Design of ethics to enhance privacy, security, and safety in e-Logistics Internet of Things.

First Name/s:	Caitlyn
Surname:	Crown
Student Number:	3720546
Department:	Department of Information Systems
Degree:	MCom Information Systems E-Logistics (Mini Thesis)
Supervisor:	Dr Johan Breytenbach

Abstract

Purpose: This study focuses on making Internet of Things (IoT) implementations in the e-logistics industry private, secure, and safe. This is achieved through meeting the following objectives: creating an operational definition of ethics, identifying how ethics can be incorporated into the design of IoT, identifying whether ethics can be employed to ensure privacy, security, and safety, and documenting recommendations on how ethics by design can be used to improve the privacy, safety, and security of IoT e-logistics devices.

Methodology/Design: This study utilises the theoretical framework detailed by Van Aken describing the main pillars of system design, namely object design, process design, and realization design. This framework guided the data collection and data analysis of the study by providing a context to inform further categorisation of the data for better insights. The data collection method used was a questionnaire to a single case study of 15 respondents using the philosophy of interpretivism to identify and understand the embarkment of knowledge during a study.

Research Limitations: This study collected and used data from a single case study in South Africa – an IoT device manufacturer and software development organization focused on retail distribution IoT devices. This data collection from the case study limited the scope of the study to a specific sample that did not cater to the full spectrum of Logistics devices and their private, secure, and safe implementation.

Practical Implications: The identification of design principles presented in this study could potentially provide a set of guidelines for developers and designers of IoT devices in the retail logistics industry, to improve the privacy, security, and safety of these devices.

Originality/Value: This study aims to provide future designers with additional recommendations – design heuristics - on how to ensure their IoT logistics devices are private, secure, and safe. Additionally, this mini thesis offers a view of where ethics in logistics can be incorporated by providing new design principles within a South African context.

Keywords:

Ethics by Design; privacy; security; safety; IoT; big data; ethics; Ethical Design, e-logistics

Declaration

I declare that *Design of ethics to enhance privacy, security, and safety in e-Logistics Internet of Things* is my own work, that it has not been submitted for any degree or examination in any other university, and that all the sources I have used or quoted have been indicated and acknowledged by complete references.

Full name: Caitlyn Crown Date: March 2023

Signed: C.Crown

Table of Contents

List of Figures

List of Tables

Abbreviations and Acronyms

IoT:	Internet of Things
SCM:	Supply Chain Management
RFID:	Radio Frequency Identification
GPS:	Global Positioning System
PoPIA:	Protection of Personal Information Act
GDPR:	General Data Protection Regulations
IS:	Information Systems
EbD:	Ethics by Design
UoA:	Unit of Analysis
AIDC:	Automatic Identification and Data Capture

Chapter 1: Introduction and Background

1.1 Introduction

The study has been divided into research steps as illustrated in the image below (see Figure 1). This chapter begins by providing background to the main themes, which include privacy, security, safety, ethics, IoT, logistics and big data. Additionally, the problem statement and research objectives of the study are outlined by providing a framework for collecting and reporting on relevant data.

1.2 Background

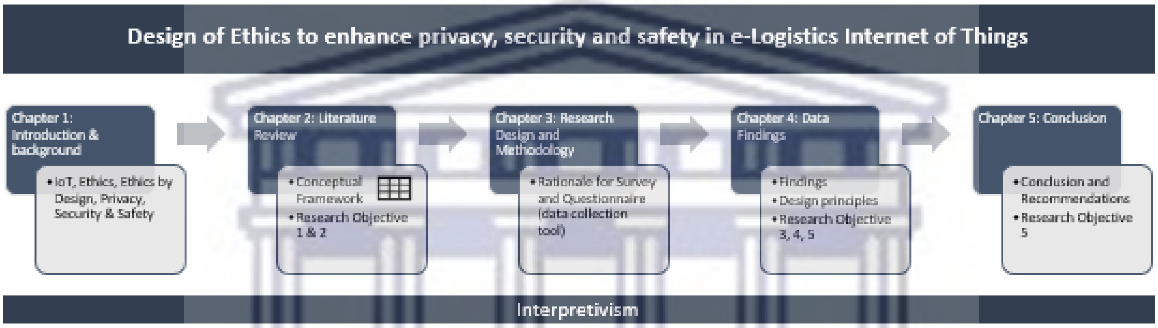

Design of Ethics to enhance privacy, security and safety in e-Logistics Internet of Things
Chapter 1: Introduction & background
• IoT, Ethics, Ethics by Design, Privacy, Security & Safety
Chapter 2: Literature Review
• Conceptual Framework
• Research Objective 1 & 2
Chapter 3: Research Design and Methodology
• Rationale for Survey and Questionnaire (data collection tool)
Chapter 4: Data Findings
• Findings
• Design principles
• Research Objective 3, 4, 5
Chapter 5: Conclusion
• Conclusion and Recommendations
• Research Objective 5
Interpretivism

