Internet of Things in Organisations: Artefactual Characteristics that Influence Adoption

Masters Research presented to the

Department of Information Systems

University of Cape Town

by

Henry Bukasa Tshilenge

in partial fulfilment of the requirements for the *Masters Information Systems course (INF5005W)*

Supervised by
Dr Irwin Brown

30 January 2025

PLAGIARISM DECLARATION

1. This dissertation has been submitted to Turnitin (or equivalent similarity and originality checking software), and I confirm that my supervisor has seen my report and any concerns revealed by such have been resolved with my supervisor.
2. I certify that I have received Ethics approval from the Commerce Ethics Committee.
3. This work has not been previously submitted in whole or in part for the award of any degree in this or any other university. It is my own work. Each significant contribution to, and quotation in, this dissertation from the work or works of other people has been attributed and has been cited and referenced.

Student Number: TSHHEN003

Full Name : Henry Bukasa Tshilenge

Signature: Signed by candidate

Date: 30 January 2025

ACKNOWLEDGEMENTS

I am grateful to my Supervisor, Dr Brown Irwin, who has been patient with me and provided excellent support and guidance. My sincere appreciation also goes to my wife, Phumla Tshilenge, and son, Georges Tshilenge, who have supported and encouraged me throughout.

Thank you to my Lord and Saviour, Jesus Christ, who granted me life and this opportunity. Special thanks to the Prolific Academic Online Panel participants who took the time to respond to the survey and made the data collection possible.

ABSTRACT

Background: The Internet of Things (IoT) has gained significant attention from businesses and academia. IoT promises are ambitious: creating, collecting, and sharing information independently of time, place, and motion. Things are rendered autonomous, able to identify themselves, network with other objects, and analyse the data they produce. IoT systems are used in some organisations to improve efficiency and facilitate trade in commodities and services. These systems help prevent errors, monitor operations, track assets, deter theft, and integrate complex systems through real-time data collection and analysis.

Problem Statement: IoT promises many benefits, which are already tangible in the agriculture, logistics, retail, and supply chain sectors. However, some organisations still adopt IoT hesitantly, while others still hold a conservative stance. Little is known about its adoption in organisations based on its artefactual characteristics.

Purpose: This study explores the artefactual characteristics of the Internet of Things that lead to its adoption and implementation in organisations. The focus is on the impact of identified IoT characteristics on its adoption as reflected by the continuance intention.

Methodology: The study adopted a quantitative survey strategy and collected data via the Academic Prolific Online Panel[1], with a sample of 293 participants from South Africa, the United Kingdom, and the United States.

Findings: The results indicate that IoT characteristics closely aligned with business needs, such as relative advantage (profitability), Compatibility (alignment with values), seamless integration, and self-adaptation (intelligent, efficient operation and future growth), significantly influence IoT adoption as reflected by the continuance intention in organisations. The study went beyond the traditional Technology-Organisational-Environment (TOE) framework technology characteristics adapted from the Diffusion of Innovation framework, such as relative advantage, complexity, and compatibility. In addition, the findings revealed that integration and self-adaptation (i.e., intelligence) significantly influence technology adoption, as reflected by

[1] (https: //www.prolific.com/)

continuance intention. The research contributes to the knowledge of IoT. The study recommends that future research look further into the technocentric characteristics such as connectivity, security and interoperability, which were unexpectedly found not to influence adoption as reflected by the continuance intention.

Key Words: Internet of Things, IoT, organisation, adoption, continuance intention, technology adoption, conceptualisation, compatibility, complexity, connectivity, scalability, relative advantage, integration, interactivity, state, security, self-adaptation, synchronicity, and interoperability.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER 1: INTRODUCTION

1.1 Background

The Internet of Things (IoT) has gained significant attention from businesses and academia (Sorri et al., 2022). However, IoT promises are ambitious, and include creating, collecting and sharing information independently of time, place and motion (Ahmetoglu et al., 2023; Dabbagh & Rayes, 2019). Using IoT, things are rendered autonomous, are able to identify themselves, can network with other objects, and can analyse the data they produce (Brous & Janssen, 2019; Sullivan et al., 2023). As a rising technology, IoT has been deployed in many organisations as a way to improve organisational performance and efficiency, and hence is expected to make it very easy to trade commodities and services (Kamble, et al., 2019). IoT can be used to prevent mistakes, stop theft and integrate complex systems by collecting real-time data using predictive analytics and big data technologies (Polgavande & Kulkarni, 2017; Rey et al., 2021; Tu, 2018). Additionally, it may be used in Smart City development to accommodate the elderly and people with disabilities. Hence it becomes ubiquitous in social life, the economic arena and technical industries (Zhou et al., 2024).

The decline in the price of computer chips, the mass availability of sensors, and the improvement in both the range and cost of network connectivity, have enabled IoT to innovate and disrupt (Osman, 2019; Rey et al., 2021). By the end of 2019 there were an estimated 7.6 billion active IoT objects worldwide and this was projected to grow to around 24.1 billion by 2030 (Vermesan & Bacquet, 2020). In 2023, Sullivan et al. (2023) reported that approximately 27 billion heterogeneous IoT things were interconnected. IoT's annual global economic impact was estimated in 2020 to be approximately \$8 trillion, with \$6.4 trillion attributed to the private sector and \$1.6 trillion in the public sector (Shah et al., 2020).

The European Union has seen significant investments in associated applications of IoT such as,

"… smart homes, personal wellness and wearables, smart energy, smart cities, and smart mobility, healthcare, energy consumption and utility monitoring, transportation and traffic control, logistics, production and supply chain management, agriculture, public space and environmental monitoring, social interactions, personalised shopping and commerce, domestic automation, and others." (Wachter, 2018, p. 436).

Organisations view innovation as a critical asset that can contribute to business success (Sullivan et al., 2023). Understandably, investments in IoT are motivated by the needs of individuals and organisations that stand to benefit from it, as well as the decision makers' expectations regarding the new insights and predictability that can be gained by making optimal use of objects and services associated with IoT (Polgavande & Kulkarni, 2017). IoT has many exceptional benefits, and progress linked to IoT has been made in recent years in the field of emerging technologies; nevertheless, the adoption of this disruptive technology has been slow and has lagged in many organisations (Brous & Janssen, 2019; Čolaković & Hadžialić, 2018; Rey et al., 2021). Furthermore, the real contribution achieved from IoT, the added value to organisations, remains unclear (Sullivan et al., 2023). Ahmetoglu et al. (2023) support this view and suggest that decision-makers find it difficult to assess the possible IoT-related value that the business can gain. To expand its sphere of adoption and its influence, and to achieve successful implementation, IoT needs to meet the expectations of organisations and stakeholders and hence make them recognise its potential value (Mineraud et al., 2016). The relatively slow uptake of IoT can also be attributed to implementation challenges (Sorri et al., 2022). Both Ahmetoglu et al. (2023) and Sullivan et al. (2023) say that most IoT projects remain in the early adoption stages and fail to deploy fully. Furthermore, challenges can emerge from the characteristics of the artefact itself; for example, the heterogeneous nature of the IoT artefact or 'thing' poses security challenges and requires integration of a new system into a legacy system, leading to complexity and a need for interoperability (Ahmetoglu et al., 2023).

Numerous calls have been made for Information Systems (IS) researchers to take the conceptualisation of the IT artefact seriously as IS studies still do not give sufficient attention to evaluating information technology artefacts based on their artefactual characteristics (Matook & Brown, 2017; Orlikowski & Iacono, 2001; Zhou et al., 2024). As Ahmetoglu et al. (2023) noted, IoT artefacts have distinct characteristics that distinguish them from general IT artefacts. Therefore, it is essential to understand the particular IoT artefactual characteristics and determine which of these can encourage the adoption as reflected by the continuance intention of IoT in organisations.

1.2 Problem Statement

The background given above has painted a picture of a promising technology, IoT, with many benefits and much to offer, some of which are easily seen in fields like logistics and retail supply chain management (Ahmetoglu et al., 2023; Kamble et al., 2019). This is, therefore, a technology that is considered to be essential to the adoption of Industry 4.0 and is viewed as a future technology that will improve the lives of many people and the world's economy (Luthra, et al., 2018; Sullivan et al., 2023). However, as noted above, IoT continues to face implementation challenges, with organisations still having a timid and hesitant adoption stance (Tu, 2018; Rey et al., 2021). It is clear that all new technologies, including IoT, present opportunities and challenges (Evans, 2015). Hence, IoT has many impediments to overcome (Brous & Janssen, 2019; Sorri et al., 2022). Since little is known about its adoption in organisations based on its artefactual characteristics, the information technology artefact (ITA) has been proposed as needing to be the core focus of IS research (Matook & Brown, 2017; Zhou et al., 2024).

1.3 Research Question

This explanatory study aims to determine the artefactual characteristics that lead to the adoption as reflected by the continuance intention of IoT in organisations. In order to achieve this, the following main question is asked, together with two sub-questions.

What IoT artefact characteristics influence organisational adoption as reflected by the continuance intention of IoT?

1) What are the key IoT artefactual characteristics?
2) Which IoT technology artefact characteristics have the greatest influence on organisational adoption?

1.4 Research Objectives

The main objective of this research is to determine the IoT artefactual characteristics that influence its adoption as reflected by the continuance intention of organisations through these two sub-objectives:

1) Identify key IoT artefactual characteristics.

2) Determine the characteristics of IoT technology artefacts that have the greatest influence on organisational adoption.

1.5 Dissertation Layout

This dissertation is divided into six chapters. The first introduces the topic of the Internet of Things by describing preliminary information and then states the problem, the question the study attempts to answer, and the objectives. Chapter 2, presents the literature review that was carried out which focussed on technology adoption, particularly of IoT. Chapter 3 explains the development of the hypotheses and the conceptual model. Chapter 4 explains the methodology adopted, and provides a short discussion on research philosophy, research approaches, strategy, instruments, data collection and analysis. Chapter 5 presents the results of the analysis and the findings that were made. This chapter presents the descriptive statistics results, measurement and structural model findings. Furthermore, hypothesis testing and path coefficients are presented and discussed. The dissertation ends with Chapter 6, which summarises the study, highlighting its theoretical contribution, the practical implications of the study, and recommendations for future research.

CHAPTER 2: LITERATURE REVIEW

2.1 Introduction

The hermeneutic circle framework proposed by Boell and Cecez-Kecmanomc (2010) was used to guide this literature review. Hence, the review consisted of repeated cycles of searches through bibliographic databases, literature selection, and then reading the abstracts, introductions and conclusions of the papers selected. These iterations were done using two interrelated hermeneutic circles, search, acquisition, analysis and interpretation, while sorting, identifying, refining, taking notes, and critiquing the selected publications until a clear understanding was gained and various themes emerged (see Figure 2.1).

The initial search was centred around the need for an overview of IoT and its status in organisations. The search progressed to find literature on technology adoption theories and technology artefact characteristics specific to IoT. Each technology characteristic discovered was identified as a keyword in a quest for meaning and measures for the instrument. As depicted in Figure 2.1, the hermeneutic circles were repeated to uncover trends, patterns, themes, gaps, agreement and contradictions related to each topic or theme identified.

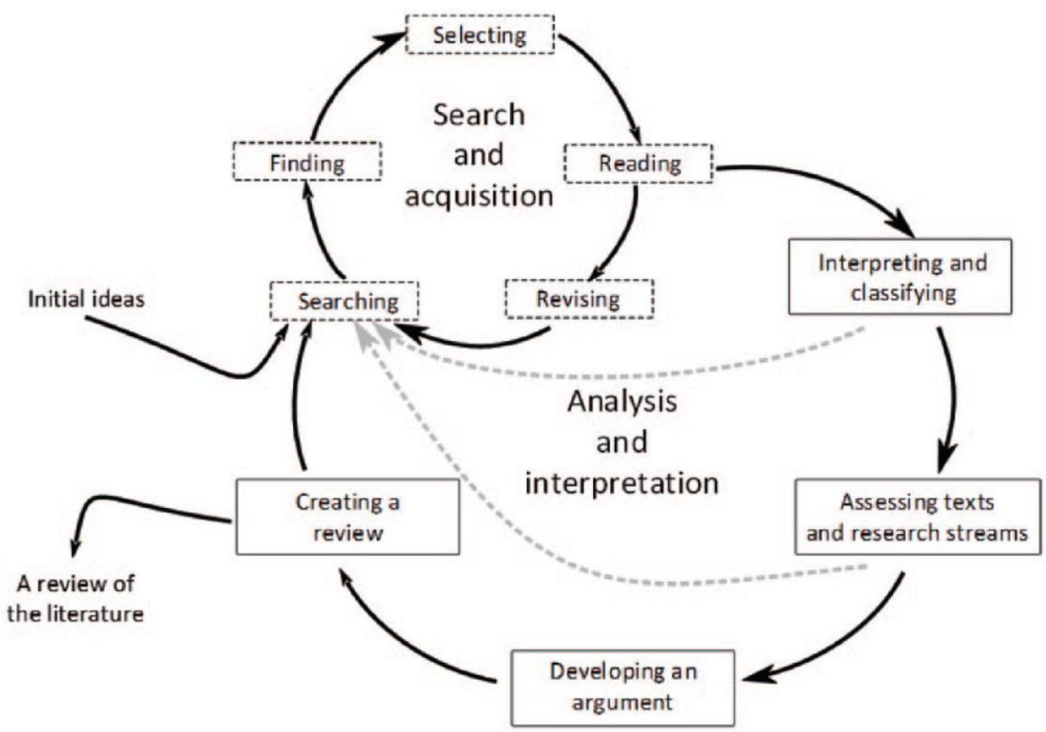

Figure 2.1: A Hermeneutic Framework Literature Review (Boell & Cecez-Kecmanomc, 2014)

Individual keywords that emerged and were used in the search and acquisition process were Internet of Things, benefits, challenges, application adoption, technology adoption, adoption theories, framework, organisations, conceptualisation, definition, compatibility, complexity, connectivity, scalability, adaptability, relative advantage, integration, interactivity, state, security, self-adaptation, intelligence, synchronicity, and interoperability. Once relevant publications were acquired, they were classified and were critically assessed.

The literature review was not meant to be exhaustive or fully systematic but was a reflection on past literature. It was limited to articles published in English in journals and conference proceedings dedicated to IS, organisational studies, and technology adoption. The literature review is structured as follows: an overview of IoT, technologies behind IoT that enable it, the application of IoT in organisations and IoT artefactual characteristics.

2.2 The Internet of Things

The term IoT is defined in many ways, with Sorri et al. (2022) cautioning that IoT is vaguely defined, even among experts, IS specialists and academics. IoT is a new technology paradigm comprising machines, things and devices that can talk to each other in an integrated environment that combines data collection, analytics, and traditional systems (Fernandez-Gago et al., 2024; Lee & Lee, 2015). IoT systems can measure, act, control and make decisions (Díaz et al., 2016; Kronlid et al., 2024). Rayes and Salam (2017, p. 2) define IoT briefly as: "IoT is the network of things, with clear element identification, embedded with software intelligence, sensors, and ubiquitous connectivity to the Internet". Additionally, IoT is a dynamic network infrastructure of easily identifiable, unique things that sense, integrate, actuate and act as an extension of the future Internet, and that possess physical attributes, virtual personalities and intelligent interfaces (Kronlid et al., 2024; Lu et al., 2018).

The strength of IoT is its ability to bring together things, devices and resources that are geographically distributed and it uses a variety of enabling technologies (Fernandez-Gago et al., 2024; Sullivan et al., 2023). Čolaković and Hadžialić (2018) classify these as sensing technologies; identification and recognition technologies; hardware, software and cloud platforms; communication technologies and networks; software and algorithms; positioning technologies; data processing solutions; power and energy storage; and security mechanisms.

2.3 Enabling Technologies

IoT was introduced by Ashton in 1999 and was inspired by a Radio Frequency Identification (RFID) community member who was trying to discover tagged objects using RFID tags and Near Field Communication (NFC) technologies by browsing the Internet. IoT uses the Internet Protocol (IP) as its primary communication method to send and receive datagrams. However, IoT is not limited to the Internet protocol; other network protocols, such as Zigbee, Bluetooth, Lora and Z-Wave are also used for communication (Gvozdenovic et al., 2024).

The solution provided by IoT depends on the integration of these technologies (Patel & Patel, 2016). The communication technologies can be grouped into several types (Evans, 2015; Sharma & Tiwari, 2016), namely NFC, RFID, Quick Response Codes and optical tags, Bluetooth low-energy, Zigbee, IP, Wi-Fi, Machine-to-Machine Communication, and Vehicle-to-Vehicle Communication. Table 2.1 summarises the IoT technologies discussed in the literature and briefly explains what they do.

Table 2.1: IoT Enabling Technologies

Technology	Description	Reference
Radio Frequency Identification (RFID)	Radio waves (electromagnetic fields) are used to identify things wirelessly, without a direct line of sight, using a serial number.	(Barbin et al., 2024; Madakam et al., 2015; Singh, 2016)
Near-Field Communication (NFC)	NFC is a subset of RFID that operates over a very short distance (approximately 4 cm) using high-frequency band signals.	(Ansari & Guo, 2024; Goyal et al., 2018)
Quick Response Codes and Optical tags	These provide another way of encoding information using a combination of bars and spaces on a printable surface which is read by an optical reading device, such as a scanner or camera.	(Scanzio et al., 2024; Singh, 2016)
Bluetooth Low Energy (BLE)	BLE is an inexpensive, short-range radio technology that eliminates the need for proprietary cabling between devices. It has an effective range of 10 - 100 meters on a 2.4GHz ISM Band with 40 channels and uses very little battery power.	(Gvozdenovic et al., 2024; Sharma & Tiwari, 2016; Singh, 2016)

Technology	Description	Reference
ZigBee.	ZigBee's characteristics include low cost, low data rate, relatively short transmission range and low power consumption. It is a network protocol that operates on 16 channels on a 2.4GHz ISM Band. It is often used as a coordinator and router for devices that control lighting, climate and access.	(Gvozdenovic et al., 2024 ; Madakam et al., 2015; Ndih & Cherkaoui, 2016)
Internet Protocol (IP)	This primary protocol is used on the Internet. There are two versions of IP on the market: IPv4 and IPv6.	(Gvozdenovic et al., 2024; Rose, et al., 2025)
Wi-Fi/ 802.11 networks	This is a wireless networking technology that allows computers and other devices to communicate via a wireless signal.	(Sharma & Tiwari, 2016)
Other technologies	Many other enabling technologies are used in the IoT environment including Wireless Sensor Networks, Artificial Intelligence, Machine-to-Machine Communication, Vehicle-to-Vehicle Communication, etc.	(Goyal et al., 2018)

2.4 Application of IoT in Organisations

IoT is changing how organisations operate today. The use of IoT has been growing and appropriate applications are found across different industries and organisations (Kronlid et al., 2024; Lu et al., 2018). This section explores how IoT is applied in organisations and examines various use cases and contexts to understand the practicalities of these applications. Table 2.2 lists some IoT applications adopted by industries but does not cover individual, infrastructural or home applications of IoT. Ahmetoglu et al. (2023) stressed that the challenge of IoT is not primarily technical but is due to a lack of realisation of benefits; finding the value in IoT implementation can reduce adoption impediments in organisations.

Table 2.2: IoT Applications

Industry	Description
Logistics and Supply Chain/Transportation	Among many applications of IoT in logistics and supply chain/transportation are inventory tracking; support logistics; management of planning, re-stocking and distribution activities; predictive equipment maintenance; vehicle tracking and monitoring; delivery management (routes, status, time); and auto-control and intelligent regulation of connected vehicles (Rey et al., 2021)
Agriculture	In agriculture, IoT enables the remote management of farms by the collection and analysis of field data, including environmental conditions, growth status, soil status, irrigation, pest and fertilisers, weed management, the greenhouse production environment, and automation of harvest (Kumar et al., 2023; Wu & Ma., 2020).
Manufacturing	IoT contributions to manufacturing range from connecting factories to tracking assets, controlling the air quality and radiation, access control, monitoring and measuring the level of substances such as gas, and enabling pro-active and remote maintenance and diagnosis (Sivathanu, 2019).
Healthcare	IoT assists medical professionals in diagnosis, patient monitoring, remote surgery, early detection of sickness, tracking hospital equipment's real-time location, and resource management in hospitals and pharmacies (Kumar et al., 2023).
Education	Tertiary education institutions and schools can use IoT to monitor student attendance and academic progress, provide tailored approaches for students with special needs by embedding knowledge in objects for effective study, ensure campus safety, and to adjust and customise the physical class environment (Lu et al., 2018; Kumar et al., 2023).

IoT has become a key factor in the industries listed in Table 2.2 and many others. It links the physical, digital and Internet. However, IoT is not without challenges and caveats. It is challenging to bring technologies together, acknowledge messages, deliver a functioning system, and maintain boundaries. Without a proper understanding of IoT, it becomes complicated for organisations to adopt it (Sorri et al., 2022). The following sections deal briefly with theories, the characteristics of technology that define an IoT system and the challenges that impede its smooth operation.

2.5 IoT Artefactual Characteristics

The IS discipline is situated between the organisational and technical sciences, making it challenging even for a group of IS specialists to define an artefact (Chatterjee et al., 2017). Orlikowski and Iacono (2001, p.288) defined Information Technology Artefact (ITA) as "… a distinctive element of our field, binding together multiple heterogeneous elements of hardware, software, humans and institutions". Later Gregor and Hevner (2013, p.341) argued that ITA is used "… to refer to a thing that has, or can be transformed into, a material existence as an artificially made object (e.g., model, instantiation) or process (e.g., method, software) ". However, these definitions do not sufficiently clarify an ITA, at least not for IoT. A description that is more appropriate for IoT is provided by Goldkuhl (2013, p.93), referring to ITA as "… a physical artefact based on technology. The software and hardware can be seen as an integrated whole. Without the software, the hardware is just an empty shell. Without hardware, the software is just symbolic expressions. However, bundled together, they are machines with the power to execute intentionally designed information-processing tasks."

The information technology artefact is the core of IS research (Matook & Brown, 2017; Orlikowski & Iacono, 2001; Petter et al., 2018). Understanding a technology based on its artefactual characteristics is essential to understanding a particular artefact's adoption (Yan et al., 2021).

