *20*(3), 457-484. https://doi.org/10.12694/scpe.v20i3.1544

ANNEXURE A – ETHICAL CLEARANCE CERTIFICATE

SCHOOL OF Literature, Language and Media RESEARCH ETHICS COMMITTEE

CLEARANCE CERTIFICATE **PROTOCOL NUMBER: SLLM-M21-02**

PROJECT TITLE Adoption and use of Internet of Things in South Africa and the implications for adaptive regulation

INVESTIGATOR Boipelo Jarvis 2275485

SCHOOL/DEPARTMENT SLLM/ LINK

DATE CONSIDERED March 2021

DECISION OF THE COMMITTEE Approved

This ethical clearance is valid for 2 years and may be renewed upon application.

EXPIRY DATE Date of submission of the project report

ISSUE DATE OF CERTIFICATE March 2021 **CHAIRPERSON**

Colleen Dawson

cc: Supervisor : Dr Lucienne Abrahams

DECLARATION OF INVESTIGATOR

To be completed in duplicate and **ONE COPY** returned to the Chairperson of the School/Department ethics committee.

I fully understand the conditions under which I am are authorized to carry out the abovementioned research and I guarantee to ensure compliance with these conditions. Should any departure to be contemplated from the research procedure as approved I/we undertake to resubmit the protocol to the Committee.

Signature **Date** 23/03/2021

ANNEXURE B – INFORMED CONSENT FORM

Informed Consent Form

Title of project: Adoption and use of Internet of Things in South Africa and the implications for adaptive regulation

Name of researcher: Boipelo Jarvis

I, ……., agree to participate in this research project. The research has been explained to me and I understand what my participation will involve. I agree to the following:

(Please circle the relevant options below).

I agree that my participation will remain anonymous	YES	NO
I agree that the researcher may use anonymous quotes in his / her research report	YES	NO
I agree that the interview may be audio recorded	YES	NO
I agree that the information I provide may be used in an anonymized format after this project has ended, for academic purposes by other researchers, subject to their own ethics clearance being obtained.	YES	NO

…… (signature)
…… (name of participant)
…… (date)

ANNEXURE C – PARTICIPANT INFORMATION SHEET

Participant Information Sheet

UNIVERSITY OF THE
WITWATERSRAND,
JOHANNESBURG

1 Jan Smuts Avenue,
Braamfontein 2000,
Johannesburg,
South Africa

Dear Sir/Madam,

My name is Boipelo Jarvis and I am a Masters student in ICT Policy and Regulation at the University of the Witwatersrand, Johannesburg. As part of my studies, I have to undertake a research project, and I am investigating the adoption and use of Internet of Things in South Africa and the implication for adaptive regulation under the supervision of Dr Ntsibane Ntlatlapa. The aim of this research project is to find out the effects that regulatory approaches have on the adoption and use of IoT in South Africa. The study will also look into ways in which challenges of security and privacy can affect the adoption and use of IoT, as well as explore ways in which adaptive regulation is being adopted and implemented globally with respect to IoT.

As part of this project, I would like to invite you to take part in an interview. This activity will involve answering questions and will take around 60 minutes. With your permission, I would also like to record the interview using a digital device.

There will be no personal costs to you if you participate in this project, you will not receive any direct benefits from participation but there are no disadvantages or penalties if you do not choose to participate or if you withdraw from the study. You may withdraw at any time or not answer any question if you do not want to. Any confidential information will not be disclosed to anyone else. The interview will be anonymous as I will not be asking you for your name or any identifying information. I will be using a pseudonym (false name) to represent your participation in my final research report. If you experience any distress or discomfort at any point in this process, we will stop the interview or resume another time. Your participation in this project is voluntary and by signing this, you accept that you have read the participant information sheet, asked questions and that your questions were answered by the researcher.

If you have any questions during or afterwards about this research, feel free to contact me on the details listed below. This study will be written up as a research report. If you wish to receive a summary of this report, I will be happy to send it to you. The data collected from this research project will be stored in a password protected computer. With your permission the data collected from this research project may

be used by other researchers. If you have any concerns or complaints regarding the ethical procedures of this study, you are welcome to contact the University Human Research Ethics Committee (Non-Medical), telephone +27(0) 11 717 1408, email hrecnon-medical@wits.ac.za

Yours sincerely,
Boipelo Jarvis

Researcher:
Boipelo Jarvis, 2275485@students.wits.ac.za, 0825962473

Supervisor:
Dr Ntsibane Ntlatlapa, NNtlatlapa@csir.co.za

ANNEXURE D – INTERVIEW QUESTIONS

Research project: Adoption and use of Internet of Things in South Africa and the implications for adaptive regulation

Name of researcher: Boipelo Jarvis

INTERVIEW QUESTIONS

1. How is the rate of IoT adoption in South Africa advancing?
2. In which sectors would you say IoT is mostly used?
3. Where is the rate of adoption and use of IoT more prevalent, is it with new IoT innovation or with existing products, processes and services that have been enhanced with internet connectivity and equipped with new features and efficiencies (i.e. retrofitting)?
4. What are the current challenges being experienced with regards to adoption of IoT in South Africa?
5. Which factors can affect ongoing and future adoption and use of IoT?
6. In which ways are regulatory approaches and frameworks with respect to IoT applications and services affecting its adoption and use?
7. Which mechanisms can be put in place to ensure that regulatory frameworks with respect to IoT are adaptive?
8. What are your thoughts on regulatory sandboxes?
9. In which ways can common security baseline measures aimed at addressing security issues in IoT be adopted and put in place by regulators and industry?
10. Do you find that privacy related frameworks (e.g. POPIA) have adequate data protection provisions? Why do you hold this view?
11. If the privacy related frameworks (e.g. POPIA) provisions are not adequate, then how can they be adapted to address data protection issues for data collected, processed, analysed and stored by IoT?