Figure 1: Approach of the study

During the last decade, many aspects of life have shifted towards a digital sphere with humans becoming more reliant on the digitalisation of society (Weinhardt, 2021). Hence, Internet of Things (IoT) emerged as a growing concept that has generated great interest over the past few years. According to Baldini and Botterman (2018) IoT can be defined as the connectivity of people and things integrated in a network. However, this concept has become quite intricate due to the various definitions promoted by various academics. Mena et al. (2018) add to this definition by stating that IoT can be further defined as a variety of devices connected to interact with users and other devices via a network infrastructure. Sutherland (2020) further states that this concept of IoT is born out of the current technological revolution.

Due to the fast-paced IoT adoption and utilisation of the last decade, many industries have found interest in this technology, specifically supply chain and logistics industries. In fact, IoT has recently been found to enhance supply chains and revolutionise supply chain management (SCM) (Núñez-Merino et al., 2020). IoT devices like RFID chips, sensors and GPS technologies are being used to monitor and track products and shipments (Tu et al., 2018). Recent studies have shown that the integration of IoT in various supply chain processes has greatly improved and optimised manufacturing and production logistics. This shows that there is potential for greater opportunities to be brought about with the adoption of IoT (Tu et al., 2018). As a consequence of this growth in adoption and utilisation of IoT, the growth of data and data-related processes have also been identified.

Data is growing at an exponential rate; a rate at which many companies struggle to understand and keep up with. This emergence of increased data generation has evolved and brought about the concept of Big Data (Baldini & Botterman, 2018). Big data is a relatively new paradigm that has triggered various debates amongst scholars and academics. Hence, the definition of big data is still evolving. There has been general consensus that big data is concerned with vast volumes of information collected through technologies (Jurkiewicz, 2018). Big data refers to the immense amounts of data collected regarding livelihoods and environments (Fang et al., 2017). This exponential growth in the amount of data has vastly increased the awareness and concerns about privacy, security, liability, property rights and ethical issues (Jurkiewicz, 2018). Moreover, the characteristics concerned with big data are tightly linked to the issues of privacy, security and ethics (Ogbuke et al., 2020). Therefore, there is a need for extensive research to identify factors that can be used to reach and achieve privacy and security standards.

Given the vast variety, velocity and volume of data, its utility has led to growing concerns of privacy and security. Hence, the need for more individuals in the logistics field to be aware of the impact these technologies can have on these end users. The concept of privacy differs from country to religion to background. However, privacy in the context of big data is sensitive data that individuals prefer not to disclose (Fang et al., 2017). This definition of privacy differs according to data owners, which is a rapidly growing concern.

The rate at which data has been growing, has highlighted multiple concerns of how data is captured, managed, and stored. The introduction of the Protection of Personal Information Act (PoPIA) in South Africa and the General Data Protection Regulations (GDPR) in Europe aim to mitigate these concerns. These and other regulatory frameworks have been introduced to provide guidelines on how personal information is collected and processed (Kandeh et al., 2018; Badii et al., 2020). Some of the key principles set out by the PoPIA are accountability, processing limitation, purpose specification, further processing limitation, information quality, openness, security safeguards, and data subject participation. In fact, Kandeh et al. (2018) state that that one of the reasons for the introduction of this act is the relationship between privacy and technology and how data is handled therein. There is thus a need to dig deeper into privacy, security, and ethical concerns in the logistics sector.

The pervasive data growth and collection through such IoT devices have highlighted various ethical concerns (Mercan et al., 2020). These concerns include the ways in which users feel disempowered as data is being controlled and protected without their consent (Baldini & Botterman, 2018). This is where Ethical Design has garnered widespread attention amongst various academics. Ethical Design has garnered various definitions. Nonetheless, growing consensus has defined Ethical Design as design that empowers users to freely guide their choices and be aware of their consequences whilst interacting with IoT/technology devices (Baldini & Botterman, 2018; Peters et al., 2020; Weinhardt, 2021).