Kronlid et al. (2024) identified nine artefact characteristics when looking into IoT adoption in healthcare. These are compatibility, complexity, costs, relative advantage, robustness, energy management, technological development, trialability and usability. Earlier, Matook and Brown (2017) drew from systems thinking to identify seven characteristics that describe an IT artefact: integration, connectivity, complexity, state, adaptation, self-adaptation and synchronicity. Since IoT is an IT artefact, it may be usefully described in terms of these characteristics. Sha et al. (2018) cited an additional two characteristics of IoT, namely scalability and interactivity; these reflect the effect of an ever-increasing number of IoT devices on the infrastructure and the resulting high level of interaction. According to Ng and Wakenshaw (2017), IoT objects possess seven properties or characteristics: sensibility, addressability and traceability, associability, communicability, programmability, and memorability. Their choice of names for the characteristics differs from the ITA characteristics defined by Matook and Brown (2017). For instance, communicability is akin to connectivity. They refer to the state as memorability, integration as associability, and self-adaptation as programmability.

Kamble et al. (2019) identified twelve potential barriers to the adoption of IoT in organisations: lack of regulations, lack of standardisation, security and privacy, costs, payback, connectivity, skills availability, integration, compatibility, scalability, validation and identification, energy consumption and architecture. Five of these can be linked to IoT artefact characteristics. Chang et al. (2014) studied the influence of IoT product characteristics on consumer intention to purchase. Six of these (connectivity, interactivity, telepresence, intelligence, convenience and security) influenced consumer intention to purchase an IoT product (Chang et al., 2014).

Pinochet et al. (2018), in order to understand what drives consumers to use disruptive technologies, stated that the attributes or characteristics of IoT products need to involve the feelings and understandings of the consumer. In another study on the influence of the attributes of IoT products on the functional and emotional experience of purchase intention, these same authors confirmed that the model proposed by Chang et al. (2014) to evaluate the effects of IoT attributes on the users' intention to purchase was valid. This model highlighted six characteristics of IoT products: connectivity, interactivity, sense of presence, intelligence, convenience, and security. A summary of IoT characteristics found in the reviewed literature provides an overview of the meaning and where the characteristics have been mentioned or discussed (see Table 2.3).

Table 2.3: Summary of IoT Characteristics

IoT Characteristics	**Description**	**Reference**
Compatibility	A state in which things can co-exist or occur together without conflict. It is also the degree to which an innovation fits with the adopter's values, needs, past experiences and practices.	Ahmetoglu et al., 2023 ; Bassi et al., 2013; Kamble et al., 2019; Rogers, 1995
Complexity	The degree to which an innovation is considered difficult to understand and use.	Ahmetoglu et al., 2023 ; Ndih & Cherkaoui, 2016; Rogers, 1995

IoT Characteristics	Description	Reference
Connectivity	The degree to which things are interconnected and able to share information and data when interconnected.	Bassi et al., 2013; Fernandez-Gago et al., 2024 ; Chang et al., 2014; Kamble et al.2019; Matook & Brown, 2017; Palattella et al.,2016; Sullivan et al., 2023
Scalability	The ability of an artefact to handle an increasing workload and volume. It can also be viewed as the ability of a system to allow the addition of new devices and services without experiencing performance degradation. It ranges from static to dynamic.	Chang et al., 2014; Čolaković & Hadžialić, 2018; Kamble et al., 2019; Patel & Patel, 2016; Pichlak, 2016; Pinochet et al., 2018; Rayes & Salam, 2017; Sharma et al.,2023
Convenience or Relative Advantage	The degree to which an innovation is perceived as better than the idea it supersedes. It often refers to benefits (such as time and effort savings when planning, purchasing, and using a product), or simply the competitive advantage the artefact offers.	Ahmetoglu et al., 2023; Al-Momani et al., 2016; Pichlak, 2016; Rogers, 1995; Sullivan et al., 2023
Integration	This refers to how various parts that form an IoT artefact work together to achieve a common goal.	Bassi et al., 2013; Brous & Janssen, 2019; Fernandez-Gago et al., 2024; Čolaković & Hadžialić, 2018; Sullivan et al., 2023
Interactivity	This is seen as the extent to which users can participate in modifying the form and content of a mediated environment in real-time and communicate bidirectionally and respond promptly to remote objects.	Chang et al., 2014; Ehie & Chilton, 2020 ; Jiang et al., 2010; Madakam et al., 2015; Pichlak, 2016; Polgavande & Kulkarni, 2017
State	It is the ability to maintain a state and to record and remember previously performed events in each interaction sequence.	Ng & Wakenshaw, 2017; Matook & Brown, 2017; Patel & Patel, 2016
Security	The degree to which damage to vulnerable and valuable assets can be avoided.	Al-Momani et al., 2016; Rekha, Shashi et al., 2023; Butun et al., 2019; Matook & Brown, 2017; Raimundo & Rosário, 2022

IoT Characteristics	Description	Reference
Self-Adaptation	The ability of an artefact to adapt on its own, based on feedback. It is also considered to be the intelligence embedded in an artefact equipped with intricate and accurate recognition functions, judgment capabilities and effective implementation features.	Butun et al., 2019; Chang et al., 2014; Ng & Wakenshaw, 2017; Pinochet et al., 2018; Sivathanu, 2019;
Synchronicity	It is a state in which systems or people work together simultaneously, with a common focus on sharing information in a timely manner and a shared pattern of coordinated behaviour.	Bassi et al., 2013; Dennis et al., 2008; Lu et al., 2018; Matook & Brown, 2017; Shin, 2019; Thomas et al., 2023;
Interoperability	The ability of two or more IoT systems to acknowledge and communicate with one another, regardless of deployed hardware and software, and hence to allow the use of key functionalities of the respective other system.	Abdelghaffar & Abousteit, 2021; Bassi et al., 2013; Brous & Janssen, 2019; Fernandez-Gago et al., 2024; Giri et al., 2017; Madakam et al., 2015; Noura et al., 2019; Polgavande & Kulkarni, 2017

2.6 Literature Review Summary

An IoT is a network of dynamic objects that can be discovered and identified, self-adapt and respond to stimuli, collect and share data, and connect to the Internet (Kronlid et al., 2024; Rayes & Salam, 2017). It has promised to revolutionise the technology world; however, despite its many benefits, organisations have hesitated to adopt IoT (Rey et al., 2021). The hermeneutic circle's framework was used to survey the literature to explain this challenge and the reasons for slow IoT adoption and low continuance in organisations (Boell & Cecez-Kecmanomc, 2010).

The technologies that enable things to talk with one another depend on integration with different technologies and working together (Patel & Patel, 2016). Previous studies have listed these technologies as RFID, NFC, Bluetooth, ZigBee, Artificial Intelligence, Wi-Fi, as well as several others (Madakam et al., 2015; Singh, 2016; Sharma & Tiwari, 2016; Goyal et al., 2018). These technologies enable logistics and supply chain industries to track inventory, auto-control and regulate vehicles, predict maintenance, and manage delivery (Rey et al., 2021). Farmers can remotely monitor their crops, livestock, and the state of the farm, such as the moisture in the soil and temperature, and detect crop diseases before they break out (Kumar et al., 2023; Wu & Ma, 2020).

There are many benefits to organisations, and opportunities for new services are made possible. However, scholars have not made understanding IoT Systems at the organisational level simple and have neglected to define the artefactual characteristics clearly (Rey et al., 2021). Hence, scholars have been calling for a deeper engagement with technology at the artefactual level (Matook & Brown, 2017; Orlikowski & Iacono, 2001; Zhou et al., 2024). Literature shows that the IoT Artefact has distinct characteristics that can influence its acceptance in organisations, namely, compatibility, complexity, connectivity, scalability, relative advantage, integration, interactivity, state, security, self-adaptation, synchronicity, and interoperability.

CHAPTER 3: THEORETICAL FRAMEWORK AND HYPOTHESES DEVELOPMENT

3.1 Introduction

This chapter covers the development of the hypotheses. It begins with a discussion of relevant theories, defines key concepts, situates them in the literature, and formulates hypotheses to be tested.

Theories describe, explain, and predict phenomena, including technology adoption behaviors in individuals and organisations (Kronlid et al., 2024; Gregor & Hevner, 2013). Many theories have been used to explain users' and organisations' adoption of technology; among these are Theory of Planned Behaviour (TPB), Diffusion of Innovation (DOI) theory (Rogers, 1995), Technology Acceptance Model (TAM), Technology-Organisational-Environment (TOE) framework (Tornatzky & Fleischer, 1990), Unified Theory of Acceptance and Use of Technology (UTAUT) (Kronlid et al., 2024). Despite the proliferation of adoption theories, the acceptance and implementation of new technologies remain imperfectly predictable (Hillmer, 2008), underscoring the need for context-specific frameworks.

A technology artefact's characteristics significantly influence its adoption (Oliveira & Martins, 2011). The Technology-Organisational-Environment (TOE) framework (Tornatzky & Fleischer, 1990) is widely used in IS research to analyse organisational adoption (Oliveira et al., 2014). It identifies three adoption contexts: Technological, Organisational, and Environmental (Baker, 2012).

TOE often integrates Diffusion of Innovation (DOI) theory (Rogers, 1995) to operationalise technological characteristics—relative advantage, compatibility, complexity, observability, and trialability (see Figure 3.1). However, DOI’s focus on generic innovation attributes overlooks IoT-specific factors. This study extends TOE and DOI by incorporating IoT-specific characteristics (see Table 2.3), enabling a holistic examination of adoption drivers.

3.2 Theoretical Background

The TOE framework is a foundational lens for studying innovation adoption, but its technological dimension often relies on DOI theory to define innovation attributes. As illustrated in Figure 3.1, DOI's characteristics (e.g., relative advantage) map onto TOE's technological context, while TOE's organisational and environmental contexts address broader adoption determinants.

TOE's Organisational Context includes factors like management support, firm size, and culture (Tornatzky & Fleischer, 1990). The Environmental Context covers external pressures (e.g., competition, regulations) (Baker, 2012). DOI's theory explains adoption speed via five characteristics (Rogers, 1995) and adopter categories (innovators, early adopters, early majority, late majority, and laggards).

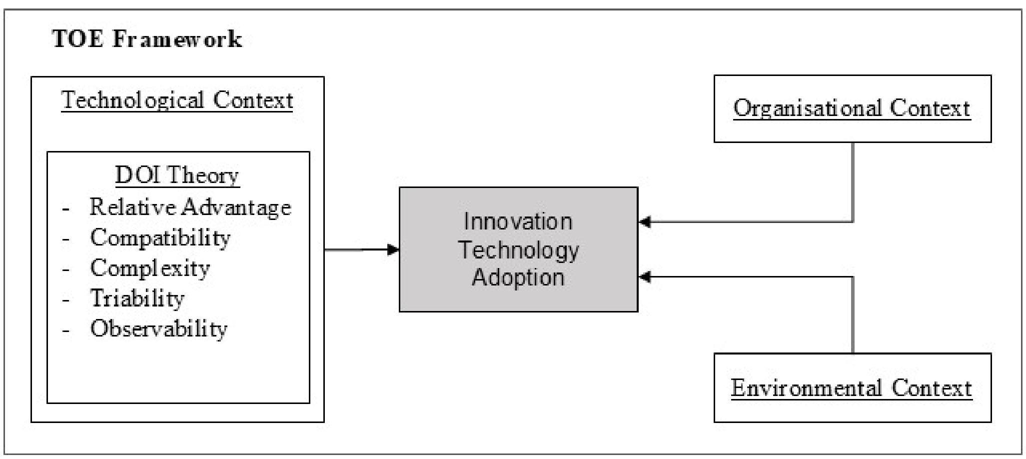

Figure 3.1: Integration of DOI and TOE Frameworks

While DOI and TOE are seminal frameworks, they fail to fully account for IoT's unique characteristics, such as security, interoperability, and scalability (see Table 2.3). This study addresses this gap by synthesizing TOE, DOI, and IoT-specific traits (e.g., connectivity, self-adaptation) to refine adoption theory. The resulting framework (Figure 3.2) integrates core DOI/TOE constructs (compatibility, complexity, relative advantage) with IoT-specific drivers (connectivity, security, interoperability, etc.), offering a holistic model for IoT adoption.

The following sections operationalise these theoretical insights into testable hypotheses, focusing on how IoT-specific characteristics moderate adoption intentions.

3.3 Compatibility

Compatibility is the degree to which an innovation fits within the adopter's existing values, past experiences, needs, practices and strategies (Rogers, 1995; Ahmetoglu et al., 2023). In line with this, organisations adopt and continue using innovations that conform to their culture, processes, corporate tradition and technology lifecycle to minimise risk and disruption (Mukherjee et al., 2024). Compatibility leads to the rapid adoption of new technology (Ramavhona & Mokwena, 2016). In the context of the present research, the first hypothesis is stated as:

H1: The Compatibility of the IoT artefact with existing organisational values and needs influences its adoption as reflected by the continuance intention of organisations.

3.4 Complexity

Complexity relates to the degree to which potential adopters perceive an innovation to be difficult to understand, learn or use (Ahmetoglu et al., 2023). In the case of IoT, the imprecision and inadequacy of clarity of the basic concept may make it difficult to understand, implement and operate (Sorri et al., 2022). In general, the complexity of innovation has, as shown in past studies, forced a significant number of organisations to outsource the implementation and ongoing use, and this pushes up the cost of adoption (Evans, 2015). Furthermore, IoT systems require highly trained professionals to develop and implement practical applications and solutions that benefit organisations (Kamble et al., 2019). Complexity has previously been shown as having a negative influence on the adoption of IoT, leading to the second hypothesis.

H2: The Complexity of the IoT artefact negatively influences its adoption as reflected by the continuance intention of organisations.

3.5 Connectivity

Connectivity is the level of linkage between system elements and the environment (Matook & Brown, 2017). Oberländer et al. (2018, p. 488) defined IoT as “the connectivity of physical objects (things) equipped with sensors and actuators to the Internet via data communication technology, enabling interactions with and among these objects”. This definition places connectivity at the centre of IoT; connectivity plays an essential and influential role. As a result, poor and unreliable Internet connectivity poses a challenge to the adoption of IoT, and conversely the diversity and availability of network technologies positively influences the adoption of IoT (Kronlid et al., 2024; Palattella et al., 2016). Therefore, the following hypothesis is proposed.

H3: The Connectivity of the IoT artefact influences its adoption as reflected by the continuance intention of organisations.

3.6 Scalability

Scalability, referred to as adaptation by Matook and Brown (2017), is the ability of a technology artefact to capture and handle change and in particular increases in scope and breadth of usage, workload, speed, volume, number of connected devices and systems (Sharma et al., 2023). Sharma et al. (2023) note that scalability creates a sustainable and repeatable capacity leading to continuance adoption. The scalability problem is not new; many innovations and organisational information systems have been reported to have performed well during the initial phase, only to fail when the load increases and the rapid proliferation of devices occurs (Hamad et al., 2024). As previously explained, IoT systems depend on interconnected things and services, and scalability can become challenging with more connected things and systems (Hamad et al., 2024; Kamble et al. (2019). This means that scalability is critical to the future and continuance of IoT. Hence the fourth hypothesis is stated as:

H4 The Scalability of the IoT artefact influences its adoption as reflected by the continuance intention of organisations.

3.7 Relative Advantage

Relative advantage is the expected benefits from an innovation; it is the degree to which the new product is perceived as being better than the one it supersedes (Ahmetoglu et al., 2023; Chang et al., 2014). The convenience offered by an innovation is relative to its level of adoption, and hence is considered to be a robust predictor (either direct or indirect) of IoT adoption as reflected by the continuance intention (Ahmetoglu et al., 2023; Ramavhona & Mokwena, 2016). The adoption barriers can be reduced and ultimately removed if adopters realise the value and benefits organisations can draw from implementing IoT (Ahmetoglu et al., 2023). Relative advantage, hence, is shown as having a positive influence on the adoption as reflected by the continuance intention of IoT, leading to the fifth hypothesis:

H5: The Relative Advantage of the IoT artefact influences its adoption as reflected by the continuance intention of organisations.

3.8 Integration

Integration is the extent of connectivity that allows the addition of more utilities to a system. In the context of IoT, this includes connectivity between various systems and sub-systems, legacy systems, physical objects and digital objects, sensors and actuators, and backend systems (for example, databases that store and distribute data) (Palacios-Marqués et al., 2015; Sullivan et al., 2023). Integrating systems facilitates a smooth transfer of data and exchange of information, allows them to work together, and influences the extent to which an organisation can adopt or continue to use a particular innovation (Ehie & Chilton, 2020; Sullivan et al., 2023). The lack of IoT standards, the native heterogeneity evident at the device level, and the need for use of heterogeneous data all add to integration challenges and are severe impediments to the adoption of IoT (Brous & Janssen, 2019; Noura et al., 2019). Hence the following hypothesis is proposed:

H6: The Integration of the IoT artefact influences its adoption as reflected by the continuance intention of organisations.

3.9 Interactivity

A major advantage of IoT lies in making it possible for things to work together and interact (Fernandez-Gago et al., 2024). IoT has expanded the meaning of interactivity, as previously consumers could only interact with objects located nearby (Chang et al., 2014).

Interactivity is the extent to which people and things can jointly participate in modifying the form and content of a mediated environment in real-time, communicating bidirectionally and responding promptly to remote objects (Jiang et al., 2010).

An IoT system must be able to interact with objects in the physical and digital world and to handle data sourced from disparate systems regardless of their physical location and distance (Ehie & Chilton, 2020). The seventh hypothesis is stated as:

H7: The Interactivity of the IoT artefact influences its adoption as reflected by the continuance intention of organisations.

3.10 State

A state-enabled system remembers its actions and can return to its original state or transition to another suitable state to maintain equilibrium (Mayar et al., 2022). The state of a system includes, but is not limited to, sleeping and waking up, being connected and disconnected, and has indicators such as location and speed (Patel & Patel, 2016). The ability of a technology artefact to keep a record of prior connections and historical logs when interacting with other parts of its environment is deemed to be an important characteristic (Ng & Wakenshaw, 2017; Matook & Brown, 2017; Patel & Patel, 2016). Hence the following hypothesis is proposed.

H8: The State of the IoT artefact influences its adoption as reflected by the continuance intention of organisations.

3.11 Security

Security is a major challenge to the implementation of IoT and its continuance intention in organisations (Ahmetoglu et al., 2023; Koohang et al., 2022; Gao and Bai, 2014). Security is the extent to which damage to things, assets, people, communities and organisations can be avoided (Chang et al., 2014), and the extent to which a product technology is risk-free (Al-Momani et al., 2016). Security and safety are essential in vulnerable environments such as the one in which IoT is located, and are used as a means to protect data, interconnected devices, and systems from unauthorised access and breaches (Kronlid et al., 2024). Therefore, IoT security is a fundamental priority to be addressed (Rose et al., 2015). Kamble et al. (2019) estimated that trillions of devices connected to the Internet were at risk from cyber-attacks and data theft. Hence, security is central to the functioning of IoT and is a major concern for many organisations as it introduces new forms of cyber security breaches and poses a challenge to the adoption of IoT in organisations (Koohang et al., 2022; Kronlid et al., 2024; Mukherjee et al., 2024). Hypothesis 9 reflects this concern.

H9: The Security of the IoT artefact influences its adoption as reflected by the continuance intention of organisations.

3.12 Self-Adaptation

Self-adaptation is the ability of an artefact to adapt on its own, based on feedback (Matook & Brown, 2017). Self-adapting objects have some form of built-in intelligence and include extensive and accurate data recognition functions, analysis and judgment capabilities, with resultant practical implementation strategies (Chang et al., 2014). Gao and Bai (2014) describe IoT as things that talk to each other using the Internet or some other form of connectivity to communicate and extend their intelligence using machine learning. As they communicate, the components can act in harmony to achieve a common goal (Brous & Janssen, 2019) and share information (Patel & Patel, 2016). Self-adaptation both simplifies product usage and reduces complexity from the point of view of the organisation (Chang et al., 2014). The following hypothesis addresses this:

H10: The Self-adaptation of the IoT artefact influences its adoption as reflected by the continuance intention of organisations.

3.13 Synchronicity

In a complex or heterogeneous environment, a system must maintain unity among its parts to continue functioning smoothly, and each part involved has to coordinate its functioning with the whole by acknowledging and sending feedback immediately (synchronously) or at a scheduled time (asynchronously) (Durant, 2002). It is a state in which systems (including the people involved) work together, with a common focus on sharing information in a timely manner and a shared pattern of coordinated behaviour (Dennis et al., 2008; Thomas et al., 2023). Like other systems, the IoT system's communication with the ecosystem needs to happen timeously and in a coordinated manner; their actions must occur at a rate that matches the activities of the other parts of the ecosystem in which they operate (Matook & Brown, 2017). Therefore, in the context of the present research, Hypothesis 11 is stated as:

H11: The Synchronicity of the IoT artefact influences its adoption as reflected by the continuance intention of organisations.

3.14 Interoperability

Interoperability is the extent to which two or more systems can communicate and share information (Abdelghaffar & Abousteit, 2021). This ability is not limited to exchanging information between systems and sub-systems but includes using the information a sub-system receives and sharing services (Noura et al., 2019).

Interoperability is a key issue in IoT, as it involves trust and functionality, as well as the interoperability of devices, networks, platforms and other interfacing components; it can be classified as syntactical interoperability or semantic interoperability (Fernandez-Gago et al., 2024; Noura et al., 2019). Interoperability is frequently a factor in IoT systems' implementation challenges. Businesses typically realise only approximately 40% of IoT potential; if interoperability challenges were overcome access to this potential benefit could increase, there would be resulting improvements in business performance, and business isolation in the market would be reduced (Abdelghaffar & Abousteit, 2021; Fernandez-Gago et al., 2024). Hence, the hypothesis:

H12: The Interoperability of the IoT artefact influences its adoption as reflected by the continuance intention of organisations.

3.15 Hypothesis Development Summary

This study proposes twelve hypotheses to be tested (see Table 3.1) and depicted in Figure 3.2. The hypotheses were derived from the twelve characteristics identified in the literature. As reflected in the hypotheses, the IoT artefactual characteristics to be investigated are compatibility, complexity, connectivity, scalability, relative advantage, integration, interactivity, state, security, self-adaptation, synchronicity and interoperability.