Due to the shift in technology, over the past few years, the Association for Computing Machinery has issued new ethical standards and guidelines (ACM, 2018). These guidelines provide pertinent information regarding the fundamental principles to be applied during ethical decision making of computing professionals. Additionally, in 2019 the IEEE identified, created and launched new standards addressing the Ethical Design of intelligent and autonomous systems (Chatila & Havens, 2019). This indicates that ethics is not only a concern of end-users but also of computing and technology professionals. With these standards and approaches, these IoT devices are able to bridge the gap between people and technology by fostering a level of trust.

1.3 Statement of the Research Problem

Increased data collection, as a consequence of the emergence and adoption of IoT, has brought about many concerns regarding the privacy, security, and safety among users thereof. As individuals become more aware of the consequences surrounding their privacy, security, and safety within various logistics industry use cases, the potential for the adoption and integration of Ethical Design has become a topic of debate (Jurkiewicz, 2018). At the time of publication of this mini thesis, there was a growing understanding of the importance of making IoT device implementations in South Africa more private, secure, and safe. This would be done by embedding ethics into the devices themselves through Ethical Design. There is a clear gap identified in Information Systems literature regarding this topic, with only a few publications discussing the ethical design of IoT devices used within logistics processes.

1.4 Primary Research Question

How can the design of privacy, security, and safety of IoT devices used in e-logistics be improved?

1.5 Research Objectives

- To create an operational definition of “ethics” and “Ethics by Design” within Information Systems.
- To identify from literature how ethics can be incorporated into the design of IoT devices.
- To identify how Ethics by Design can be employed to ensure the privacy, security, and safety of logistics systems.
- To identify the perspectives of logistics experts towards the use of Ethics by Design within IoT devices used in the e-logistics industry.
- To make recommendations about how Ethics by Design can be used to improve privacy, security, and safety standards within logistics implementations of IoT.

Table 1 below provides a summary of the alignment of the primary research question to research sub-questions, method, and research objectives.

Table 1: Alignment of research questions, method, and research objectives

Research Question: How can the design of privacy, security, and safety of IoT devices used in e-logistics be improved?		
Research Sub-Question	Method/s	Research Objective
What is the operational definition of ethics and Ethics by Design within Information Systems?	Literature Review	To create an operational definition of ethics and Ethics by Design within Information Systems.
How can ethics be incorporated into the design of IoT?	Literature Review	To identify how ethics can be incorporated into the design of IoT.
How can Ethics by Design be employed to ensure privacy, security, and safety?	Data Analysis	To identify how Ethics by Design can be employed to ensure privacy, security, and safety.
What are the perspectives of logistics experts towards the utilisation of Ethics by Design within IoT devices in the logistics industry?	Data Analysis	To identify perspectives of logistics experts towards the utilisation of Ethics by Design within IoT devices in the logistics industry.
What recommendations can be made on how Ethics by Design can be utilised to improve the privacy, security, and safety standards within logistics implementations of IoT?	Findings	To make recommendations about how Ethics by Design can be utilised to improve the privacy, security, and safety within logistics implementations of IoT.

1.6 Literature Review

Technology is evolving at a rapid pace and contributing to the advancement of various businesses in multiple industries. This evolution of technology has brought about the adoption and utilisation of more Internet of Things (IoT) devices driven by various factors of advancement, improvement, and growth. Since its inception, IoT has become one of the largest business growth drivers, inadvertently contributing to the large growth of data otherwise known as big data. The nature of IoT has resulted in easier creation, collection, storage, and exchange of data. The growing realm of big data has sparked a new economy which has been the catalyst for the rapid evolution of technologies (Jurkiewicz, 2018).

Within the context of the exponential growth of IoT and IoT-related data, privacy, security, and other ethical concerns around IoT have arisen. These concerns include how user data is being used without consent. Therefore, this literature review identifies the privacy, security and related ethical concerns of IoT and big data, while also providing definitions and background into IoT and the big data paradigm. The intersection of literature that receives primary attention is literature that discusses how system (or computer) ethics relate to IoT devices.

1.6.1 Big Data Paradigm

Big data has become a concept that is interlinked with IoT because of the way IoT has developed and revolutionised business. IoT devices generate large volumes of data in various formats – structured and unstructured. In fact, many academics believe big data is the precursor of IoT. As big data is used in a range of applications, its definition has matured to contain three primary dimensions: velocity, volume, and variety. According to Ogbuke et al. (2020) big data can be described as high velocity, high volume and high variety of structured, unstructured and semi-structured information sets. On the other hand Dubey et al. (2018) define big data as the complex process of storing, retrieving and processing data using suitable algorithms to extract integral information to improve decision-making. The consensus amongst scholars is that big data focuses specifically on data that satisfies the factors of volume, velocity and variety whilst being used to make better informed decisions (Jurkiewicz, 2018; Ogbuke et al., 2020; Weinhardt, 2021).