Table 3.1: Research Study Hypotheses

	Hypothesis description
H1	The Compatibility of the IoT artefact with existing organisational values and needs

	Hypothesis description
	influences its adoption as reflected by the continuance intention of organisations.
H2	The Complexity of the IoT artefact negatively influences its adoption as reflected by the continuance intention of organisations.
H3	The Connectivity of the IoT artefact influences its adoption as reflected by the continuance intention of organisations.
H4	The Scalability of the IoT artefact influences its adoption as reflected by the continuance intention of organisations.
H5	The Relative Advantage of the IoT artefact influences its adoption as reflected by the continuance intention of organisations.
H6	The Integration of the IoT artefact influences its adoption as reflected by the continuance intention of organisations.
H7	The Interactivity of the IoT artefact influences its adoption as reflected by the continuance intention of organisations.
H8	The State of the IoT artefact influences its adoption as reflected by the continuance intention of organisations.
H9	The Security of the IoT artefact influences its adoption as reflected by the continuance intention of organisations.
H10	The Self-adaptation of the IoT artefact influences its adoption as reflected by the continuance intention of organisations.
H11	The Synchronicity of the IoT artefact influences its adoption as reflected by the continuance intention of organisations.
H12	The Interoperability of the IoT artefact influences its adoption as reflected by the continuance intention of organisations.

The conceptual framework (Figure 3.2) shows the complete set of IoT artefact characteristics (or constructs) that are deemed to influence organisational adoption as reflected by the continuance intention of IoT derived from the hypotheses.

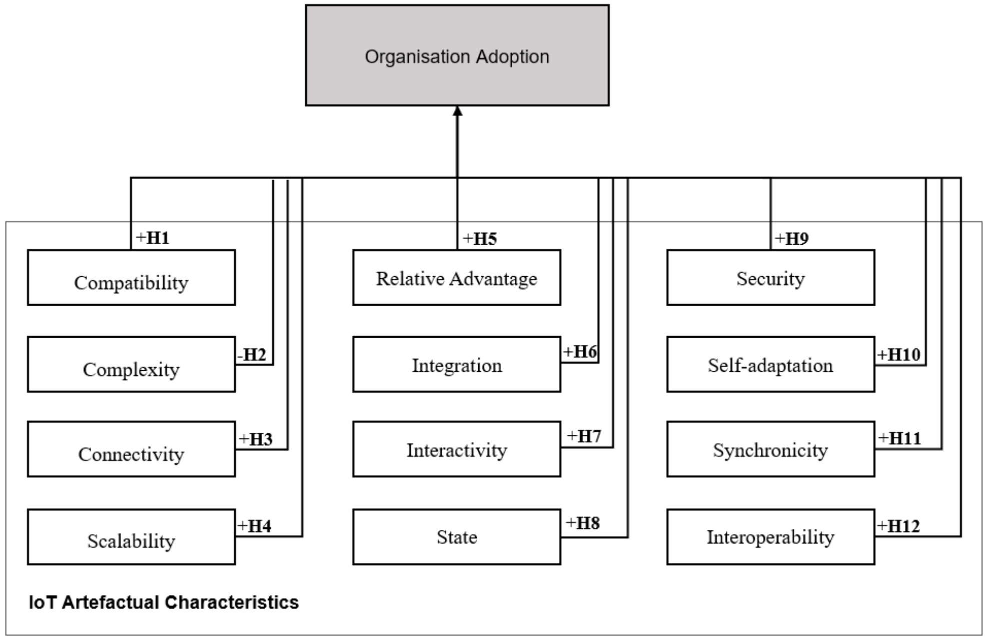

Figure 3.2: Conceptual Model – IoT Characteristics' Impact on IoT Organisation Adoption

CHAPTER 4: RESEARCH METHODOLOGY

4.1 Introduction

This chapter covers the methodology used to carry out this study. The research onion model developed by Saunders et al. (2019) provided guidance on steps to follow and their order. The onion layers and the different layers of this model are philosophies, approaches, strategies, method choices (mono, multi, and mixed), time horizon, and data collection and analysis (Saunders et al, 2019). Chapter 4 begins with a brief discussion of the research philosophy, followed by the research approach. Next, it deals with the research strategy, data collection, and analysis. The chapter ends with the research quality and ethical considerations.

4.2 Research Philosophy

Research philosophy deals with the set of beliefs related to the nature of reality being considered; it is often studied in terms of ontology and epistemology. Ontology focuses on 'being' and is interested in knowing 'what is' and what can be known about the world. It refers to the assumptions we make when we look at the world (Bhattacherjee, 2012). The ontology adopted considers pragmatic, constructivist, and objective views. The ontology followed in this study is objectivism, which believes that knowledge exists outside of us and is independent of our personal beliefs; hence, it assumes a scientific research method can uncover the links between casual things and their causes (Saunders et al., 2019).

On the other hand, epistemology refers to the researcher's assumptions about the best way to study the world (Bhattacherjee, 2012) and whether to use an objective or subjective approach. Interpretivism, realism, and positivism are often linked to epistemology. This research used the positivist epistemology, which maintains that knowledge creation should be based entirely on what can be observed and measured. Positivism supports the creation of theories using evidence that can be tested and measured (Saunders et al., 2019). It is typically characterised by testing hypotheses derived from existing theories of knowledge. This study required rigorous testing of IoT artefact characteristics that influence its adoption as reflected by the continuance intention of organisations.

4.3 Research Approach

A research approach can be abductive, inductive or deductive (Saunders et al., 2019). This study adopted the deductive approach, also known as theory testing. A deductive approach is used to extend or modify existing theories and to answer new questions or explain new phenomena. Such a study starts with a theory and moves on to test, confirm or reject hypotheses using new empirical data (Battacherjee, 2012). The study identified the hypotheses in Table 3.1 and the conceptual model depicted in Figure 3.1.

4.4 Research Strategy

A research strategy is a plan to answer a researcher's research question. It is the link between the underlying philosophy and the subsequent choice of methods to collect and analyse data. Different strategies exist (namely, experiment, survey, archival and documentary research, case study, ethnography, action research, grounded theory methodology and narrative inquiry) (Saunders et al., 2019).

This research adopted a quantitative survey strategy, using standardised questionnaires to systematically collect data about the people participating as research participants, and their preferences, thoughts and behaviours (Bhattacherjee, 2012). Surveys provide a cost-effective way to test hypotheses as they allow many potential participants to be reached over a relatively short period, even those located remotely, and at a lower data collection cost.

4.5 Research Timeframe

The limited time available for the study restricted it to a cross-sectional or snapshot view with data collected only over the given period (Saunders et al., 2019; Yilmaz, 2013). Nevertheless, using the survey strategy access to scarce experts in IoT was possible despite the time constraints.

4.6 Measurement Instrument

The instrument's measurements were adapted from previous studies. The questionnaire used to collect data consisted of two sections. The first collected demographic information and the second section collected responses related to questions focussing on the twelve independent variables and one dependent variable. Before the section related to the demographic information, the participants were asked screening questions.

1) Demographic information: This section collected information such as age, gender, highest education, positions occupied by the participants in their organisations, IT experience, IoT experience, the sector in which the organisation operates (private, public, not-for-profit), the industry in which the organisation operates, the period of existence of the organisation, and the size of the organisation measured in the number of employees in the organisation. The last question dealt with the IoT adoption status of the organisation.
2) The second part of the questionnaire evaluated the twelve IoT characteristics used in the formulated hypotheses and their influence on IoT adoption as reflected by the continuance intention. Data was collected for each of these IoT characteristics by means of between two and six questions (items) in the questionnaire, All items were evaluated using a five-point Likert scale, with one (1) indicating 'strongly disagree' and five (5) indicating 'strongly agree'. Fifty-three questions were presented to the participants randomly. Two of these were in reverse mode to evaluate the attentiveness of the participants. These were one of the Complexity items (item five) and one of the Interactivity items (item three). Table 4.1 shows the source in the literature from which each characteristic (represented as a construct in the model) was adopted, the name of the associated variable and how many items (that is, questions) were used to collect data per construct. All of the items which were used as measures were adapted from the sources indicated in Table 4.1 and the complete instrument can be found in Appendix A: Research Instrument. Variable names are assigned to constructs as these are short and can be used in the tables reporting statistical analyses. These variable names were also given in the questionnaire (Appendix A) and the items (questions) associated with a construct were assigned codes as identifiers which could easily be associated with the corresponding variable.

Table 4.1: Construct, Number of Items and Measurement Sources

Variable	Construct	Number of Items	Adapted from Source
OADP	Organisation Adoption	3	Lai et al. (2016)
SCA	Scalability	5	Sharma et al. (2023)
CMPA	Compatibility	3	Mohammed et al., 2016
CMPX	Complexity	5	Mohammed et al., 2016
CON	Connectivity	4	Dong et al. (2017)
INTG	Integration	5	Wixom & Todd (2005)
INTA	Interactivity	4	McMillan & Hwang (2002)
INTO	Interoperability	3	Derived from Bassi et al. (2013)
RA	Relative Advantage	6	Tsai et al. (2010)
SEC	Security	5	Chong & Chan (2012)
SAD	Self-adaptation	3	Dong et al. (2017)
STA	State	4	Derived from Matook & Brown (2017) Definition
SYN	Synchronicity	4	Thomas et al. (2023)

4.7 Data Collection

This section provides details of the target population, how the sample size was determined, and measures taken to avoid bias and improve generalisability.

4.7.1 Sampling

The process of selecting the participants for a study, sampling, begins with determining the population, the sampling frame and the sampling strategies to follow.

A population is the relatively large group of people from whom a researcher plans to collect the data; the findings can eventually be inferred from that data (Haegele & Hodge, 2015). Hence it is comprised of all the people or items that possess the characteristics one wishes to study. In the case of this study the researcher set out to establish the status of IoT adoption in organisations and the technological artefacts that influence its adoption as reflected by the continuance intention. In order to achieve this, the study targeted IT professionals (including IoT experts, IT executives, IT managers, and technology specialists) with knowledge of IoT implementation and whose organisations had already implemented or were in the process of implementing IoT. The study refined the population further to include only organisations that had investigated or adopted IoT. This allowed the study to measure IoT adoption as reflected by the continuance intention.

4.7.2 Sampling Strategy

The research used an online survey. Prolific Academic (https: //www.prolific.com/), an online panel platform, sourced potential participants, and the Qualtrics Online Platform (https: //www.qualtrics.com/) was used to design and collect the survey data. Survey research is increasingly moving online, with an increasing number of potential research participants having Internet access (Newman et al., 2021). Use of online panels has been growing, even among scholars, for the last decade and is accepted by many as a legitimate way to collect quantitative research data (Porter et al., 2019). There are several advantages to using this method, such as extensive geographical coverage, less intrusiveness, reduced researcher bias, and a relatively low level of inattentiveness on the part of participants (Evans & Mathur, 2018; Newman et al., 2021).

In this research, measures for attention checks were included by presenting three reverse questions; participants were specifically encouraged to consider choosing "somewhat disagree" rather than only considering the other options. Measures were in place to prevent multiple submissions and to limit geographical location; this was done by recording IP addresses and removing duplicates. The participant's degree of involvement with the content was tracked by recording the time the participants took to complete the survey. One of the recommendations from Kees et al. (2017) as a way to avoid group bias is to collect data at various times of day and days of the week. This advice was followed to obtain a diverse and representative sample, and the data was collected in a series of batches which were made available several times during the day and night and on different days, including weekdays and weekends.

Prolific[2] predominantly uses purposeful sampling, as potential participants are assigned to the survey based on their profile and background, which must meet the set criteria. In the case of the research reported here, participants needed to have one of these qualifications or titles: IoT

[2] (https: //www.prolific.com/)

expert, IT executive, IT manager, or technology specialist, or have had a say in adopting new technology in his or her organisation. A fair knowledge and understanding of IoT implementation was also a prerequisite. These eligibility criteria meant that the label ‘purposive sampling’ is appropriate for this study, as it adopted non-probability and purposeful sampling techniques. Bhattacherjee (2012) indicates that purposeful sampling is used when participants need to have a stipulated degree of knowledge and understanding of the phenomenon being researched. The phenomenon being studied, that is, the artefactual characteristics that lead to the adoption of IoT in organisations, require expertise and technical knowledge of IoT.

4.7.3 Sample Size

At the time of the data collection, Prolific[3] had 212279 potential participants on its platform, of whom 1138 fitted the given criteria and hence were eligible to participate in the study. The sample size of this study was determined using Slovin's formula. This simple formula has been used in many studies to determine the sample size (Tejada & Punzalan, 2012). To determine the sample size, the study needed a 95 per cent confidence level and a tolerable margin of error of 5 per cent; according to a table provided by Saunders et al. (2019, p. 784), a 95 per cent confidence level results in a z score of 1.96. These values were applied to Slovin's formula (provided in Figure 4.1) to obtain the minimum sample size required.

$$n = \frac{n_0}{1 + \frac{n_0}{N}} \qquad \text{Where} \qquad n_0 = \frac{z^2 p(1-p)}{e^2}$$

Figure 4.1: Slovin's Formula

N is the population size (1138), z is the standard normal variate based on the 95 per cent degree of confidence, and e is the error margin (5 per cent), resulting in n_0=384.15 and a minimum sample size (n) of 287. The resulting sample size 287 was compared to the one obtained using the Qualtrics sample size calculator[4]. Using the same confidence level, margin of error, and population size, the Qualtrics Sample Size Calculator suggested 288 as the ideal sample size.

[4] https: //www.qualtrics.com/

<table>
<tr><td rowspan="3">Z^2</td><td>Z Score</td><td>1,96</td><td rowspan="3">3.84</td></tr>
<tr><td>Confidence Interval</td><td>95%</td></tr>
<tr><td>Alpha divided by 2</td><td>0.025</td></tr>
</table>

p	0.5
Error margin	0.05
Population size	1138

.

Three hundred fifteen (315) responses were collected, and after cleaning the data (removing obviously incomplete data or data entered too fast indicating low level of attention), the final sample size was two hundred and ninety-three (293). This sample size was suitable for this study as it exceeded the minimum of 287 set by Slovin's formula and the minimum of 288 set by the Qualtrics Sample Size Calculator.

4.8 Pilot Study

The research instrument was first tested using an online panel from Survey Monkey (https://www.surveymonkey.com/). A sample size of 120 participants was used. The pilot study aimed to get feedback specifically on how participants understand and interpret the instrument items. Doing a pilot study helped the researcher to rephrase the questions and prevent fatal flaws that might have affected the internal validity and reliability of the data that would be collected later. The pilot study set out to ensure that each question measured what it was intended to measure, was understood in the same way by the participants, and that each set of questions covered most if not all aspects of the construct it measured (Saunders et al., 2019).

The result of the pilot study indicated that the questions were too long; with the questionnaire consisting of twelve (12) constructs that were to be tested using 53 questions, keeping each question as short and succinct as possible was necessary. Results from calculations of Cronbach's alpha and cross-loading factors were taken into consideration. Evidence of undesirable cross-loading helped identify ambiguous items and these were revisited, rephrased and, where required, removed (Hite et al., 2016). One of the most important feedbacks obtained from the pilot study was that it highlighted the subject's complexity and the audience's limited understanding of the implementation of IoT.

The purpose of the pilot survey was to refine the instrument (questionnaire) to improve, at minimum, its face value and content value and to alert both the researcher and potential research participants of the time it would take to complete the survey (Saunders et al., 2019). This was achieved through this pilot study, and the instrument was considered to be ready for data collection.

4.9 Data Analysis Procedures

Data analysis procedures aid in understanding and summarising the data simply and meaningfully. In the data analysis phase similarities, differences and variability in the data were highlighted. Quantitative data analysis can be done using Smart PLS, SPSS, Statistica, or SAS tools. This research used Smart PLS 4 software to analyse the data. Smart PLS can be used to analyse data through Partial Least Square Structural Equation Modelling (PLS-SEM). PLS-SEM has been used in many studies; Hair et al. (2019) indicate that PLS-SEM use has increased in recent years compared to the Covariance-based Structural Equation Modelling (CB-SEM). They further note that PLS-SEM enables researchers to estimate models with many constructs and indicators. Since this study had high number of constructs and indicators (twelve independent and one dependent variable, with fifty-three indicators or items), PLS-SEM was suitable.

PLS-SEM analysis is done in two stages. The first step assesses the measurement model validity and reliability, good indicator loading, convergent validity, discriminant validity, variance inflation factor (VIF), outer weights, and outer loadings (Latif et al., 2021). The second step assesses the structural model using the coefficient of determination, goodness of fit, statistical significance and path coefficients (Hair et al., 2019).

Reliability measures the dependability of constructs to the extent that they would yield the same results if multiple tests were performed (Bhattacherjee, 2012). Of the many methods used to test the internal consistency of responses, Saunders et al. (2019) state that Cronbach’s alpha is most frequently used. Cronbach’s alpha measures internal consistency by calculating an alpha coefficient in the range from 0 to 1. A Cronbach alpha coefficient of .70 or above means that the measurements or items are measuring the same thing and indicates a high level of internal consistency (Fornell & Larcker, 1981). This study used Cronbach's alpha to test the reliability of the data.

Validity is sometimes referred to as construct validity. Validity tests the extent to which measurements adequately represent the underlying construct rather than another one. Several different validity tests can be done (namely, face validity, content validity, convergent validity, and discriminant validity) (Battacherjee, 2012). The underlying idea is to check whether the items are effectively measuring the construct they are meant to measure. Confirmatory factor analysis can be performed to test the validity of the construct. The study reported on here used convergent and discriminant validity to achieve this. In the convergent validity test, items belonging to the same construct are expected to have a loading factor of 0.60 or higher, and the discriminant validity is expected to have a loading factor of 0.3 or less. Other methods that can be used are the Fornell-Larcker Criterion and heterotrait-monotrait ratio of correlations (HTMT). The study only proceeded to the second stage of PLS-SEM analysis after the reliability and validity tests were met. Figure 4.2 summarises all the steps and tests carried out.

PLS-SEM Models Analysis Summary		
Measurement Model Assessment		
	Internal consistency reliability	
	Construct reliability assessment	
	Convergent validity assessment	
	Discriminant validity test	
		Cross-loadings
		Fornell-Larcker Criterion
		heterotrait-monotrait ratio of correlations (HTMT)
Structural Model Assessment		
	Coefficient of determination	
	Goodness of fit	
Hypotheses Testing and Direct Path Coefficients Analysis		

Figure 4.2: PLS-SEM Models Analysis Summary (after the fashion of Behardien, 2023)

4.10 Ethics and Confidentiality

The research followed the Ethics in Research Committee of the Faculty of Commerce rules and regulations. This committee gave its permission for the study to proceed.

The study used a survey to collect data from participants. Prolific Academic online platform was used to identify potential participants and the researcher had no direct contact with the selected participants other than to approve or reject the submitted response. The participants were anonymous and were only linked to the study through their Prolific ID. The Prolific ID was then passed to Qualtrics, where the participants took the survey.

The selected participants were notified of their voluntary participation and the right to withdraw from the study at any time. The researcher did not have access to the participants' personal information; their identities were preserved to ensure confidentiality and prevent bias. A consent form was presented to the participants before the start of the survey. As part of the consent form, a checkbox needed to be ticked to acknowledge that they understood and agreed to participate voluntarily in this research study.

The collected data will at no time be shared with a third party and will only be used to assess the adoption of IoT in organisations.

4.11 Research Methodology Summary

The researcher adopted objectivism as the research ontology and positivism as its epistemology. The study followed the deductive approach, known as theory testing, and employed a quantitative survey strategy. The study utilised the services of Academic Prolific Online Panel to source participants and used Qualtrics Online Platform to design the survey and collect responses. Two hundred and ninety-three (293) valid responses were considered for the analysis from a population of 1138, all of whom were IT professionals with a knowledge of IoT implementation in organisations.

This chapter discussed various considerations regarding data collection and analysis methods. The data analysis was done using Smart PLS4 and Partial Least Square Structural Equation Modelling was applied to the measurement model. This and included evaluating the reliability and validity of both the measurement model and the structural model. An outline of the assessments followed in Smart PLS is reported in Figure 4.2.

CHAPTER 5: FINDINGS AND DISCUSSIONS

5.1 Introduction

This research aimed to identify the artefactual characteristics that lead to the adoption of IoT as reflected by the continuance intention in organisations. In order to achieve this, a literature review was conducted to identify the technological characteristics related to IoT technology. From this, a survey instrument was developed and administered to an online panel of IT professionals and IoT Experts. This chapter will start by reviewing the demographic status of the online panel that participated in the survey. Assessments of the measurement model and the structural model follow. Thereafter the findings are presented and discussed.

5.2 Descriptive Statistics

The data was collected from participants in South Africa, the United Kingdom and the United States of America. These participants completed an online survey distributed by the Academic Prolific platform[5] hosted on Qualtrics[6]. The first part of the survey collected demographic information regarding the participants: gender, age, country of residence, education level, the position the participant occupied in his current organisation, number of years of experience in Information Technology, number of years of experience using or working with IoT. This section also collected data about the organisation where the participant was employed: the status of IoT adoption, the industry that organisation operated in, the number of employees, and the years of organisation existence.

Table 5.1 (Participant's demographic status) summarises the demographic information of the 293 participants (n = 293) who participated in the study. The first column indicates the demographic construct; the second has various categories for each construct; the third has the number of participants per category; and the last has the percentage.

[5] (https: //www.prolific.com/)
[6] https: //www.qualtrics.com/

The sample consisted of 293 participants, 230 (78.5%) of whom identified as male and 63 (21.5%) as female. These values reflect the valid percentage of participants within each category. There were no missing values.

The largest group of participants fell into the 25-34 age group (n = 132, 45.1%), followed by 35-44 years (n = 82, 28.0%), and 45-54 years (n = 36, 12.3%). Participants aged 18-24 represented 7.8% (n = 23) of the sample, while those 55 or older comprised 6.8% (n = 20).

Table 5.1: Participants' Demographic Status

	Category	**N**	**%**
Gender	Male	230	78.5
	Female	63	21.5
Age	18-24	23	7.8
	25-34	132	45.1
	35-44	82	28
	45-54	36	12.3
	55 or older	20	6.8
Country	SA	49	16.7
	UK	137	46.8
	USA	107	36.5
Education	Some college	5	1.7
	2 year degree (certification or diploma)	11	3.8
	4-year degree	183	62.5
	Professional degree	85	29
	Doctorate	9	3.1
Position/Job title	Application Engineer/Developer	92	31.4
	Chief Information Officer (CIO)	4	1.4
	Director	6	2
	IoT Specialist	3	1
	IT Specialist	121	41.3
	Manager	67	22.9
IT Experience	0-1 year	9	3.1
	2-3 years	43	14.7
	4-5 years	56	19.1
	6 years and above	185	63.1

	Category	N	%
IoT Experience	0-1 year	48	16.4
	2-3 years	110	37.5
	4-5 years	67	22.9
	6 years and above	68	23.2
IoT Adoption Status	No details provided	21	7.2
	Have not considered IoT yet	22	7.5
	Spoken informally about IoT	53	18.1
	Formally investigated IoT and currently running an IoT pilot	57	19.5
	Completed a pilot and will not be implementing IoT	8	2.7
	Have completed a pilot and planning to implement IoT	25	8.5
	Currently implementing IoT	107	36.5
Industry	No details provided	21	7.2
	Information Technology/Telecomms	175	59.7
	Financial Services	14	4.8
	Healthcare	13	4.4
	Manufacturing	9	3.1
	Engineering	33	11.3
	Retail	5	1.7
	Transport/Logistics	4	1.4
	Government	3	1
	Academic/Education	9	3.1
	Others	7	2.4
Organisation Age	No details provided	21	7.2
	Less than 1 year	2	0.7
	1-2 years	7	2.4
	3-5 years	17	5.8
	6-9 years	29	9.9
	10 years and above	217	74.1
Organisation Size	No details provided	25	8.5
	Fewer than 5	5	1.7
	5-50	36	12.3
	51-300	71	24.2
	Above 300	156	53.2

Participants were predominantly from the United Kingdom (n = 137, 46.8%), followed by the United States of America (n = 107, 36.5%) and South Africa (n = 49, 16.7%). This was influenced by the population found on Prolific, as the majority are from the United Kingdom and the United States of America.

Most participants held a 4-year degree (n = 183, 62.5%), followed by those with a professional degree (n = 85, 29.0%). A smaller portion of the participants had a 2-year college certification or diploma (n = 11, 3.8%), a doctorate (n = 9, 3.1%), or had completed some college training (n = 5, 1.7%). All the 293 participants were accounted for.

All 293 participants reported their positions or job titles within their organisations. The most common role was IT Specialist (n = 121, 41.3%), followed by Application Engineer/Developer (n = 92, 31.4%). Other positions recorded were Manager (n = 67, 22.9%), Director (n = 6, 2.0%), Chief Information Officer (CIO) (n = 4, 1.4%) and IoT Specialist (n = 3, 1.0%).

The participants' IT experience varied, with 63.1% (n = 185) reporting 6 years or more of experience, 19.1% (n = 56) reporting 4-5 years, 14.7% (n = 43) reporting 2-3 years, and only 3.1% (n = 9) reporting 0-1 year of experience.

Participants had varying levels of experience in IoT**.** The largest group reported having 2-3 years of IoT experience (n = 110, 37.5%), followed by those with 6 years or more of experience (n = 68, 23.2%) and 4-5 years of experience (n = 67, 22.9%). Few participants had only 0-1 year of IoT experience (n = 48, 16.4%). All participants were accounted for.

The participants' organisations operated in various industries, with a large majority in Information Technology/Telecommunications (n = 175, 59.7%). Other industries included Engineering (n = 33, 11.3%), Financial Services (n = 14, 4.8%), Healthcare (n = 13, 4.4%), Manufacturing (n = 9, 3.1%), and Academic/Education (n = 9, 3.1%). Additionally, 7.2% (n = 21) of participants did not specify their industry, and 2.4% (n = 7) were categorised as "Others". In the group who marked “Others”, at least one participant was from each of the following industries: Hospitality, Energy Utilities, Biotech, Wholesale, Entertainment, Housing Association.

Most of the organisations had been in business for 10 years or more (n = 217, 74.1%). A smaller group of organisations had been in business for 6-9 years (n = 29, 9.9%), followed by those in business for 3-5 years (n = 17, 5.8%), and 1-2 years (n = 7, 2.4%). Only two (2) organisations (0.7%) had been operating for less than 1 year. Additionally, 21 participants (7.2%) did not specify the age of their organisation.

Participants' organisations varied in size. Most organisations had more than 300 employees (n = 156, 53.2%), while 24.2% (n = 71) had 51-300 employees. Additionally, 12.3% (n = 36) had 5-50 employees, and 1.7% (n = 5) participants reported working in organisations with fewer than 5 employees. A total of 8.5% (n = 25) did not specify the size of their organisation.

Regarding IoT adoption status, 36.5% (n = 107) of organisations were implementing IoT when the survey was done, while 19.5% (n = 57) were running an IoT pilot project. An additional 18.1% (n = 53) had spoken informally about IoT, and 8.5% (n = 25) had completed a pilot project and were planning to implement IoT. A small percentage had either not considered IoT yet (n = 22, 7.5%) or had completed a pilot project but decided not to implement IoT (n = 8, 2.7%). Lastly, 7.2% (n = 21) of participants did not provide details on their organisations' IoT adoption status.

In summary, most participants were male (78.5%), 45.1% were aged 25-34, predominantly from the United Kingdom (46.8%), 62.5% held a 4-year degree, 41.3% were Information Technology Specialists, 63.1% had more than 6 years' experience in Information Technology, and 37.5% had 2-3 years IoT experience. 59.7% of participants worked in the Information Technology/ Telecoms industry. 74.1% of their organisations had been in business for 10 years or more, and 53.2% of the participants said that their organisations employed 300 or more workers. The profiled participants had adequate knowledge and experience to answer questions about adopting IoT in their organisations.

5.3 Measurement Model Assessment Findings

The measurement or outer model assessment evaluates the reliability of the constructs and their indicators or items. As indicated in the guidelines provided by Hair et al. (2019), this is the first step in data analysis. This assessment begins by evaluating indicator loadings, which are recommended to be above 0.708 and, for exploratory studies, above 0.60. These guidelines vary based on the context and the availability of the data. An indicator loading of 0.708 means that the construct explains at least 50 per cent of the items' variance.

The second step in the measurement model assessment is to assess the reliability of internal consistency. Hair et al. (2019) say that two measures can be used to assess internal consistency reliability, namely composite reliability (CR) and Cronbach's alpha. Composite reliability values between 0.60 and 0.70 are considered acceptable for exploratory studies, and 0.70 to 0.90 are considered satisfactory to good. Anything above 0.90 can be problematic.

Once the internal consistency is established, the construct's convergent validity must be measured. In this third step, the convergent validity measures "the extent to which construct converges to explain the variance of its items" (Hair et al., 2019, p. 9). This can be done by using the average variance extracted (AVE). It is recommended that AVE should be 0.50 or above.

The final and fourth step in the measurement model assessment measures the discriminant validity of the constructs. During this stage the study evaluates how different or distinct constructs are from each other. This can be determined using three measures, namely Cross-loading, Fornell-Larcker Criterion or heterotrait-monotrait (HTMT).

Table 5.2 contains the results of the Item Loadings, Reliability and Convergent Validity. The codes assigned to each item are easily linked to the code assigned to the construct with which they are associated. The results will be discussed according to the steps described above, that is, indicator reliability, reliability of internal consistency and convergent validity. Finally, the measurement model assessment measures discriminant validity.

Table 5.2: Item Loadings, Reliability and Convergent Validity

Item	**Construct**	**Λ**	**α**	**CR**	**AVE**
	Scalability (SCA)		0.71	0.71	0.54
SCA01		0.73			
SCA03		0.71			
SCA04		0.77			
SCA05		0.73			
	Compatibility (CMPA)		0.65	0.74	0.58
CMPA01		0.86			
CMPA02		0.58			
CMPA03		0.82			

Item	Construct	Λ	α	CR	AVE
	Complexity (CMPX)		0.61	0.62	0.55
CMPX01		0.68			
CMPX02		0.77			
CMPX04		0.78			
	Connectivity (CON)		0.75	0.76	0.67
CON01		0.80			
CON03		0.81			
CON04		0.85			
	Interactivity (INTA)		0.76	0.77	0.68
INTA01		0.83			
INTA02		0.83			
INTA04		0.81			
	Integration (INTG)		0.75	0.76	0.57
INTG01		0.78			
INTG02		0.70			
INTG03		0.77			
INTG05		0.78			
	Interoperability (INTO)		0.63	0.63	0.57
INTO01		0.73			
INTO02		0.79			
INTO03		0.75			
	Organisation Adoption (OADP)		0.81	0.81	0.73
OADP01		0.86			
OADP02		0.87			
OADP03		0.82			
	Relative Advantage (RA)		0.82	0.82	0.58
RA01		0.70			
RA02		0.73			
RA03		0.83			
RA04		0.74			
RA06		0.79			
	Self-Adaptation (SAD)		0.79	0.79	0.70
SAD01		0.83			
SAD02		0.88			
SAD03		0.81			

Item	Construct	Λ	α	CR	AVE
	Security (SEC)		0.83	0.84	0.60
SEC01		0.83			
SEC02		0.84			
SEC03		0.70			
SEC04		0.78			
SEC05		0.72			
	State (STA)		0.72	0.73	0.54
STA01		0.79			
STA02		0.69			
STA03		0.66			
STA04		0.80			
	Synchronicity (SYNC)		0.81	0.81	0.72
SYNC01		0.85			
SYNC02		0.85			
SYNC03		0.85			

5.3.1 Item Loadings

The items loadings reliability test was done using Smart PLS 4 bootstrapping. It was important to achieve the minimum loading of 0.50 and the desired loading of 0.70 or above (Latif et al., 2020). The study first looked at the outer loading results (see column 3 labelled **Λ** in Table 5.2). Eight items out of fifty-three were removed to achieve the desired 0.70. These were SCA02, CMPX03, CMPX05, CON02, INTA03, INTG04, RA05, SYNC04. Although it is always desirable to have item loadings above 0.70, Hair et al. (2019) state that often researchers do not reach it, and these authors recommend that items that do not meet the minimum acceptable factor loading of 0.50 should only be removed after checking their impact on the composite reliability and average variance extracted. One Compatibility item (CMPA02) did not meet the desired factor loading of 0.70, but was kept after checking its impact on the AVE and composite reliability (CR), which were 0.58 and 0.78, respectively (see columns 5 and 6 in Table 5.2). Three other items loaded also under 0.70; these were STA03 (0.66), CMPX01 (0.68), and STA02 (0.69). The remaining items loaded at 0.70 or higher with the highest being 0.88. The factor loadings of the retained items were satisfactory, and items deemed reliable.

5.3.2 Construct Reliability

The construct reliability (CR) was assessed using Cronbach's alpha, composite reliability (rho_a) and AVE. The CR for all constructs was between Cronbach's alpha and AVE, as seen in Table 5.2. AVE for all constructs was above 0.5, and Cronbach's alpha was above the acceptable level of 0.6, as Hair et al. (2019) guidelines recommend. The Complexity and Interoperability constructs had an acceptable CR of 0.63 and 0.62, while the rest had a good or satisfactory CR above 0.70, with the highest being Security at 0.84 (Hair et al., 2019). All the constructs were retained, indicating high internal consistency (Fornell & Larcker, 1981).

5.3.3 Construct Validity

Construct validity was tested through convergent and discriminant validity. Fornell and Larcker (1981) advise that convergent validity can be established by looking at the AVE value. They recommend a value of 0.50 and higher for convergent validity to be achieved. All AVE values in Table 5.2 indicate that convergent validity was established and demonstrate the appropriateness of items to their constructs (Bhattacherjee, 2012).

The second test of construct validity done was the discriminant validity test. Discriminant validity evaluates how different or distinct the constructs are from each other. Three measures were used to establish how distinct the constructs were: Cross-loading, Fornell-Larcker criterion, and heterotrait-monotrait ratio of correlations (HTMT).

The cross-loadings in Table 5.3 report that every item loaded higher on their own construct than on their cross-loading; this demonstrates that the indicators (individual questions or items) of each individual construct had a low correlation to the indicators of other constructs' discriminants (Bhattacherjee, 2012).

Discriminant validity can also be established using the Fornell-Larcker criterion. According to Fornell and Larcker (1981), discriminant validity is present when the construct's squared root correlation value is higher than the inter-correlations of other constructs. Table 5.4 shows the results of the Fornell-Lacker test. The AVE of each construct was higher than the highest squared correlation with any other construct (Hair et al., 2019), showing that discriminant validity was established.

Table 5.3: Cross-loadings

	SCA	CMPA	CMPX	CONN	INTA	INTG	INTO	OADP	RA	SAD	SEC	STA	SYNC
SCA01	0.73	0.36	-0.23	0.50	0.41	0.51	0.48	0.44	0.48	0.47	0.43	0.49	0.44
SCA03	0.71	0.41	-0.14	0.45	0.44	0.46	0.45	0.38	0.51	0.40	0.39	0.51	0.47
SCA04	0.77	0.39	-0.21	0.50	0.47	0.56	0.49	0.43	0.53	0.48	0.40	0.51	0.50
SCA05	0.73	0.46	-0.19	0.53	0.48	0.52	0.51	0.39	0.46	0.48	0.48	0.54	0.50
CMPA01	0.54	0.86	-0.36	0.61	0.61	0.62	0.59	0.72	0.64	0.64	0.57	0.58	0.60
CMPA02	0.23	**0.58**	-0.09	0.29	0.26	0.15	0.27	0.29	0.25	0.35	0.31	0.22	0.37
CMPA03	0.41	0.82	-0.26	0.54	0.45	0.48	0.50	0.55	0.51	0.55	0.51	0.42	0.48
CMPX01	-0.18	-0.17	0.68	-0.22	-0.14	-0.22	-0.15	-0.15	-0.23	-0.16	-0.19	-0.14	-0.23
CMPX02	-0.21	-0.30	0.77	-0.34	-0.20	-0.25	-0.29	-0.26	-0.26	-0.27	-0.28	-0.25	-0.27
CMPX04	-0.20	-0.27	0.78	-0.31	-0.24	-0.28	-0.22	-0.25	-0.33	-0.28	-0.29	-0.25	-0.32
CON01	0.49	0.53	-0.31	0.80	0.59	0.52	0.56	0.49	0.46	0.54	0.59	0.55	0.56
CON03	0.59	0.46	-0.32	0.81	0.55	0.60	0.55	0.53	0.53	0.62	0.54	0.57	0.67
CON04	0.58	0.63	-0.35	0.85	0.65	0.65	0.62	0.60	0.63	0.67	0.61	0.66	0.66
INTA01	0.52	0.52	-0.18	0.64	0.83	0.56	0.57	0.49	0.56	0.58	0.54	0.59	0.59
INTA02	0.50	0.50	-0.25	0.58	0.83	0.56	0.53	0.52	0.51	0.53	0.49	0.54	0.55
INTA04	0.50	0.51	-0.22	0.59	0.81	0.53	0.53	0.50	0.55	0.58	0.46	0.58	0.59
INTG01	0.56	0.48	-0.27	0.60	0.50	0.78	0.60	0.52	0.65	0.59	0.45	0.50	0.53
INTG02	0.51	0.39	-0.20	0.46	0.43	0.70	0.42	0.44	0.50	0.46	0.38	0.44	0.45
INTG03	0.48	0.43	-0.25	0.53	0.54	0.77	0.51	0.51	0.54	0.47	0.38	0.51	0.46
INTG05	0.58	0.53	-0.30	0.60	0.53	0.78	0.56	0.58	0.57	0.58	0.51	0.57	0.56
INTO01	0.48	0.51	-0.09	0.50	0.50	0.47	0.73	0.40	0.45	0.51	0.46	0.44	0.47
INTO02	0.50	0.50	-0.28	0.51	0.49	0.52	0.79	0.43	0.50	0.51	0.41	0.48	0.49
INTO03	0.53	0.43	-0.32	0.59	0.51	0.58	0.75	0.46	0.53	0.49	0.49	0.57	0.56
OADP01	0.45	0.59	-0.23	0.51	0.48	0.53	0.42	0.86	0.54	0.57	0.44	0.43	0.45
OADP02	0.46	0.67	-0.28	0.59	0.51	0.59	0.46	0.87	0.56	0.61	0.47	0.49	0.51
OADP03	0.52	0.62	-0.28	0.59	0.56	0.60	0.57	0.82	0.61	0.61	0.55	0.49	0.57
RA01	0.46	0.44	-0.25	0.50	0.46	0.47	0.46	0.49	0.70	0.49	0.41	0.42	0.52

	SCA	CMPA	CMPX	CONN	INTA	INTG	INTO	OADP	RA	SAD	SEC	STA	SYNC
RA02	0.53	0.50	-0.22	0.47	0.50	0.56	0.46	0.49	0.73	0.52	0.39	0.48	0.54
RA03	0.57	0.59	-0.34	0.56	0.56	0.63	0.58	0.57	0.83	0.57	0.48	0.59	0.56
RA04	0.51	0.47	-0.26	0.45	0.45	0.53	0.48	0.44	0.74	0.50	0.47	0.47	0.48
RA06	0.51	0.50	-0.31	0.54	0.51	0.64	0.51	0.55	0.79	0.56	0.47	0.49	0.56
SAD01	0.46	0.57	-0.27	0.59	0.55	0.53	0.52	0.57	0.53	0.83	0.55	0.54	0.53
SAD02	0.57	0.59	-0.28	0.66	0.55	0.62	0.58	0.61	0.58	0.88	0.58	0.57	0.66
SAD03	0.53	0.60	-0.27	0.62	0.63	0.59	0.57	0.58	0.64	0.81	0.56	0.60	0.63
SEC01	0.48	0.52	-0.33	0.59	0.43	0.48	0.52	0.44	0.46	0.55	0.83	0.47	0.50
SEC02	0.47	0.49	-0.25	0.56	0.45	0.46	0.47	0.48	0.45	0.54	0.84	0.49	0.47
SEC03	0.39	0.49	-0.27	0.52	0.46	0.40	0.38	0.41	0.40	0.48	0.70	0.44	0.46
SEC04	0.36	0.46	-0.27	0.49	0.42	0.36	0.42	0.43	0.40	0.50	0.78	0.43	0.46
SEC05	0.53	0.47	-0.26	0.58	0.55	0.50	0.53	0.45	0.55	0.55	0.72	0.56	0.56
STA01	0.47	0.47	-0.22	0.56	0.53	0.46	0.50	0.42	0.50	0.53	0.51	0.79	0.51
STA02	0.48	0.42	-0.19	0.50	0.45	0.43	0.51	0.37	0.38	0.49	0.45	0.69	0.48
STA03	0.54	0.36	-0.30	0.53	0.48	0.53	0.45	0.38	0.48	0.43	0.41	0.66	0.46
STA04	0.55	0.44	-0.20	0.56	0.56	0.55	0.48	0.47	0.53	0.55	0.44	0.80	0.52
SYNC01	0.57	0.52	-0.33	0.62	0.61	0.59	0.55	0.52	0.63	0.63	0.53	0.56	0.85
SYNC02	0.55	0.53	-0.33	0.70	0.60	0.56	0.57	0.50	0.60	0.61	0.55	0.60	0.85
SYNC03	0.54	0.60	-0.28	0.66	0.58	0.54	0.59	0.53	0.55	0.62	0.53	0.54	0.85

Table 5.4: Fornell and Larcker

	SCA	CMPA	CMPX	CONN	INTA	INTG	INTO	OADP	RA	SAD	SEC	STA	SYNC
SCA	0.73												
CMPA	0.55	0.76											
CMPX	-0.27	-0.34	0.74										
CONN	0.68	0.67	-0.40	0.82									
INTA	0.61	0.62	-0.27	0.73	0.82								
INTG	0.70	0.61	-0.34	0.73	0.66	0.76							
INTO	0.66	0.63	-0.31	0.70	0.66	0.70	0.76						
OADP	0.56	0.74	-0.31	0.66	0.61	0.68	0.57	0.85					
RA	0.68	0.66	-0.37	0.67	0.66	0.75	0.66	0.67	0.76				
SAD	0.62	0.70	-0.33	0.75	0.69	0.70	0.67	0.70	0.70	0.84			
SEC	0.58	0.63	-0.36	0.71	0.60	0.57	0.60	0.57	0.58	0.68	0.78		
STA	0.69	0.58	-0.30	0.73	0.69	0.67	0.66	0.56	0.65	0.68	0.62	0.74	
SYNC	0.65	0.65	-0.37	0.78	0.70	0.66	0.67	0.61	0.70	0.73	0.63	0.67	0.85

Table 5.5: Heterotrait-Monotrait

	SCA	CMPA	CMPX	CONN	INTA	INTG	INTO	OADP	RA	SAD	SEC	STA	SYNC
SCA													
CMPA	0.76												
CMPX	0.40	0.46											
CONN	**0.92**	0.89	0.57										
INTA	0.83	0.81	0.38	**0.96**									
INTG	**0.96**	0.77	0.49	**0.95**	0.87								
INTO	**0.99**	**0.92**	0.46	**1.02**	**0.95**	**1.00**							
OADP	0.73	**0.92**	0.42	0.84	0.77	0.86	0.79						
RA	0.89	0.83	0.51	0.84	0.83	**0.95**	**0.91**	0.82					
SAD	0.83	**0.93**	0.46	**0.96**	0.89	0.90	**0.95**	0.87	0.87				
SEC	0.75	0.81	0.49	0.90	0.75	0.72	0.82	0.69	0.71	0.84			
STA	**0.98**	0.77	0.45	**0.99**	**0.93**	0.91	**0.99**	0.73	0.84	**0.91**	0.80		
SYNC	0.86	0.86	0.52	**0.99**	0.89	0.85	**0.94**	0.74	0.86	**0.91**	0.77	0.88	

The last method used to test discriminant validity was the heterotrait-monotrait ratio of correlations. HTMT is "the mean value of the item correlations across constructs relative to the (geometric) mean of the average correlations for the items measuring the same construct" (Hair et al., 2019, p.9). Hair et al. (2019) suggest a threshold value of 0.90 for constructs that are similar and 0.85 for constructs that are conceptually different; values above 0.90 show a lack of discriminant validity. The results of the HTMT test, shown in Table 5.5, indicated discriminant validity problems for the values highlighted in red.

Ab Hamid et al. (2017) state that HTMT should be used in assessing discriminant validity because of its high density when compared to cross-loading and the Fornell-Larcker criterion. However, they also say that the study's researchers' view on how conservative they want the HTMT to be in their assessment should be considered.

The outer model assesses the relationship between the items and their constructs (Hair et al., 2019; Ab Hamid et al., 2017), and in the results of the current study the results were satisfactory, except for the test of discriminant validity obtained when using HTMT. Since discriminant validity was established through cross-loading and the Fornell-Larcker criterion (as recommended by Latif et al., 2020), overall validity was deemed adequate.

5.3.4 The Constructs' Descriptive Statistics

The descriptive statistics for each construct are presented in Table 5.6 which shows the sample Mean, Median, Standard Deviation, Excess Kurtosis, Skewness and participant Count. This section will briefly review the descriptive statistics of each construct.

Intention to Adopt IoT as reflected by the continuance intention (OADP), the dependent variable, was assessed using three items. The descriptive statistics (see Table 5.6) for this variable indicated that the participants reported a particularly strong intention to continue using IoT systems (M = 4.06, SD = 0.99), followed by using IoT regularly in the future (M = 3.97, SD = 1.09) and recommending IoT adoption to other firms (M = 3.96, SD = 1.04). All three items exhibited negative skewness (a range of -0.83 to -0.97), indicating a tendency for responses to cluster toward higher agreement levels. Kurtosis values ranged from -0.16 to 0.50, suggesting relatively normal distributions. Overall, organisations appeared to be favourably disposed toward IoT adoption as reflected by the continuance intention.

Table 5.6: Constructs Descriptive Statistics

	Mean		Median	SD	Excess kurtosis	Skewness	Count
SCA01	4.083	4.218	4.000	0.801	0.416	-0.896	293
SCA03		3.959	4.000	0.873	0.918	-0.878	293
SCA04		4.065	4.000	0.822	0.918	-0.863	293
SCA05		4.089	4.000	0.882	0.307	-0.865	293
CMPA01	3.649	4.041	4.000	0.991	0.903	-1.078	293
CMPA02		3.253	3.000	1.135	-0.832	-0.269	293
CMPA03		3.652	4.000	1.112	-0.489	-0.611	293
CMPX01	2.616	2.867	3.000	1.242	-1.092	0.104	293
CMPX02		2.427	2.000	1.159	-0.584	0.582	293
CMPX04		2.553	2.000	1.166	-0.788	0.41	293
CON01	4.076	4.024	4.000	0.91	0.03	-0.729	293
CON03		4.089	4.000	0.821	1.200	-0.909	293
CON04		4.116	4.000	0.843	0.905	-0.945	293
INTA01	4.068	4.068	4.000	0.936	0.445	-0.94	293
INTA02		4.126	4.000	0.863	0.746	-0.951	293
INTA04		4.010	4.000	0.929	0.251	-0.816	293
INTG01	4.116	4.119	4.000	0.88	1.067	-1.052	293
INTG02		4.177	4.000	0.785	1.199	-0.919	293
INTG03		4.113	4.000	0.825	1.063	-0.946	293
INTG05		4.055	4.000	0.849	0.846	-0.912	293
RA01	4.092	4.123	4.000	0.854	1.025	-0.966	293
RA02		4.044	4.000	0.851	0.248	-0.685	293
RA03		4.109	4.000	0.917	0.288	-0.859	293
RA04		3.928	4.000	0.934	0.232	-0.741	293
RA06		4.256	4.000	0.752	1.771	-1.042	293
SEC01	3.932	3.969	4.000	0.982	0.148	-0.85	293
SEC02		4.041	4.000	1.004	0.55	-0.997	293
SEC03		3.877	4.000	1.013	-0.079	-0.704	293
SEC04		3.771	4.000	1.054	-0.485	-0.551	293
SEC05		4.000	4.000	0.96	0.281	-0.861	293
SAD01	4.093	4.113	4.000	0.833	1.426	-1.034	293
SAD02		4.106	4.000	0.905	0.73	-0.989	293
SAD03		4.061	4.000	0.951	0.733	-1.009	293

	Mean		Median	SD	Excess kurtosis	Skewness	Count
STA01	4.105	4.020	4.000	0.963	0.267	-0.87	293
STA02		4.229	4.000	0.747	1.478	-0.992	293
STA03		4.205	4.000	0.792	1.502	-1.046	293
STA04		3.966	4.000	0.897	0.424	-0.789	293
SYNC01	4.065	4.143	4.000	0.73	0.517	-0.6	293
SYNC02		4.133	4.000	0.761	0.571	-0.696	293
SYNC03		3.918	4.000	0.909	0.016	-0.605	293
INTO01	3.926	3.638	4.000	1.005	-0.38	-0.485	293
INTO02		3.942	4.000	0.924	1.147	-1.007	293
INTO03		4.198	4.000	0.785	0.457	-0.791	293
OADP01	4.045	4.058	4.000	0.988	0.498	-0.971	293
OADP02		3.969	4.000	1.091	-0.157	-0.827	293
OADP03		3.956	4.000	1.039	0.045	-0.828	293

Considering the mean and standard deviation of the three items used to assess the **Compatibility (CMPA)** construct, the participants generally agreed that IoT systems align well with their organisation's current operations (M = 4.04, SD = 0.99), indicating a favourable view of compatibility. The participants agreed moderately, with some variability, with the statement “IoT systems would not require many business processes changes in my organisation” (M = 3.25, SD = 1.14). This suggests that, while participants see some compatibility, there may be concerns that adopting IoT could require changes in their business processes, and this led to the wider variety of perceptions. The statement "IoT systems would be compatible with all aspects of work in my organisation" (M = 3.65, SD = 1.11), received a favourable response, as indicated by a moderately high mean, but perhaps with some reservations about full compatibility with all aspects of work.

The descriptive statistics for the **Complexity (CMPX)** construct were examined using three items. Participants generally disagreed with the statements related to complexity, with all mean scores below the midpoint of the 5-point Likert scale. The item "It would not be easy to get IoT systems to do what the organisation wants them to do" had the highest mean score (M = 2.87, SD = 1.24), suggesting this was the most significant complexity-related challenge. "Interacting with IoT systems would be difficult" received the lowest mean score (M = 2.43, SD = 1.16), indicating that this aspect was not perceived as a major difficulty. The item "It would take too much time for IT staff if they want to use IoT systems to do their normal duties" had a mean score of 2.55 (SD = 1.17).

The three **Connectivity (CON)** construct items considered by the participants had mean scores ranging from 4.02 to 4.12. This indicates a generally high perception of IoT connectivity quality, with stable, responsive and seamless data flow perceived as beneficial features. It also expresses the participants' confidence in IoT artefact connectivity. The item "IoT systems would have stable connectivity" had a mean score of 4.02 (SD = 0.91), indicating agreement that IoT systems provide reliable connectivity. The item "IoT systems connectivity would quickly respond to input" had the second-highest mean score (M = 4.09, SD = 0.82), suggesting that IoT responsiveness was viewed positively. The item "IoT systems connectivity would allow a seamless flow of data" was rated the highest (M = 4.12, SD = 0.84), reflecting pronounced agreement that IoT systems facilitate smooth data transfer. Overall, the results demonstrate that organisations perceive connectivity as a key strength of IoT, with particularly high confidence in its ability to facilitate seamless data flow and quick responsiveness.

Scalability (SCA) was measured with four items. The descriptive statistics findings highlight that knowledgeable employees in organizations perceive IoT systems to be scalable and adaptable, particularly in their ability to handle changes in device numbers and to support multi-service assignments. Standard deviations ranged from 0.80 to 0.88, indicating relatively low variability and a consensus among participants. The item "IoT system capacity can be scaled to handle increasing or decreasing numbers of connected devices" received the highest mean score (M = 4.22, SD = 0.80), suggesting strong confidence in IoT scalability. The item "IoT system devices can be reallocated from one service to another" had the lowest mean score (M = 3.96, SD = 0.88), though it still indicated substantial agreement among participants. The item "Once an IoT system device is set up for one geographical area, it is easy to reuse it to expand to other geographical areas" showed a mean score of M = 4.06, SD = 0.82, reflecting positive perceptions of scalability across geographical areas.

The descriptive statistics for the items assessing the **Relative Advantage (RA)** of IoT systems in influencing organizational adoption and continuation intention are also in Table 5.6. These items evaluated the perceived benefits of IoT systems in terms of cost efficiency, inventory management, customer service, marketing strategies, asset tracking, and overall productivity.

The results show high mean scores ranging from 3.93 to 4.26, indicating a generally positive perception of IoT's relative advantage in efficiency, service improvement and productivity, with business productivity receiving the highest endorsement. Standard deviations were moderate (0.75 to 0.94), showing some response variability, particularly for items related to customer service and competitive marketing strategies.

The descriptive statistics for the items measuring the impact of **Integration (INTG)** on organisational adoption of IoT reported high mean scores across all items (ranging from 4.05 to 4.18 on a 5-point scale), This suggests that participants largely agreed that IoT systems offer strong integration capabilities, such as combining data from different areas and connecting with existing systems. This indicates that integration is perceived as an important and even essential advantage of IoT in an organisational context, possibly reflecting the expectation that IoT can improve operational efficiencies by streamlining data flow and connectivity across departments and systems. The relatively low standard deviations (ranging from 0.787 to 0.881) indicate that responses were consistent, with participants agreeing on the positive role of IoT integration. This consistency suggests a consensus among participants about the benefits of IoT systems in terms of integration, possibly due to common experiences with IoT technology or shared organisational needs for interconnected data systems.

Interactivity (INTA) was measured using three items, and indicated that IoT systems are widely perceived as being interactive and having strong capabilities for two-way and concurrent communication (M = 4.07, SD = 0.937). The participants assigned the highest level of agreement when asked about the IoT systems' ability to enable concurrent communication (M = 4.13, SD = 0.865), suggesting that it might be a particularly valued aspect of IoT interactivity. These findings reinforce the importance of interactive IoT systems.

The descriptive statistics for the **State (STA)** construct show participants' strong agreement with the usefulness of state-related capabilities in IoT systems, particularly regarding their ability to provide sufficient state information (M = 4.23) and trace system actions (M = 4.20). The slightly lower mean for remembering previously performed events (M = 3.97) indicates slightly less agreement. Negative skewness across all items suggests that most responses were toward the high end of the Likert scale, reflecting favourable perceptions of these features.

The descriptive statistics analysis of the **Security (SEC)** construct's items revealed that participants generally believed IoT systems were able to transmit data securely (M = 3.97, SD = 0.982). The participants also showed confidence in the ability of IoT systems to deliver security patches or updates to remote devices. The participants' mean scores for cybersecurity protection and physical security of devices (respectively 3.77 and 3.88) were the lowest for this construct. The participants were relatively less confident regarding these two aspects of IoT security and were not in total agreement with one another (as seen in the moderately high standard deviations - 1.013 and 1.054).

All three **Self-adaptation (SAD)** items, namely, competent, sensible and intelligent operation, had high mean scores (above 4.00) indicating strong positive perceptions of IoT systems' self-adaptation capabilities. The moderate skewness toward high values and slightly peaked kurtosis in each item suggest that most participants agree with the self-adaptation capabilities of IoT systems. This consistency and positive outlook imply that participants view IoT self-adaptation as an essential and beneficial characteristic, potentially making IoT systems more desirable for organisational use.

The descriptive statistics results of **Synchronicity (SYNC)** indicate that participants believe that IoT systems respond quickly or immediately to requests, a key feature for real-time applications in organisational contexts. This is seen in the high means of all three items (all were equal to or greater than 3.92). There was consensus among participants on this (standard deviation of 0.731 and 0.761) and only slight variability (standard deviation of 0.910).

The descriptive statistics of the **Interoperability (INTO)** construct show that participants moderately agree that IoT systems would interoperate regardless of the underlying communication protocols (M=3.64, SD=1.006, Skewness = -0.485). They agreed to a greater extent on the aspects of interoperability related to data consistency regardless of the devices and platforms involved (M =3.94, SD=0.925, Skewness =0.142). Participants strongly agreed on the advisability of using well-defined APIs to allow diverse devices and applications to interact (M=4.20, SD=0.786, Skewness=-0.791).

In summary, the descriptive statistics results highlight that the participants had favourable perceptions of IoT systems across most constructs, with slightly more variability in Compatibility (SD range from 0.99 to 1.13), Complexity (SD range from 1.16 to 1.24), and

Security (ranged from 0.96 to 1.05). These three constructs had higher standard deviations than the others, implying that these aspects of IoT systems are subject to different interpretations based on participants' experiences or contexts.

5.4 Structural Model Assessment Findings

The structural model, also called the inner model, assesses the relationships between constructs using the coefficient of determination, statistical significance and path coefficients (Hair et al., 2019). In this section, the findings on the relationships between the dependent variable Intention to Adopt IoT as reflected by the continuance intention (OADP) and each of the independent variables (Scalability (SCA), Compatibility (CMPA), Complexity (CMPX), Connectivity (CON), Integration (INTG), Interactivity (INTA), Interoperability (INTO), Relative Advantage (RA), Security (SEC), Self-adaptation (SAD), State (STA) and Synchronicity (SYN)) are presented. This assessment enables the study to answer the research questions and test the hypotheses. According to Hair et al. (2019), assessment criteria for the inner model should include, but not be limited to, the coefficient of determination (R^2) and the relevance of the path coefficient.

5.4.1 The Coefficient of Determination (R^2)

The coefficient of determination (R^2) determines the strength of the relationship between two variables (Saunders et al., 2019). R^2 values range from 0 to 1, with 0 indicating the predictor or independent variable cannot explain or predict the variation in the dependent variable at all, 0.5 the predictor can only explain 50% of the variation or change in the dependent variable, and finally, the value of 1 indicating the independent variable is a perfect predictor (Saunders et al., 2019). R^2 values less than 0.190 are considered weak, between 0.333 and 0.70 moderate, and greater than 0.70 to have very good predictive accuracy (Hair et al., 2019).

The coefficient of determination was assessed using SmartPLS bootstrapping with a sample value of 5000, two tails and a confidence level of 95%. The results of this assessment are shown in Table 5.7 (coefficient of determination results) and include the coefficient of determination (R^2), T-statistics and P-Value (p).

Table 5.7: Coefficient of Determination Results

Dependent Variable	R^2	Adjusted R^2	T-statistics	P-Value
Intention to Adopt IoT as reflected by the Continuance Intention (OADP)	0.656	0.641	18.758	0.000

Results show that overall, the model had good predictive accuracy, as shown by the R^2 value of 0.656 and adjusted R^2 of 0.641, which is considered moderate and acceptable (Hair et al., 2019). The model was, therefore, a good predictor of IoT adoption as reflected by the continuance intention in organisations. This means this model explained more than 65% of the dependent variables' variance. The probability of these results being achieved by chance was less than 0.05, making the results statistically significant at $p < 0.05$. The inner model is, therefore, valid.

5.4.2 The Model's Goodness-of-Fit

The goodness-of-fit measures how well the model fits the data; it quantifies "the divergence between the observed and the estimated covariance matrices" (Hair et al., 2019, pp. 7). Many methods are used to assess goodness-of-fitness; in PLS_SEM, the Standardized Root Mean Square Residual (SRMR) is used. Table 5.8 shows the results of the goodness-of-fitness test done in SmartPLS through bootstrapping. The results indicate that the model fit indices for the saturated and estimated models were consistent.

Table 5.8: Goodness-of-fitness SRMR Results

SRMR Test	Original sample (O)	Sample mean (M)	95%	99%
Saturated model	0.062	0.046	0.051	0.053
Estimated model	0.062	0.046	0.051	0.053

The observed value in the results for the saturated and estimated models was 0.062. Hair et al. (2019) propose a threshold of 0.08 below which there is an acceptable fit. The model fit indices obtained in the study suggest that the model is well-calibrated with minimal deviation between the observed and predicted values, and the model fits the data.

5.5 Hypotheses Testing

The present study also examined the relationships between the twelve identified characteristics of IoT artefacts given by the constructs Scalability, Compatibility, Complexity, Connectivity, Integration, Interactivity, Interoperability, Relative Advantage, Security, Self-Adaptation, State, and Synchronicity, and the single dependent construct, Intention to Adopt IoT as reflected by the continuance intention in organisations. The significance of these relationships and estimate standards errors were evaluated through SmartPLS bootstrapping with 5000 resamples.

Table 5.9 shows the hypotheses testing results and the significance of the direct paths. Four of the twelve hypotheses were confirmed. The results show that Compatibility, Integration, Relative Advantage and Self-Adaptation were significant factors positively influencing the adoption as reflected by the continuance intention of IoT in organisations. However, other constructs, including Scalability, Complexity and Security, did not impact adoption significantly. Hence, these findings suggest that organisations are more likely to adopt IoT technology when they perceive it as compatible with existing systems, easy to integrate, advantageous and self-adaptive.

Table 5.9: Path Coefficients

	Relationship	Path Coefficient	SD	T-Values	P-value	Decision
H1	CMPA -> OADP	0.393	0.052	7.634	0.000	Supported
H2	CMPX -> OADP	0.009	0.037	0.234	0.815	Not Supported
H3	CONN -> OADP	0.124	0.074	1.675	0.095	Not Supported
H4	SCA -> OADP	-0.002	0.062	0.027	0.979	Not Supported
H5	RA -> OADP	0.135	0.065	2.086	0.037	Supported
H6	INTG -> OADP	0.230	0.079	2.933	0.004	Supported
H7	INTA -> OADP	0.049	0.066	0.742	0.459	Not Supported
H8	STA -> OADP	-0.064	0.070	0.922	0.357	Not Supported
H9	SEC -> OADP	0.002	0.053	0.029	0.977	Not Supported
H10	SAD -> OADP	0.197	0.071	2.761	0.006	Supported
H11	SYNC -> OADP	-0.065	0.061	1.052	0.293	Not Supported
H12	INTO -> OADP	-0.092	0.063	1.450	0.148	Not Supported

The path coefficient value is interpreted based on thresholds to determine its strength or significance. The path coefficient values range from -1 to +1, with values closer to -1 signalling a strong negative relationship and values close to +1 indicating a strong positive relationship (Hair et al., 2019). However, the path coefficient (β) alone is insufficient to assess the hypotheses. Roky and Al Meriouh (2015) stress that the T-value also needs to be greater than 1.95. These same authors give the thresholds for T-value and significance: at 10%, the T-value should be greater than or equal to 1.64, at 5% risk error significance, the T-value must be greater than 1.95; at 1% risk error significance, the T-value has to be greater than 2.56; and at 0.1% risk error significance needs to have a T-value equal to or greater than 3.29.

The following sections discuss each hypothesis individually, before proceeding to recommendations. In assessing the constructs' relationships with organisational adoption, we considered how each relates to the business in terms of functionality, business fit and infrastructure.

5.5.1 Compatibility

Compatibility, as defined in Table 2.3 and Section 3.2, is the degree to which the technology to be adopted fits within the adopters' values, needs, past experiences and practices. This study hypothesised:

H1: Compatibility of the IoT artefact with existing organisational values and needs influences its adoption as reflected by the continuance intention of organisations.

Compatibility → Organisational Adoption: The results show that Compatibility significantly affects Organisational Adoption as reflected by the continuance intention of IoT ($\beta = 0.393$), with a p-value < 0.001. This suggests that Compatibility is positively and significantly related to IoT's Organisational Adoption as reflected by the continuance intention, and the relationship is highly robust (T-statistic = 7.634). Therefore, the hypothesis was supported.

The findings differ from Savoury's (2018) conclusion in his study on IoT adoption in the US manufacturing sector where compatibility did not significantly impact IoT adoption. His findings also differ from other studies, such as the research of Ramavhona and Mokwena (2016), who found that compatibility influences the adoption of new technologies in organisations. This finding confirms the Diffusion of Innovation Theory (Rogers, 1995) which states that compatibility leads to rapid adoption of technology. Wang et al. (2010) confirmed this relationship in their study on RFID adoption in the manufacturing industry; they found that compatibility is a facilitator for technology adoption, and they also found that compatibility has a significantly positive impact on organisations' adoption of new technology.

These findings highlight the need for IoT artefacts to be compatible with the existing values and needs of the organisation. IoT technologies should be flexible, faultless, easy to implement and fit into the existing organisation's systems, strategic intent and resources. Although the participants expressed a positive sentiment or view towards IoT compatibility, and the path coefficient confirmed a strong relationship between compatibility and the intent to adopt and continue using IoT, they also expressed concerns about the extent of this compatibility (Ahmetoglu et al., 2023). This could imply that while organisations view IoT as a good fit, practical concerns about compatibility may require further consideration or support, specifically during implementation.

5.5.2 Complexity

Complexity is the extent to which an innovation or technology is easy to understand or use (Rogers, 1995; Pichlak, 2016). This study hypothesised:

H2: The Complexity of the IoT artefact negatively influences its adoption as reflected by the continuance intention of organisations.

The path coefficient Complexity → Organisational Adoption as reflected by the continuance intention of IoT indicates that Complexity has a non-significant positive effect on Organisational Adoption as reflected by the continuance intention ($\beta = 0.009$), with a p-value of 0.815 (see Table 5.9). These results show that Complexity has no statistically significant influence on Organisational Adoption as reflected by the continuance intention.

Complexity has been reported in many studies to have a negative impact on the adoption of innovation (Ahmetoglu et al., 2023; Lai et al., 2016; Pichlak, 2016). During the initial phase of adoption and implementation, perceptions of complexity tend to become negative based on the organisational context, such as the flexibility of the decision-makers and access to information and knowledge (Pichlak, 2016). This negativity associated with complexity is seen in the research done by Lai et al. (2016) on technology evaluation and imitation. In this research, Lai et al. (2016) found that ERP systems had a high failure rate because of the complexity of implementation. A lack of internationally accepted standards and protocols for IoT and its heterogeneous nature contribute to the perception of IoT as challenging to use and understand (Ahmetoglu et al., 2023).

Contrary to these studies, the data analysis of this present research indicated that complexity had a weak correlative relationship on the organisational adoption of IoT. However, this was statistically insignificant. Therefore, it was found that complexity does not significantly impact organisations' adoption as reflected by the continuance intention of IoT. An explanation for this could be that the participants did not perceive or foresee any significant challenges related to the complexity of IoT. This is evident in the means of all three items, which ranged from 2.43 to 2.87, measured using a five-point Likert scale, with one (1) strongly disagree and five (5) strongly agree. Therefore, the participants disagreed with the three statements (that is, the difficulty of interacting with IoT systems; that IoT would consume too much time from the IT staff; and that IoT artefacts would not make achieving the organisation's goals easy). The moderate standard deviation of 1.16 to 1.24 indicated some variability in this view.

In summary, Complexity has a small positive effect on Organisational Adoption as reflected by the continuance intention ($\beta = 0.009$). However, since the p-value is 0.815, the results show that Complexity does not have a statistically significant influence on Organizational Adoption as reflected by the continuance intention. Therefore, the hypothesis is rejected.

5.5.3 Connectivity

The absence of reliable connectivity has been found in findings from previously reported research to be an element that poses a challenge to adopting IoT (Kamble et al., 2019; Kronlid et al., 2024; Palattella et al., 2016). Matook and Brown (2017) defined connectivity as the strength of linkage between system elements and their environments. Connectivity is recognised to be an essential and distinct element of IoT, allowing objects to interact with each other and with users (Dong et al., 2017; Sullivan et al., 2023). This study hypothesised that:

H3: The connectivity of the IoT artefact influences its adoption as reflected by the continuance intention of organisations.

In the current study, the enquiry into the influence of connectivity on adopting IoT in organisations (Connectivity → Organisational Adoption as reflected by the continuance intention) found that the relationship was marginally non-significant, $\beta=0.124$, $t=1.675$, $p=0.095$. While the effect is positive, it did not meet the significance threshold of 0.05. Therefore, the hypothesis (H3) was not supported; connectivity does not influence the adoption as reflected by the continuance intention of IoT in organisations.

Although the positive coefficient together with the high mean scores for the beneficial features of IoT suggests that improved connectivity quality may positively influence IoT adoption to some extent, these results were not statistically significant. A possible explanation is that the participants shared Oberländer et al.'s (2018) view that connectivity is the defining feature of IoT technology, and they took it for granted that its connection quality would be acceptable. Palattella et al. (2016) noted a wide variety of types of connectivity used in IoT devices, some of which, such as 5G Cellular, are ubiquitous, reliable, scalable and cost-efficient.

These findings imply that organisations expect IoT connectivity to be reliable, responsive and seamless, and hence connectivity is not a deciding factor when adopting or continuing to use the IoT systems. The hypothesis (H3) was not supported.

5.5.4 Scalability

Scalability is the ability of an artefact or technology to handle change, increased workload and increased usage volume (Matook & Brown, 2017; Sharma et al., 2023). IoT systems anticipate that increasing numbers of devices will be connected over time, making the system's scalability a significant challenge and need (Kamble et al., 2019). This study hypothesised:

H4: The scalability of the IoT artefact influences its adoption as reflected by the continuance intention of organisations.

The results of the influence of Scalability on Organisational Adoption as reflected by the continuance intention of IoT show a non-significant negative effect ($\beta = -0.002$), with a p-value of 0.979, indicating no statistically significant relationship between scalability and organisational adoption as reflected by the continuance intention. It is important to note the negative effect reported. However, since the negative effect of $\beta = -0.002$ is very close to zero it must be interpreted as not meaningful and having no practical effect. Therefore, the hypothesis, H4, was not supported.

The findings differ from the work of Hamad et al. (2024), who reported that the proliferation of IoT devices pose a significant challenge. Kamble et al. (2019) sounded the same alarm over the increasing number of IoT network devices that are physically connected.

A possible explanation of the findings is the focus on the future; both Kamble et al. (2019) and Hamad et al. (2024) speak of the threat of scalability as devices are being added and networks expanded, this points mainly to the future. It is possible that most of the research participants' organisations currently do not have many devices deployed or used in a pilot project. Therefore, the scalability challenge may not be attracting much attention at this time. It is important to note that in the results of the current study scalability does not affect the adoption decision. The practical implication is that organisations must nevertheless keep themselves aware of future requirements so as to effectively handle the probable future increase in size of the IoT systems network and the complexity of the data this produces (as recommended by Kamble et al., 2019).

5.5.5 Relative Advantage

Relative advantage is the extent to which an innovation or technology provides benefits beyond those of the existing operational environment (Sivathanu, 2019). The advantages a technology offers can determine its level of adoption (Ramavhona & Mokwena, 2016; Rogers, 1995). This study hypothesised:

H5: Relative Advantage of the IoT artefact influences its adoption as reflected by the continuance intention of organisations.

The results in Table 5.9 show that the impact of Relative Advantage on the Organisational Adoption as reflected by the continuance intention of IoT was statistically significant, with a path coefficient of $\beta=0.135$, $t=2.086$, $p=0.037$. This shows that as organisations perceive more significant benefits they are increasingly likely to adopt IoT technology. Therefore, Hypothesis 5 was supported.

The participants agreed strongly that IoT has advantages, particularly in terms of productivity, cost efficiency and customer service, and this perceived relative advantage was found to positively influence organisational adoption decisions.

These findings differ from those of Savoury (2019) which studied IoT adoption in the US manufacturing sector. Savoury (2019) found that relative advantage did not impact IoT adoption significantly. However, his results were inconclusive and, therefore, he called for more research to be done in this regard.

On the other hand, Rogers (1995) found that the perception of benefits of technology do influence its adoption. Sivathanu (2019) concluded that relative advantage influences the adoption of the Industrial Internet of Things (IIoT) in the manufacturing sector. Sivathanu (2019) found that IIoT offered important benefits including connecting factories, predicting maintenance upgrades, bringing in new business opportunities, controlling assets remotely and increasing productivity. The results of the current study are also consistent with those of Sorri et al. (2022), who said that firms consider a technology's practical benefits before adopting it as they expect these to give them a competitive advantage in an increasingly challenging market. In two case studies undertaken by Brous and Janssen (2019) it was clearly established that adoption of IoT is deeply rooted in a need to achieve tangible benefits.

Based on the descriptive statistics and path analysis, the current results show that organisations see substantial benefits in adopting and continuing to use IoT systems, particularly in enhancing productivity and cost efficiency. These perceived advantages positively influence organisational adoption decisions.

5.5.6 Integration

An important aspect of IoT systems is the integration of technologies, legacy systems, hardware and communications protocols, actuators, sensors, software, back-end cloud computing and data storage systems to form a comprehensive and enabling system (Sivathanu, 2019). Technology integration is described as the degree of connectivity between systems and sub-systems (such as sensors and actuators) to the backend systems (such as databases that store and distribute the collected data and applications) (Palacios-Marqués et al., 2015; Sullivan et al., 2023). This integration includes incorporating new technologies and processes into existing ones. Integration also refers to the flow of data from and to various sources (Wixom & Todd, 2005). The lack of IoT standards, heterogeneity at the device level and diverse data consumers all pose integration challenges and are severe impediments to the adoption of IoT (Brous & Janssen, 2019). An absence of integration leads to the fragmentation and isolation of systems that could have opened doors to a new offering of services and products (Abdelghaffar & Abousteit, 2021).

This study hypothesised:

H6: The Integration of the IoT artefact influences its adoption as reflected by the continuance intention of organisations.

The results in Table 5.9 show a significant positive relationship between Integration and Organisational Adoption as reflected by the continuance intention of IoT (β=0.230, t=2.933, p=0.004). This indicates that enhanced integration capabilities within an organisation positively influence IoT adoption as reflected by the continuance intention. Therefore, Hypothesis 6 was supported.

These results confirm Chan et al.'s (2012) and finding that integration is a significant factor in technology adoption. Chan et al.'s (2012) study looked into factors affecting e-collaboration in small and medium enterprises (SMEs) and concluded that organisations looking to adopt new technologies would be concerned about integrating existing systems. These authors noted that both large firms and SMEs are concerned about integrating legacy systems.

Wixom and Todd (2005) argue that it is increasingly unlikely that a system will be built from scratch. Instead, over time companies will continue to add new applications and systems to meet specific business needs and to gain competitive advantage. As a result, integration becomes an essential part of the systems development process. The escalating accumulation of varying types of equipment, and an associated lack of technical knowledge, present a risk and undermine positive integration of IoT during the implementation phase (Brous & Janssen, 2019). To counter this challenge, Brous and Janssen (2019) suggested that companies need to: a) identify and define the services and solutions that may be required before implementation, b) ensure staff have the required knowledge to develop and implement these services and solutions and c) ensure the capacity to use, manage and maintain these services and technologies is and continues to be available. Savoury (2019) shares this view and stresses the importance of having the necessary infrastructure and a skilled and knowledgeable workforce before implementing or integrating IoT systems. Organisations must be aware that integration is a key component of IoT (Abdelghaffar & Abousteit, 2021; Fernandez-Gago et al., 2024). It not only allows systems to communicate and exchange data, but can uncover many new services and business opportunities.

Overall, this analysis suggests that integration is perceived as a valuable characteristic of IoT systems. The research participants consistently saw strong integration as an asset in adopting and continuing to use IoT technologies. The significant path coefficient between integration and IoT adoption highlights the role of integration as a driving factor, noting its importance in organisations' decision-making processes regarding new technologies.

5.5.7 Interactivity

Interactivity is a complicated concept described in different ways in the literature (Jiang et al., 2010). However, the following explanation of interactivity regarding IoT is used here. Interactivity is the extent to which people and things can participate in modifying the form and content of a mediated environment in real-time by communicating bidirectionally with, and responding promptly to remote objects (Chang et al., 2014; Jiang et al., 2010).

This study hypothesised:

H7: Interactivity of the IoT artefact influences its adoption as reflected by the continuance intention of organisations.

The path coefficient results in Table 5.9 show that the relationship between Interactivity and Organisational Adoption as reflected by the continuance intention of IoT was not statistically significant ($\beta = 0.049$, $t = 0.742$, $p = 0.459$). This indicates that perceived interactivity on its own does not significantly impact the likelihood of IoT adoption as reflected by the continuance intention in organisations. Therefore, Hypothesis 7 was not supported.

It is important to note that the strength of IoT systems lies in the interactivity they allow among things, whether physical or digital, handling data from disparate systems regardless of their physical location and distance (Ehie & Chilton, 2020). However, as reported above, the analysis results of the current study reveal that interactivity does not affect participants' adoption as reflected by the continuance intention of IoT. An explanation for this could be that interactivity is not a concept seen by the participants as affecting the business directly in the way that relative advantage, integration or compatibility do. When deciding to continue with an innovation, decision-makers are likely to prioritise factors that offer them a tangible benefit that clearly impacts the organisation's operations in terms of productivity, cost efficiency, customer service and satisfaction, profitability, downtime, collaboration, and time-saving. The second possible explanation is that some organisations and industries do not require instantaneous interactive communication (Kiousis, 2002).

5.5.8 State

State is the extent to which a system can record and hence 'remember' its preceding sequence of events (Matook & Brown, 2017). A system is stateful when it remembers its actions and can return to its original state or transition to another suitable state; it is considered stateless when it cannot achieve either (Mayar et al., 2022). IoT systems interact with other systems, whether machines or people, and records of these interactions and are needed and contribute to system stability.

The study hypothesised:

H8: The State of the IoT artefact influences its adoption as reflected by the continuance intention of organisations.

The results from the direct path analysis between State and Organisational Adoption as reflected by the continuance intention of IoT ($\beta = -0.064$, $t = 0.922$, $p = 0.357$) indicate that the impact of state-related factors on adoption as reflected by the continuance intention was not statistically significant (see Table 5.9). Therefore, the hypothesis (H8) was not supported.

The results suggest that, while participants may perceive system state information, traceability, and memory as being valuable, these features do not strongly influence the decision to adopt IoT within organisations. State is not a factor recognised as being closely related to the operation of an organisation, in contrast with interactivity. Nguyen et al. (2015) found that organisations adopt innovation mainly to meet customers' requirements, expand business, meet industry standards, make a profit, and improve the quality of products and services so as to remain competitive in the market. A possible explanation for rejecting the hypothesis is that organisations do not see the state characteristic of technology innovation as being able to make a meaningful contribution to any of the aforementioned benefits of adoption.

5.5.9 Security

Studies have highlighted serious concerns about, and evident threats resulting from weak security in IoT systems (Ahmetoglu et al., 2023; Kronlid et al., 2024; Mukherjee et al., 2024). Security is the extent to which damage can be avoided (Chang et al., 2014) and the extent to which a product, system, or artefact is risk-free (Al-Momani et al., 2016; Gao & Bai, 2014). Jalali et al. (2019) highlighted three unique IoT weaknesses that are obstacles to its adoption, namely a high number of endpoints, inconsistent protocols and physical safety. Rose et al. (2015)

pointed out that security must be given top priority in order to address the challenges faced by IoT implementations. Kamble et al. (2019) state that the trillions of devices that are connected to the Internet worldwide face the threat of cyber-attacks and data theft. Chan et al. (2012), in their study on the diffusion of RFID in the healthcare industry, found that security had the most significant impact on the adoption of RFID technology. These same authors found that a general concern existed regarding the protection and privacy of information that was transmitted in an automated and wireless manner, and the transmissions of such details were susceptible to eavesdropping by hackers.

This study hypothesised:

H9: Security of the IoT artefact influences its adoption as reflected by the continuance intention of organisations.

The analysis results (see Table 5.9), on the impact of Security on the Organisational Adoption as reflected by the continuance intention of IoT, indicated that security did not have a statistically significant effect on IoT adoption ($\beta = 0.002$, $t = 0.029$, $p = 0.977$). The extremely high p-value ($p > 0.05$) suggests that security concerns do not affect the decisions of the organisations represented by participants in this sample to adopt IoT systems. The negligible beta coefficient ($\beta = 0.002$) also implies an almost non-existent relationship between security and IoT adoption. These findings indicate that, within this context, other factors play a more crucial role in influencing adoption decisions. Therefore, the hypothesis (H9) was not supported.

The instrument used for data collection addressed five security concerns: data transmission security, data storage security, physical security of IoT devices, cyber security protection, and finally the challenge of distributing security patches to remote devices.

The absence of a significant effect of Security on Organisational Adoption as reflected by the continuance intention of IoT in these findings is inconsistent with previous studies that have found security to have a significant impact on technology adoption in general (Chan et al, 2012; Ahmetoglu et al., 2023). Security problems related to linked devices have increased enormously and hence should be taken seriously (Rekha et al., 2023). Brous and Janssen (2019) supported the view that there is a risk to organisations due to the nature of IoT systems, and that these are related to the interoperability and integration of the systems. Other technology professionals concur that security is a significant concern for IoT systems (Sivathanu 2019, Koohang et al., 2022; Mukherjee et al., 2024).

This inconsistency with literature might be explained by participants expecting that any IoT solution intended for organisational use already meets a minimum security standard, thus making security less influential in their adoption decisions. In other words, security may be considered necessary but insufficient to drive adoption and is not a determinant factor. Secondly, the participants may perceive that IoT systems are secure, making security less of a determinant factor in their decision to adopt IoT as reflected by the continuance intention.

These findings imply that technical executives need to strive harder to influence their community's attitude towards IoT system security at a commercial level (Rekha et al., 2023). Organisations need to keep up with security enhancements and implement measures that prevent significant expected failures (Raimundo & Rosário, 2022). Raimundo and Rosário (2022) add that more can be done at the design level by protecting IoT systems using AI. This needs to focus on the entry points of the system to detect and classify attacks and on decentralising end-to-end security using technologies such as blockchain, and to introduce both public key iterative authentication methods and compact self-healing processes for wireless communications (Rekha et al., 2023).

5.5.10 Self-Adaptation

The grand vision behind IoT is to connect people and things to anyone and anything (Butun et al., 2019); in doing so, it enables things to think and interact (Ng & Wakenshaw, 2017). IoT systems are self-adapting as they can analyse, judge, act and handle the data by means of sensors, memory, data processing and the communication capabilities that empower them (Dong et al., 2017; Pinochet et al., 2018; Sivathanu, 2019). Self-adaptation is the extent to which an artefact can constantly improve its own ‘memory’ by learning from the new data collected; self-adaptation is also called intelligence (Dong et al. (2017). Through self-adaptation, an artefact can adjust its responses based on feedback received and react to stimuli in its environment or outside the system; this allows it to improve its internal processes and perform the same task more effectively in the future (Matook & Brown, 2017). Pinochet et al. (2018) argue that smart, connected objects are changing the competitiveness of organisations and hence bring new economic opportunities for businesses.

This study hypothesised:

H10: Self-adaptation of the IoT artefact influences its adoption as reflected by the continuance intention of organisations.

The relationship between the direct path between Self-adaptation and Organisational Adoption as reflected by the continuance intention of IoT (β=0.197, t=2.761, p=0.006) was statistically significant. This showed that self-adaptation strongly influences IoT adoption as reflected by the continuance intention in organisations (See Table 5.9). Therefore, the hypothesis (H10) was supported.

This means that an increase in positive perception of IoT's self-adaptive capabilities is associated with an increase in the likelihood of IoT adoption. This statistically significant result suggests that organisations are more likely to adopt IoT systems when they perceive them as self-adaptive - capable of operating competently, sensibly and intelligently over an extended period of time.

These findings align with the literature on self-adaptation and intelligence in technologies. Organisations can extract meaningful insights from their data by integrating intelligence into IoT, and this allows them to optimise and secure operations and unlock new transformative services relatively easily (Sivathanu, 2019). Similarly, intelligent, precise and predictable IoT systems can offer a wide range of services and new digital artefacts, thereby offering many new possibilities to organisations (Butun et al., 2019). Ng and Wakenshaw (2017) concur, they say that the IoT systems' ability to reveal situations and contexts introduces opportunities to design and offer real-time, on-demand, responsive services and goods from the data.

This comprehensive analysis supports the idea that self-adaptive features in IoT systems are essential for organisational adoption. They offer organisations operational competence, sensible decision-making and adaptive intelligence, all of which align well with organisational needs and promote favourable adoption attitudes. Furthermore, the findings reported in the literature emphasise that organisations find IoT systems that adjust to dynamic conditions particularly valuable, as they can operate effectively without constant human oversight (Ng & Wakenshaw, 2017). This is particularly evident in an era where intelligence in physical things has become ubiquitous and has transformed products that could become obsolete into dynamic, reconfigurable and engaging services (Ng & Wakenshaw, 2017). This suggests that, for organisations considering IoT adoption as reflected by the continuance intention, self-adaptation is recognised as being a valuable characteristic that enhances the perceived benefits of IoT and is likely to encourage adoption. The findings confirm that factors closely associated with to business interests influence innovation adoption as reflected by the continuance intention (Nguyen et al., 2015).

5.5.11 Synchronicity

Synchronicity is the ability of a system and the people using it to share information in a timely and coordinated manner (Thomas et al., 2023). It is the extent to which applications, systems and people work together simultaneously with a shared pattern of coordinated behaviour and focus (Dennis et al., 2008). It is immediacy, a perception of technology speed in response to requests (Shin, 2019). IoT systems work in a heterogeneous environment; therefore, their actions must move at a rate that is compatible with the processing speeds of the other ecosystem components with which they operate. Synchronicity captures the time when the IOT artefact exchanges inputs and outputs with its environment (Matook & Brown, 2017).

This study hypothesised:

H11: The Synchronicity of the IoT artefact influences its adoption as reflected by the continuance intention of organisations.

The direct path analysis between Synchronicity and Self-adaptation and Organisational Adoption as reflected by the continuance intention of IoT ($\beta=-0.065$, $t=1.052$, $p=0.293$) (see Table 5.9) revealed that synchronicity has no significant impact on the adoption of IoT in organisations. Therefore, Hypothesis 11 was not supported.

These results are not entirely surprising since this study evaluated only the velocity or speed of response of synchronicity. In the current high-information-exchange age, delay in sharing information is no longer acceptable. In the reported findings the participants mean response for this construct (Synchronicity) was high, indicating that organisations do value fast response times in IoT systems. Synchronicity may, therefore, contribute to a positive perception of IoT and could play a supportive role in adoption if it enhances other critical factors.

The negative path coefficient of -0.065 suggests a small inverse relationship between perceptions of synchronicity and organisational adoption of IoT. This may be explained by examining various industries separately, or by assessing practical implementation cases in isolation. The industries' needs for simultaneous communication may vary; certain industries may urgently require immediate communication, meaning all communication participants must communicate simultaneously, while other industries may be able to tolerate a delay (be asynchronous).

Dennis et al. (2008) argued that in some instances, optimal media communication performance can only be achieved when there is a balance between conveyance and convergence. Communication aims to create and share information to reach a mutual understanding. This is where conveyance and convergence begin to make sense. Dennis et al. (2008) found that, although the effective exchange of information benefits the production of valuable data, it does not necessarily fulfil synchronicity, which requires all the entities involved to move at the same rate and exactly together to receive and process the data and produce output. However, the participants may need to do extensive information processing in the *conveyance* communication process, which requires time. In this case the process would benefit from relatively low synchronicity rather than *convergent* communication, which is more about transmitting information and requires rapid transmission of information.

The practical implications of these findings are that communication transmission speed alone cannot achieve synchronicity; each communication participant's conveyance and convergence needs should be considered. Technology vendors should be prepared to reassure organisations that system performance and fast response requirements can be maintained, but only if information is processed quickly. The study found that synchronicity does not play a decisive role in the organisational adoption as reflected by the continuance intention of IoT in organisations.

5.5.12 Interoperability

Businesses and academic researchers often highlight the importance of interoperability of IoT systems (Fernandez-Gago et al., 2024; Noura et al., 2019). The lack of standards and manufacturing lock-in has mainly resulted in challenges regarding interoperability. Noura et al. (2019) emphasise the consequences of vendor lock-in due to platforms promoting their own IoT infrastructure, proprietary protocols and interfaces, as well as incompatible standards, formats and semantics. These create closed ecosystems, increase the operational cost of IoT systems, and cause product functionality and stability issues.

Abdelghaffar and Abousteit (2021) state that, in order to achieve the conceived objectives of IoT systems in organisations, a variety of devices, platforms, services and systems should be able to operate together without problems.

This study hypothesised:

H12: Interoperability of the IoT artefact influences its adoption as reflected by the continuance intention of organisations.

Table 5.9 shows the results of a regression analysis performed to measure the impact of Interoperability on Organisational Adoption as reflected by the continuance intention of IoT systems. The analysis revealed no statistically significant relationship, $\beta = -0.092$, $t = 1.450$, $p = 0.148$. This means that interoperability does not influence the adoption of IoT in organisations. Therefore, the hypothesis (H12) is not supported.

These findings do not align with the literature on interoperability. Brous and Janssen (2019) claimed that interoperability issues impede the adoption of IoT. Hamal et al. (2024) concurred that interoperability can help organisations harness the full benefits of IoT. Noura et al. (2019) shared the same sentiments when they said that a lack of interoperability prevents the emergence of IoT technology use on a large scale.

A possible explanation of this disparity is the gap between the technical factors that are more difficult to understand and other factors that decision-makers are more familiar with. The current findings suggest that interoperability does not influence the adoption of IoT in organisations. However, it could be a tool to accelerate the implementation of IoT and elevate its emergence to a large scale. This would transform how business is done by creating new services benefitting from extensive data exchange. Butun et al. (2019) recommended that there should be a predetermined and standardised data exchange format as this could make interoperability more feasible and simplify its achievement within the business environment.

5.6 Summary of Findings

The study examined several artefactual characteristics of IoT that could influence its adoption as reflected by the continuance intention in organisations. Of the participants in the survey, 36%

stated that they were already implementing IoT, 19% were currently involved in a pilot project, and a further 8% had completed a pilot study and decided not to continue using IoT.

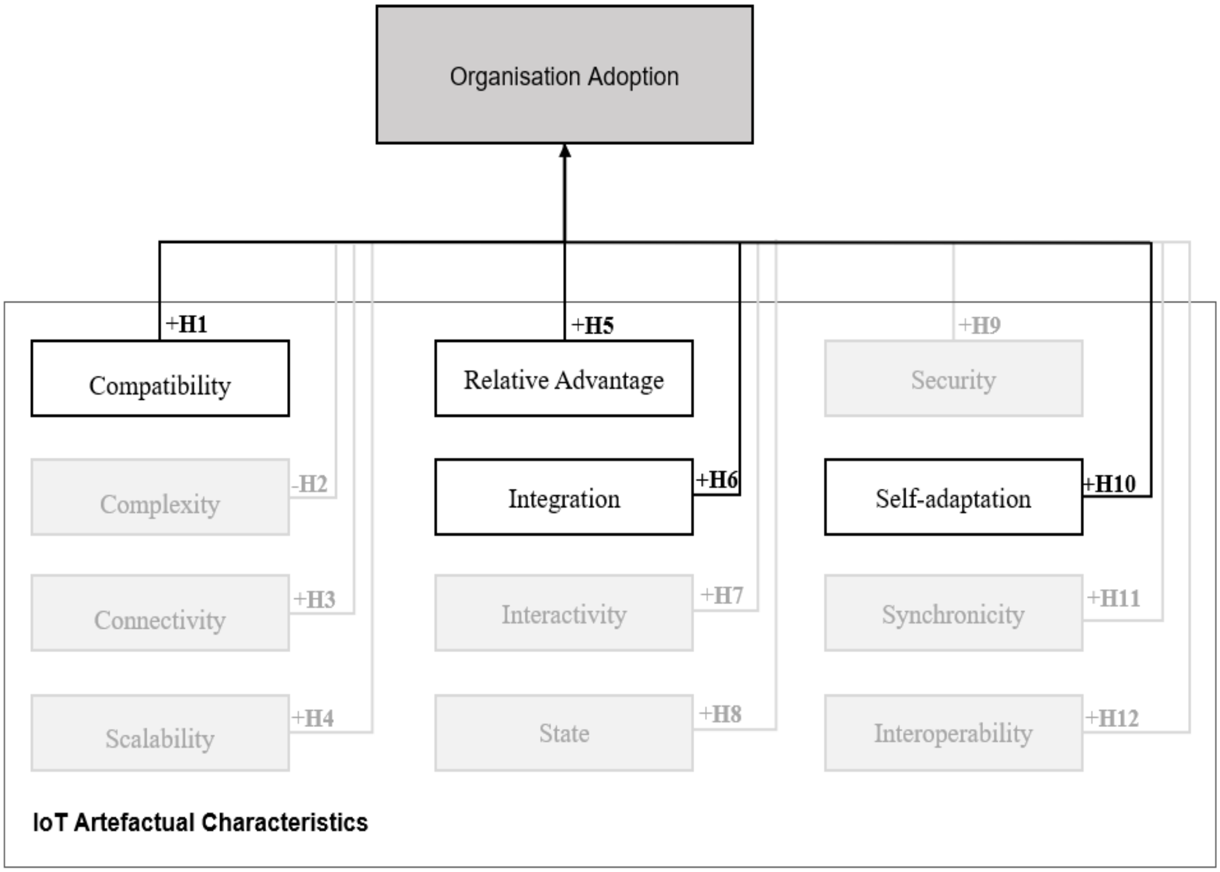

Figure 5.1: Resultant Model

Twelve characteristics were identified each of which were represented by an independent variable: Compatibility, Complexity, Connectivity, Scalability, Relative Advantage, Integration, Interactivity, State, Security, Self-Adaptation, Synchronicity, and Interoperability. The dependent variable, Organisation Adoption, measured the intention to implement IoT and to continue using IoT. The results (see Figure 5.1) showed that Compatibility, Relative Advantage, Integration and Self-Adaptation had a significant positive effect on adoption as reflected by the continuance intention of IoT in organisations. All four of these are closely linked to core business issues, indicating that organisations will adopt and continue to use IoT if they believe it will help them to become or remain competitive. This means the new technology and systems must provide features that clearly assist the organisation to meet customers' requirements, expand the business, meet industry standards, make a profit, and improve the quality of products and services offered. The study shows that organisations seek intelligent, self-adaptable IoT systems that can analyse, judge, act and handle the data, and can integrate it with that of other systems, including legacy systems. Such IoT systems are, therefore, compatible with current systems, can be integrated quickly and easily and offer tangible business value.

CHAPTER 6: CONCLUSION

6.1 Overview

The study aimed to identify key IoT artefact characteristics, and determine those characteristics that influence organisational adoption as reflected by the continuance intention. It is a cross-country study with 293 participants from South Africa, the United Kingdom, and the United States of America. The study reported a suitable variety in levels of adoption and implementation.

Twelve technology characteristics were identified as relevant to IoT adoption as reflected by continuance intention. These are compatibility, complexity, connectivity, scalability, relative advantage, integration, interactivity, state, security, self-adaptation, synchronicity and interoperability. The findings suggest that four of these, relative advantage, compatibility, integration and self-adaptation, significantly impact adoption as reflected by continuance intention. These explain approximately 65% of the variation in the organisations' intention to adopt.

It was found that the characteristics close to the business, such as relative advantage, compatibility, integration, and self-adaptation, influence the decision to adopt more than the technocentric characteristics, such as complexity, connectivity, interactivity, state, synchronicity and interoperability.

6.2 Theoretical Contribution

This study is a response to several calls made for IS research, first by Orlikowski et al. (2001) and later by Matook and Brown (2017), to take the conceptualisation of IT artefacts more seriously. The study went beyond the traditional Technology-Organisational-Environment framework technology characteristics adapted from the Diffusion of Innovation framework, such as relative advantage, complexity, and compatibility, to show that integration and self-adaptation, also called intelligence, significantly impact technology adoption as reflected by continuance intention. The comprehensive operationalisation of IoT artefact factors and measurement instrument produced in this study can be used in similar future studies for technology artefacts in general.

6.3 Practical Implications

Given the study found that the characteristics close to business influence IoT adoption, as reflected by the continuance intention of IoT in organisations, greater emphasis should be placed on business-centric factors to help organisations identify why they need to continue using IoT and aid decision-makers and technology professionals in future implementations of IoT. Organisations cannot continue to use IoT systems without deriving sufficient benefits and competitive advantage; therefore, it is recommended that before considering adoption, organisations ensure that the proposed IoT system offers measurable advantages, such as reduced operational costs, enhanced productivity, new revenue channels and improved customer experience.

The findings highlighted the need for IoT artefacts to be compatible with organisations' values, needs, and practices and to grow with them by being able to include other emerging technologies in the future. In an era when it is less likely that a system can be built from scratch, organisations should ensure, through an audit, that the IoT system being considered can integrate easily, coexist with existing systems, and support industry standards. The managers responsible for the implementation should be aware of any changes and modifications required.

Technology leaders and organisations should consider IoT systems that can adapt and modify their behaviour at runtime in response to system or environment changes. These intelligent, precise, predictable IoT systems can extend various services, be used with digital artefacts and data services, and reveal various profitable opportunities for organisations.

6.4 Limitations and Future Research

This study is not without limitations, revealing several opportunities for future studies. The cross-sectional time frame was limited to the academic period during which the study was undertaken. Due to this time constraint, the study was conducted using the services of an online panel to gather participants to make up an acceptable sample during a short period. Future studies may consider a longitudinal study to observe the adoption as reflected by continuance intention over a more extended period and with a larger sample.

Eight of the twelve proposed hypotheses were not supported, which may be attributed to contextual differences related to the geographical locations of the participants—South Africa, the

United Kingdom, and the United States. Additionally, the study did not account for potential moderating factors such as industry type or organizational size, which could have influenced the results. Future research should build on this foundation by examining the model within specific industries or national contexts and by including relevant moderating variables. This would provide a more nuanced understanding of the factors influencing technology adoption and allow for greater insight into how contextual elements shape these outcomes.

The results of the HTMT validity test (see Table 5.5) indicated discriminant validity problems. However, the study proceeded despite this, as validity was established through cross-loading and the Fornell-Larcker criterion. Future research could improve the current study by using a larger sample and further operationalise the constructs.

Additional research is needed to clarify why technocentric characteristics such as connectivity, security, and interoperability were unexpectedly found not to influence adoption as reflected by the continuance intention. Future studies can measure the influence of IoT technology artefact characteristics on each other.

References

Abdelghaffar, H., & Abousteit, M. (2021). Internet of Things (IoT) interoperability success criteria. *International Journal of Enterprise Information Systems (IJEIS), 17* (1), 85-105.

Ab Hamid, M. R., Sami, W., & Sidek, M. M. (2017, September). Discriminant validity assessment: Use of Fornell & Larcker criterion versus HTMT criterion. In *Journal of Physics: Conference series* (Vol. 890, No. 1, p. 012163). IOP Publishing.

Ahmetoglu, S., Che Cob, Z., & Ali, N. A. (2023). Internet of things adoption in the manufacturing sector: A conceptual model from a multi-theoretical perspective. *Applied Sciences*, *13*(6), 3856.

Al-Momani, A. M., Mahmoud, M. A., & Ahmad, M. S. (2016). Modeling the adoption of Internet of things services: A conceptual framework. *International Journal of Applied Research, 2* (5), 361-367.

Ansari, O., & Guo, H. (2024). extending near field communication range for ultra-dense Internet of things. *IEEE Journal of Radio Frequency Identification*, 8, 770–779. https: //doi.org/10.1109/JRFID.2024.3453770

Barbin, M. V., Leonardo, E. J., & Yacoub, M. D. (2024). Passive RFID tag for detection of electric energy consumption. *IEEE Internet of Things Journal*, *11* (7), 12146-12152. https: //doi.org/10.1109/JIOT.2023.3333239

Baker, J. (2012). The technology–organization–environment framework. In *Y.K. Dwivedi et al. (eds.), Information systems theory: Explaining and predicting our digital society, Vol. 1*, (pp. 231–245). Integrated Series in Information Systems 28, Springer Science+Business Media, https: //doi.org/10.1007/978-1-4419-6108-2_12

Bassi, A., Bauer, M., Fiedler, M., Kramp, T., Van Kranenburg, R., Lange, S., & Meissner, S. (Eds.). (2013). *Enabling things to talk: Designing IoT solutions with the IoT architectural reference model*. Springer Nature. https: //doi.org/10.1007/978-3-642-40403-0

Behardien, R. (2023). *Antecdents and consequences of consumer Internet of things security self-efficiency.* (Masters Dissertation, Faculty of Commerce, Department of Information Systems, University of Cape Town). [Accessed 20 Jan 2025] https://open.uct.ac.za/items/908b4d52-0f8f-469e-8ccd-a013da32272d

Bhattacherjee, A. (2012). *Social science research: Principles, methods, and practices*. University of South Florida.

Boell, S. K., & Cecez-Kecmanovic, D. (2010). Literature reviews and the hermeneutic circle. *Australian Academic & Research Libraries*, *41* (2), 129-144.

Boell, S. K., & Cecez-Kecmanovic, D. (2014). A hermeneutic approach for conducting literature reviews and literature searches. *Communications of the Association for Information Systems*, *34* (1), 12.

Brous, P., & Janssen, M. (2015). A systematic review of impediments blocking Internet of things adoption by governments. In M Janssen et al. (Eds), *Open and Big Data Management and Innovation* (pp. 81-94) Lecture Notes in Computer Science 9373. Springer, ISBN 978-3-319-25012-0

Butun, I., Österberg, P., & Song, H. (2019). Security of the Internet of Things: Vulnerabilities, attacks, and countermeasures. *IEEE Communications Surveys & Tutorials*, *22* (1), 616-644.

Chan, F. T., Chong, A. Y. L., & Zhou, L. (2012). An empirical investigation of factors affecting e-collaboration diffusion in SMEs. *International Journal of Production Economics*, *138* (2), 329-344.

Chang, Y., Dong, X., & Sun, W. (2014). Influence of characteristics of the Internet of things on consumer purchase intention. *Social Behavior and Personality: An International Journal, 42* (2), 321-330. doi: 10.2224/sbp.2014.42.2.321

Chatterjee, S., Xiao, X., Elbanna, A., & Sarker, S. (2017). The information systems artifact: A conceptualization based on general systems theory. In Bui, T & Sprague Jr, R (Eds.), *Proceedings of the 50th Hawaii International Conference on System Sciences. University of Hawaii, United States of America, ISBN: 978-0-9981331-0-2*

Chong, A. Y.-L., & Chan, F. T. S. (2012). Structural equation modeling for multi-stage analysis on Radio Frequency Identification (RFID) diffusion in the health care industry. *Expert Systems with Applications*, *39*(10), 8645–8654. https://doi.org/10.1016/j.eswa.2012.01.201

Čolaković, A., & Hadžialić, M. (2018). Internet of things (IoT) : A review of enabling technologies, challenges, and open research issues. *Computer Networks, 144*, 17-39.

Dabbagh, M., & Rayes, A. (2019). Internet of things security and privacy. In *Internet of things from hype to reality* (pp. 211-238) Springer. https: //doi.org/10.1007/978-3-319-99516-8_8.

Dennis, A. R., Fuller, R. M., & Valacich, J. S. (2008). Media, tasks, and communication processes: A theory of media synchronicity. *MIS Quarterly, 32* (3), 575-600.

Díaz, M., Martín, C., & Rubio, B. (2016). State-of-the-art, challenges, and open issues in the integration of Internet of things and cloud computing. *Journal of Network and Computer Applications, 67*, 99-117.

Dong, X., Chang, Y., Wang, Y., & Yan, J. (2017). Understanding usage of Internet of Things (IOT) systems in China: Cognitive experience and affect experience as moderator. *Information Technology & People*, *30* (1), 117-138.

Durant, R. (2002). Synchronicity: a post-structuralist guide to creativity and change. *Journal of Organizational Change Management*, *15* (5), 490-501.

Evans, H. I. (2015). Barriers to successful implementation of the Internet of things in marketing strategy. *International Journal of Information and Communication Technology Research*, *5* (9).

Evans, J. R., & Mathur, A. (2018). The value of online surveys: A look back and a look ahead. *Internet Research*, *28*(4), 854-887.

Ehie, I. C., & Chilton, M. A. (2020). Understanding the influence of IT/OT Convergence on the adoption of Internet of Things (IoT) in manufacturing organizations: An empirical investigation. *Computers in Industry*, *115*, 103166.

Fernandez-Gago, C., Ferraris, D., Roman, R., & Lopez, J. (2024). Trust interoperability in the Internet of things. *Internet of Things, 26*, 101226. doi:10.1016/j.iot.2024.101226

Fornell, C., & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research, 18* (1), 39-50.

Gao, L., & Bai, X. (2014). A unified perspective on the factors influencing consumer acceptance of Internet of things technology. *Asia Pacific Journal of Marketing and Logistics, 26* (2), 211-231. doi: 10.1108/APJML-06-2013-0061

Giri, A., Dutta, S., Neogy, S., Dahal, K., & Pervez, Z. (2017). Internet of Things (IoT) a survey on architecture, enabling technologies, applications and challenges. In *The International Conference on Internet of Things and Machine Learning* (pp. 1-12). Association for Computing Machinery. https: //doi.org/10.1145/3109761.3109768

Goldkuhl, G. (2013). The IT artefact: An ensemble of the social and the technical? – A rejoinder : An ensemble of the social and the technical? – A rejoinder. *Systems, Signs & Actions*, 7(1), 90–99.

Goyal, K. K., Garg, A., Rastogi, A., & Singhal, S. (2018). A literature survey on Internet of things (IoT). *International Journal of Advanced Networking and Applications, 9* (6), 3663-

3668.

Gregor, S., & Hevner, A. R. (2013). Positioning and presenting design science research for maximum impact. *MIS Quarterly, 37* (2), 337-355.

Gvozdenovic, S., Becker, J. K., Mikulskis, J., & Starobinski, D. (2024). IoT-scan: Network reconnaissance for the Internet of Things. *IEEE Internet of Things Journal*, 11 (8), 13091-13107. doi: 10.1109/JIOT.2023.3327293

Haegele, J. A., & Hodge, S. R. (2015). Quantitative methodology: A guide for emerging physical education and adapted physical education researchers. *The Physical Educator*, *72* (5), 59–75. https: //doi.org/10.18666/TPE-2015-V72-I5-6133

Hair, J. F., Risher, J. J., Sarstedt, M., & Ringle, C. M. (2019). When to use and how to report the results of PLS-SEM. European Business Review, 31 (1), 2–24.

Hamad, D., Yalda, K., Tapus, N., Okumus, I.T. (2024). Enhancing IoT scalability and security through SDN. *Romanian Journal of Information Technology and Automatic Control*, *34* (2), 113-126.

Hillmer, U. (2008). Technology acceptance: An analysis of the social and personal influences that affect human reaction to disruptive technological change. *International Journal of Technology, Knowledge and Society, 4 (4), 91.*

Hite, D. M., Voelker, T., & Robertson, A. (2016). Measuring Perceived Anonymity: The Development of a Context Independent Instrument. Journal of Methods and Measurement in the Social Sciences, 6 (1). https: //doi.org/10.2458/azu_jmmss.v5i1.18305

Jalali, M. S., Kaiser, J. P., Siegel, M., & Madnick, S. (2019). The Internet of things promises new benefits and risks: A systematic analysis of adoption dynamics of IoT products. *IEEE Security & Privacy, 17* (2), 39-48.

Jiang, Z., Chan, J., Tan, B. C., & Chua, W. S. (2010). Effects of Interactivity on Website Involvement and Purchase Intention. *Journal of the Association for Information Systems*, *11* (1), 34-59.

Kamble, S. S., Gunasekaran, A., Parekh, H., & Joshi, S. (2019). Modeling the Internet of things adoption barriers in food retail supply chains. *Journal of Retailing and Consumer Services, 48*, 154-168.

Kees, J., Berry, C., Burton, S., & Sheehan, K. (2017). An analysis of data quality: Professional panels, student subject pools, and Amazon's Mechanical Turk. *Journal of Advertising*, *46*(1), 141-155.

Kiousis, S. (2002). Interactivity: A concept explication. *New Media & Society*, *4* (3), 355-383.

Kronlid, C., Brantnell, A., Elf, M., Borg, J., & Palm, K. (2024). Sociotechnical analysis of factors influencing IoT adoption in healthcare: A systematic review. *Technology in Society*, *78*, 102675-102675.

Kumar, A., Dhingra, S., & Falwadiya, H. (2023). Adoption of Internet of Things: A systematic literature review and future research agenda. *International Journal of Consumer Studies*, *47* (6), 2553-2582.

Koohang, A., Sargent, C. S., Nord, J. H., & Paliszkiewicz, J. (2022). Internet of Things (IoT): From awareness to continued use. *International Journal of Information Management*, *62*, 102442.

Lai, V. S., Lai, F., & Lowry, P. B. (2016). Technology evaluation and imitation: do they have differential or dichotomous effects on ERP adoption and assimilation in China? *Journal of Management Information Systems*, *33* (4), 1209-1251.

Latif, K. F., Sajjad, A., Bashir, R., Shaukat, M. B., Khan, M. B., & Sahibzada, U. F. (2020). Revisiting the relationship between corporate social responsibility and organizational performance: The mediating role of team outcomes. *Corporate Social Responsibility and Environmental Management*, *27* (4), 1630-1641. https: //doi.org/10.1002/csr.1911

Latif, K. F., Machuca, M. M., Marimon, F., & Sahibzada, U. F. (2021). Servant leadership, career, and life satisfaction in higher education: A cross-country study of Spain, China, and Pakistan. *Applied Research in Quality of Life*, *16*, 1221-1247.

Lee, I., & Lee, K. (2015). The Internet of things (IoT) : Applications, investments, and challenges for enterprises. *Business Horizons, 58* (4), 431-440.

Lu, Y., Papagiannidis, S., & Alamanos, E. (2018). Internet of things: A systematic review of the business literature from the user and organisational perspectives. *Technological Forecasting & Social Change, 136*, 285-297. doi: 10.1016/j.techfore.2018.01.022.

Luthra, S., Garg, D., Mangla, S. K., & Berwal, Y. P. S. (2018). Analyzing challenges to Internet of Things (IoT) adoption and diffusion: An Indian context. *Procedia Computer Science*, *125*, 733-739.

Madakam, S., Ramaswamy, R., & Tripathi, S. (2015). Internet of Things (IoT) : A literature review. *Journal of Computer and Communications*, *3* (5), 164-173.

Matook, S., & Brown, S. A. (2017). Characteristics of IT artifacts: A systems thinking-based framework for delineating and theorizing IT artifacts. *Information Systems Journal*, *27* (3), 309-346.

Mayar, K., Carmichael, D. G., & Shen, X. (2022). Resilience and systems - A review. Sustainability, 14 (14), 8327.

McMillan, S. J., & Hwang, J. S. (2002). Measures of perceived interactivity: An exploration of the role of direction of communication, user control, and time in shaping perceptions of interactivity. *Journal of Advertising*, *31*(3), 29-42.

Mineraud, J., Mazhelis, O., Su, X., & Tarkoma, S. (2016). A gap analysis of Internet-of-things platforms. *Computer Communications, 89*, 5-16.

Mohammed, F., Ibrahim, O., & Ithnin, N. (2016). Factors influencing cloud computing adoption for e-government implementation in developing countries: Instrument development. *Journal of Systems and Information Technology*, *18*(3), 297–327. https://doi.org/10.1108/JSIT-01-2016-0001

Mukherjee, S., Baral, M. M., Chittipaka, V., Nagariya, R., & Patel, B. S. (2024). Achieving organizational performance by integrating industrial Internet of things in the SMEs: A developing country perspective. *The TQM Journal*, 36 (1), 265–287.

Ndih, E. D. N., & Cherkaoui, S. (2016). On enhancing technology coexistence in the IoT era: ZigBee and 802.11 case. *IEEE Access, 4*, 1835-1844.

Newman, P. A., Guta, A., & Black, T. (2021). Ethical considerations for qualitative research methods during the COVID-19 pandemic and other emergency situations: Navigating the virtual field. *International Journal of Qualitative Methods*, 20, 16094069211047823.

Ng, I. C. L., & Wakenshaw, S. Y. L. (2017). The Internet-of-Things: Review and research directions. *International Journal of Research in Marketing*, 34 (1), 3–21.

Nguyen, T. H., Newby, M., & Macaulay, M. J. (2015). Information technology adoption in small business: Confirmation of a proposed framework. *Journal of Small Business Management*, 53(1), 207–227.

Noura, M., Atiquzzaman, M., & Gaedke, M. (2019). Interoperability in Internet of things: Taxonomies and open challenges. *Mobile Networks and Applications,* 24 (3), 796–809.

Oberländer, A. M., Röglinger, M., Rosemann, M., & Kees, A. (2018). Conceptualizing business-to-thing interactions - A sociomaterial perspective on the Internet of things. *European Journal of Information Systems, 27* (4), 486-502.

Oliveira, T., & Martins, M. F. (2011). Literature review of information technology adoption models at firm level. *Electronic Journal of Information Systems Evaluation, 14* (1), 110.

Oliveira, T., Thomas, M., & Espadanal, M. (2014). Assessing the determinants of cloud computing adoption: An analysis of the manufacturing and services sectors. *Information & Management, 51* (5), 497-510.

Orlikowski, W. J., & Iacono, C. S. (2001). Research commentary: Desperately seeking the "IT" in IT research - A call to theorizing the IT artifact. *Information Systems Research*, *12* (2), 121-134. https: //doi.org/10.1287/isre.12.2.121.9700

Osman, A. M. S. (2019). A novel big data analytics framework for smart cities. *Future Generation Computer Systems*, *91*, 620-633.

Palattella, M. R., Dohler, M., Grieco, A., Rizzo, G., Torsner, J., Engel, T., & Ladid, L. (2016). Internet of things in the 5G era: Enablers, architecture, and business models. *IEEE Journal on Selected Areas in Communications, 34* (3), 510-527.

Palacios-Marqués, D., Soto-Acosta, P., & Merigó, J. M. (2015). Analyzing the effects of technological, organizational and competition factors on Web knowledge exchange in SMEs. Telematics and Informatics, 32 (1), 23-32.

Patel, K. K., Patel, S. M., & Scholar, P. (2016). Internet of things-IOT: Definition, characteristics, architecture, enabling technologies, application & future challenges. International Journal of Engineering Science and Computing, 6 (5).

Pichlak, M. (2016). The innovation adoption process: A multidimensional approach. Journal of Management & Organization, 22 (4), 476-494.

Petter, S., Carter, M., Randolph, A., & Lee, A. (2018). Desperately seeking the information in information systems research. ACM SIGMIS Database: the DATABASE for Advances in Information Systems, 49 (3), 10-18. https: //doi.org/10.1145/3242734.3242736

Pinochet, L. H. C., Lopes, E. L., Srulzon, C. H. F., & Onusic, L. M. (2018). The influence of the attributes of "Internet of Things" products on functional and emotional experiences of purchase intention. *Innovation & Management Review*, *15* (3), 303-320.

Polgavande, A. S., & Kulkarni, A. D. (2017). Internet of things (IoT) : A literature review *International Journal of Research in Advent Technology (IJRAT),* (E-ISSN: 2321-9637), 2321-9637.

Porter, C. O., Outlaw, R., Gale, J. P., & Cho, T. S. (2019). The use of online panel data in management research: A review and recommendations. *Journal of Management*, *45*(1), 319-344.

Ramavhona, T. C., & Mokwena, S. (2016). Factors influencing Internet banking adoption in

South African rural areas. South African Journal of Information Management, 18 (2), 1-8.

Rayes, A., & Salam, S. (2017). Internet of things from hype to reality (2nd ed.). Switzerland: Springer. https: //doi.org/10.1007/978-3-319-99516-8

Rey, A., Panetti, E., Maglio, R., & Ferretti, M. (2021). Determinants in adopting the Internet of Things in the transport and logistics industry. *Journal of Business Research*, *131*, 584-590.

Rogers, E. M. (1995). *Diffusion of innovations* (4th ed.). The Free Press (Sept. 2001). New York, 15-23.

Roky, H., & Al Meriouh, Y. (2015). Evaluation by users of an industrial information system (XPPS) based on the DeLone and McLean model for IS success. *Procedia Economics and Finance*, 26, 903-913.

Rose, K., Eldridge, S., & Chapin, L. (2015). *The Internet of things: An overview*. The Internet Society (ISOC), 80 (15), 1-53. *Https: //Www.Internetsociety.Org/Sites/Default/Files/ISOC-IoT-Overview-20151014_0.Pdf* [Accessed 12 Jan 2024]

Raimundo, R. J., & Rosário, A. T. (2022). Cybersecurity in the Internet of things in industrial management. Applied Sciences, 12 (3), 1598.

Rekha, S., Thirupathi, L., Renikunta, S., & Gangula, R. (2023). Study of security issues and solutions in Internet of Things (IoT). *Materials Today: Proceedings*, *80*, 3554-3559.

Saunders, M., Lewis, P., & Thornhill, A. (2019). *Research methods for business students (8th ed.).* Prentice Hall: London.

Savoury, R. D. (2019). *Influential determinants of Internet of things adoption in the US manufacturing sector* (Doctoral dissertation, Walden University). https: //scholarworks.waldenu.edu/dissertations/7076/

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.

Shah, S., Bolton, M., & Menon, S. (2020, January). A study of Internet of things (IoT) and its impacts on global supply chains. In *2020 International Conference on Computation, Automation and Knowledge Management (ICCAKM)* (pp. 245-250). IEEE. doi: 10.1109/ICCAKM46823.2020.9051474

Sharma, C., Bharadwaj, S. S., Gupta, N., & Jain, H. (2023). Robotic process automation adoption: contextual factors from service sectors in an emerging economy. *Journal of Enterprise Information Management*, *36* (1), 252-274. https://doi.org/10.1108/JEIM-06-

2021-0276.

Sharma, V., & Tiwari, R. (2016). A review paper on "IOT" & It's Smart Applications. *International Journal of Science, Engineering and Technology Research (IJSETR)*, *5*(2), 472-476.

Shin, D. D. (2019). Blockchain: The emerging technology of digital trust. *Telematics and Informatics*, *45*, 101278

Scanzio, S., Rosani, M., Scamuzzi, M., & Cena, G. (2024). QR codes: From a Survey of the State-of-the-Art to Executable eQR Codes for the Internet of Things. *IEEE Internet of Things Journal*, 11(13), 23699- 23710.

Sivathanu, B. (2019). Adoption of industrial IoT (IIoT) in auto-component manufacturing SMEs in India. *Information Resources Management Journal (IRMJ), 32* (2), 52-75.

Singh, P. (2016). Internet of things (IoT) : A literature review. *International Research Journal of Engineering and Technology (IRJET), 03* (12), 943-949. [Accessed 12 Jan 2024] https: //www.irjet.net/archives/V3/i12/IRJET-V3I12221.pdf

Sorri, K., Mustafee, N., & Seppänen, M. (2022). Revisiting IoT definitions: A framework towards comprehensive use. *Technological Forecasting and Social Change*, *179*, 121623. https: //doi.org/10.1016/j.techfore.2022.121623

Sullivan, Y., Fosso Wamba, S., & Dunaway, M. (2023). Internet of things and competitive advantage: a dynamic capabilities perspective. *Journal of the Association for Information Systems*, *24* (3), 745-781.

Tejada, J. J., & Punzalan, J. R. B. (2012). On the misuse of Slovin's formula. *The Philippine Statistician*, *61* (1), 129-136.

Thomas, M. A., Sandhu, R. K., Oliveira, A., & Oliveira, T. (2023). Investigating the effect of media synchronicity in professional use of video conferencing applications. *Internet Research*, *33*(6), 2131–2171. https://doi.org/10.1108/INTR-12-2021-0887

Tornatzky, L. G., & Fleischer, M. (1990). *The Processes of Technological Innovation*. Lexington Books.

Tsai, M. C., Lee, W., & Wu, H. C. (2010). Determinants of RFID adoption intention: Evidence from Taiwanese retail chains. *Information & Management*, *47*(5-6), 255-261.

Tu, M. (2018). An exploratory study of Internet of things (IoT) adoption intention in logistics and supply chain management. *The International Journal of Logistics Management,* 29 (1), 131-151.

Vermesan, O., & Bacquet, J. (Eds.). (2020). *Internet of Things - the call of the edge: Everything intelligent everywhere*, (1st ed.). Rivers Publishers.

Wachter, S. (2018). Normative challenges of identification in the Internet of things: Privacy, profiling, discrimination, and the GDPR. *Computer Law & Security Review, 34* (3), 436-449.

Wang, Y.-M., Wang, Y.-S., & Yang, Y.-F. (2010). Understanding the determinants of RFID adoption in the manufacturing industry. *Technological Forecasting & Social Change*, *77*(5), 803–815. https://doi.org/10.1016/j.techfore.2010.03.006.

Wixom, B. H., & Todd, P. A. (2005). A theoretical integration of user satisfaction and technology acceptance. *Information Systems Research*, *16*(1), 85–102. https://doi.org/10.1287/isre.1050.0042.

Wu, F., & Ma, J. (2020). Evolution dynamics of agricultural Internet of things technology promotion and adoption in China. *Discrete Dynamics in Nature and Society*, *2020* (1), 1854193. DOI: 10.1155/2020/1854193.

Yilmaz, K. (2013). Comparison of quantitative and qualitative research traditions: Epistemological, theoretical, and methodological differences. *European* Journal *of Education*, 48 (2), 311-325.

PART A: Demographics.

1. **Gender**: Male ☐ Female ☐ Prefer not to answer. ☐
2. **Age**: 18-24 ☐ 25-34 ☐ 35-44 ☐ 45-54 ☐ 55 & Above. ☐
3. Highest Education:

Primary ☐ Secondary ☐ College (Certificate) ☐

College (Diploma) ☐ Bachelor's Degree ☐ Masters/PhD. ☐

4. Position:

Senior Application Engineer ☐ Head of IT ☐ IoT Specialist ☐

CIO ☐ Innovation Officer ☐ Project Manager ☐ Director ☐

5. Information Technology Years of Experience .

3) Below 1 ☐ 1-2 ☐ 3-4 ☐ 5-6 ☐ Above 6 ☐

6. Internet of Things Years of Experience .

4) Below 1 ☐ 1-2 ☐ 3-4 ☐ 5-6 ☐ Above 6. ☐

7. Organisation Sector.

Public sector ☐ Private sector ☐ Not-for-profit ☐ Other ________________ .

8. Industry:

Academic/Education ☐ Information Technology/Telecomms ☐ Manufacturing ☐
Financial Services ☐ Engineering Government ☐ Healthcare ☐ .

Retail ☐ Other _______________ .

9. Age of Organisation .

Below 1 year ☐ 1-2 years ☐ 3-5 years ☐ 6 -9 years ☐ 10 years and above. ☐

10. Size of Organisation (number of employees in all locations) .

Below 5 ☐ 5-50 ☐ 51-300 ☐ Above 300 ☐ Don't know ☐

11. Which of the following best describes your organisation?

- ☐ Have not considered IoT yet.
- ☐ Spoken informally about IoT.
- ☐ Formally investigated IoT and currently running an IoT pilot.
- ☐ Completed a pilot and will not be implementing IoT.
- ☐ Have completed a pilot and planning to implement IoT.
- ☐ Currently implementing IoT.

PART B: IoT Characteristics.

To what extent do you agree with the following statements as they relate to your firm

Construct	Code	Items	Source
Scalability	SCA01	IoT system capacity can be scaled to handle increasing or decreasing numbers of connected devices.	Sharma et al. (2023)
	SCA02	IoT system capacity can easily be increased by adding more computing resources (e.g. processors and memory).	
	SCA03	IoT system devices can be reallocated from one service to another.	
	SCA04	Once an IoT system device is set up for one geographical area, it can be easy to reuse it to expand to other geographical areas.	
	SCA05	IoT system devices can be assigned to multiple services at the same time	
Compatibility	CMPA1	Using IoT systems would fit well with the way my organisation performs.	Mohammed et al., 2016
	CMPA2	IoT systems would not require many business process changes in my organisation.	
	CMPA3	IoT systems would be compatible with all aspects of work in my organisation.	
Complexity	CMPX01	It would not be easy to get IoT systems to do what the organisation wants them to do.	Mohammed et

Construct	Code	Items	Source
	CMPX02	Interacting with IoT systems would be difficult.	al., 2016
	CMPX03	Learning to operate IoT systems would not be easy for employees.	
	CMPX04	It would take too much time for IT staff if they want to use IoT systems to do their normal duties.	
	CMPX05	Overall, IoT systems would be easy to use*.	
Connectivity	CON01	IOT systems would have stable connectivity.	Dong et al. (2017)
	CON02	IOT systems would have few connectivity errors.	
	CON03	IOT systems connectivity would quickly respond to input.	
	CON04	IOT systems connectivity would allow a seamless flow of data.	
Interactivity	INTA01	IoT systems would enable two-way communication	McMillan & Hwang (2002)
	INTA02	IoT systems would enable concurrent communication.	
	INTA03	IoT systems would not be capable of doing real-time communication*.	
	INTA04	IoT systems would be interactive.	

Integration	INTG01	IoT systems would effectively integrate data from different areas in the organisation.	Wixom & Todd (2005)
	INTG02	IoT systems would pull together data that comes from different places in the organisation	
	INTG03	IoT systems would effectively combine data from different areas of the organisation.	
	INTG04	IoT systems would effectively integrate into existing IT infrastructure in my organisation.	
	INTG05	IoT systems would integrate with systems that are already in use in my organisation.	
Relative Advantage	RA01	IoT systems would contribute to increased cost efficiency	Tsai et al. (2010)
	RA02	IoT systems would contribute to improved inventory replenishment.	
	RA03	IoT systems would contribute to improved customer service.	
	RA04	IoT systems would contribute to competitive marketing strategies.	
	RA05	IoT systems would contribute to increased asset tracking.	
	RA06	IoT systems would contribute to increased business productivity.	
Security	SEC01	Data transmitted via IoT systems would be secure.	Chong & Chan (2012)
	SEC02	Data stored in IoT systems would be secure.	

	SEC03	IoT system devices would be physically secure	
	SEC04	IoT systems would be well protected against cyber-attacks	
	SEC05	IoT systems would securely distribute patches and updates to remote devices.	
Self-Adaptation	SAD01	IoT systems in my organisation would operate competently.	Dong et al. (2017)
	SAD02	IoT systems in my organisation would operate sensibly.	
	SAD03	IoT systems in my organisation would be intelligent.	
State	STA01	IoT systems would keep records of prior connections.	Derived from the definition of: Matook & Brown (2017)
	STA02	IoT system logs would provide sufficient information about its state.	
	STA03	IoT systems actions would be traceable.	
	STA04	IoT systems would remember previously performed events.	
Synchronicity	SYNC01	IoT system response would be quick.	Thomas et al. (2023)
	SYNC02	IoT systems would respond quickly.	
	SYNC03	IoT systems would respond immediately.	
	SYNC04	IoT systems would take a long time to send a response.	

Interoperability	INTO01	IoT systems would interoperate regardless of the underlying communication protocols.	Derived from Bassi et al. (2013)
	INTO02	IoT systems would interpret data consistently, regardless of the different devices or platforms involved.	
	INTO03	IoT systems would have well-defined APIs that would allow diverse devices and applications to interact.	
Organisation Adoption	OADP01	My organisation intends to continue using IoT systems.	Lai et al. (2016)
	OADP02	My organisation intends to use IoT regularly in the future.	
	OADP03	My organisation would highly recommend IoT for other firms to adopt.	

.

Appendix B: Survey Cover letter

.

Survey Cover letter .

Dear Participant, .
My name is Henry Tshilenge, and I am a Masters student at the University of Cape Town. For my final project, I am examining the adoption of the Internet of Things in Organisations. Because you are an IT leader or specialist who has a say in adopting new technology in your organisation, I am inviting you to participate in this research study by completing this online survey.
The following questionnaire will require approximately 10 minutes to complete. This research is approved by the Faculty of Commerce Ethics Research Committee. Your participation in this research is voluntary. You can choose to withdraw from the study at any time. You are not required to supply any identifiable information, and all responses will be confidential and used for this research only.
Should you have any questions regarding the research, please feel free to contact the researcher: Henry Tshilenge (Tshhen003@myuct.ac.za) .
Dr Irwin Brown (Supervisor) .
Sincerely, .
Henry Tshilenge.

Appendix C: Descriptive Statistics

	Mean		Median	SD	Excess kurtosis	Skewness	Count
SCA01	4.083	4.218	4.000	0.801	0.416	-0.896	293
SCA03		3.959	4.000	0.873	0.918	-0.878	293
SCA04		4.065	4.000	0.822	0.918	-0.863	293
SCA05		4.089	4.000	0.882	0.307	-0.865	293
CMPA01	3.649	4.041	4.000	0.991	0.903	-1.078	293
CMPA02		3.253	3.000	1.135	-0.832	-0.269	293
CMPA03		3.652	4.000	1.112	-0.489	-0.611	293
CMPX01	2.616	2.867	3.000	1.242	-1.092	0.104	293
CMPX02		2.427	2.000	1.159	-0.584	0.582	293
CMPX04		2.553	2.000	1.166	-0.788	0.41	293
CON01	4.076	4.024	4.000	0.91	0.03	-0.729	293
CON03		4.089	4.000	0.821	1.200	-0.909	293
CON04		4.116	4.000	0.843	0.905	-0.945	293
INTA01	4.068	4.068	4.000	0.936	0.445	-0.94	293
INTA02		4.126	4.000	0.863	0.746	-0.951	293
INTA04		4.010	4.000	0.929	0.251	-0.816	293
INTG01	4.116	4.119	4.000	0.88	1.067	-1.052	293
INTG02		4.177	4.000	0.785	1.199	-0.919	293

	Mean		Median	SD	Excess kurtosis	Skewness	Count
INTG03		4.113	4.000	0.825	1.063	-0.946	293
INTG05		4.055	4.000	0.849	0.846	-0.912	293
RA01	4.106	4.123	4.000	0.854	1.025	-0.966	293
RA02		4.044	4.000	0.851	0.248	-0.685	293
RA03		4.109	4.000	0.917	0.288	-0.859	293
RA04		3.928	4.000	0.934	0.232	-0.741	293
RA05		4.177	4.000	0.777	-0.041	-0.672	293
RA06		4.256	4.000	0.752	1.771	-1.042	293
SEC01	3.932	3.969	4.000	0.982	0.148	-0.85	293
SEC02		4.041	4.000	1.004	0.55	-0.997	293
SEC03		3.877	4.000	1.013	-0.079	-0.704	293
SEC04		3.771	4.000	1.054	-0.485	-0.551	293
SEC05		4.000	4.000	0.96	0.281	-0.861	293
SAD01	4.093	4.113	4.000	0.833	1.426	-1.034	293
SAD02		4.106	4.000	0.905	0.73	-0.989	293
SAD03		4.061	4.000	0.951	0.733	-1.009	293
STA01	4.105	4.020	4.000	0.963	0.267	-0.87	293
STA02		4.229	4.000	0.747	1.478	-0.992	293
STA03		4.205	4.000	0.792	1.502	-1.046	293
STA04		3.966	4.000	0.897	0.424	-0.789	293

	Mean		Median	SD	Excess kurtosis	Skewness	Count
SYNC01	4.065	4.143	4.000	0.73	0.517	-0.6	293
SYNC02		4.133	4.000	0.761	0.571	-0.696	293
SYNC03		3.918	4.000	0.909	0.016	-0.605	293
INTO01	3.926	3.638	4.000	1.005	-0.38	-0.485	293
INTO02		3.942	4.000	0.924	1.147	-1.007	293
INTO03		4.198	4.000	0.785	0.457	-0.791	293
OADP01	4.328	4.058	4.000	0.988	0.498	-0.971	293
OADP02		3.969	4.000	1.091	-0.157	-0.827	293
OADP03		3.956	4.000	1.039	0.045	-0.828	293

.