Big data is a paradigm that has been used prolifically in supply chains and logistics industries (Ogbuke et al., 2020). This is particularly true of big data analytics, which can be used to improve the adaptability, agility, and alignment of business processes (Dubey et al., 2018). Additionally big data analytics has been adopted and employed in manufacturing to optimise, automate, and enhance the efficiency of processes.

1.6.2 Internet of Things

The concept of Internet of Things (IoT) has gained momentum quite recently in the business and IT worlds. The widespread development of IoT has grown profusely in the past few years and is resultantly impacting business greatly (Botterman, 2017). According to Chaudhuri (2017), IoT can be defined as the composition of billions of interconnected devices connected anytime and anywhere to a network. This definition of IoT has been agreed upon amongst various Information Systems academics and scholars (Allhoff & Henschke, 2018; Karale, 2021; Ustek-Spilda et al., 2019) This definition highlights the pervasiveness of IoT and its contribution to improving the integration between the real and digital world (Baldini & Botterman, 2018). In fact, due to the growth in interest in IoT, many companies in the supply chain and logistics industry have found themselves investing in these technologies. The most widespread uses of these IoT use cases in logistics are inventory tracking, fleet management, predictive analytics systems, drone-based delivery, and automated vehicles.

The rapid evolution and adoption of IoT has brought light to the growing concerns over IoT privacy, security, and ethics. As IoT has been so widely adopted within business and continually proves the benefits that data generating devices can add to processes, the security and privacy of end user data remains to be one of the biggest challenges and issues to date. Allhoff and Henschke (2018) go on to state that there is an intersection between privacy and IoT. This is because there are such vast amounts of data being shared and analysed. Hence, users may end up feeling disempowered through the use of IoT and because of the related misuse of their data (Allhoff & Henschke, 2018).

1.6.3 Ethical Design of IoT

The fast development of IoT, combined with the above-mentioned ethical concern around IoT data management, necessitates a discussion on Ethical Design within the context of IoT. In Information Systems the question arises whether IoT devices can potentially be designed to be more secure and handle data ethically as part of the devices' inherent design. Baldini and Botterman (2018) introduce this concept as IoT products and technologies that are designed and deployed to empower users. They go on to state that this concept is a new approach for users' interaction and empowerment through IoT. Peters (2017) agrees and mentions that Ethical Design is a relatively new concept with a focus on the technology engineering space. As this is still a novel approach, many designers have not adopted this notion in their designs of IoT.

Ethical Design is a concept with various meanings due to its novelty. According to Lapointe and Fishbane (2019) Ethical Design is a tool or approach for integrating the users' values and ethical intentionality into the design of technology. Karr (n.d.) states that it is an approach used to empower users by respecting human rights, human effort, and human experience. It is quite evident throughout various definition from literature that the main focus of this concept is the ethical usage of the devices. Fostering this approach in the design of IoT devices can mitigate conflict between stakeholders as well as promote user satisfaction (Baldini & Botterman, 2018).

1.6.4 Ethics by Design

Ethics plays an important role in the design of IoT and Artificial Intelligence technologies, primarily due to the impact of these technologies on our society (UNESCO, n.d.). Hence the term, Ethics by Design (EbD). Ethics by Design can be defined as the embedment of ethical principles and considerations into the process of designing and developing systems (Dignum et al., 2018). It can also be described as an approach that can be used to prevent ethical issues in the development stage of design. Chatila and Havens (2019) state that ethics by design focuses on how technology can be aligned with human values and norms. However, this concept raises the question of whether (relating to the feasibility and desirability thereof) machines and technology can be taught ethics.

However, this term differs from Ethical Design as it looks more at the enforcement of ethics in the technical design of systems and technologies. On the contrary, Ethical Design focuses on the designer's awareness of the ethical concerns of design. However, according to various academics, the relationship between these two concepts is the empowerment of users to control their personal data through the embedding of ethics in the algorithms of technologies (Baldini & Botterman, 2018; Dignum et al., 2018).

1.6.5 Ethics by Design as it relates to Information Systems

As ethics varies according to domains, it is important to identify the definition of Ethics in Information Systems, particularly in relation to IoT. The ethical dimension of Information Systems has attracted much attention amongst academics. Ethics in Information Systems has been defined by various scholars as a set of guidelines that govern the use of information towards moral good. According to Chaudhuri (2017), the main features of Ethics in Information Systems consist of information accuracy, information property, information privacy and information accessibility.

Similarly to computer ethics, Ethics in Information Systems is ethics incorporated in the design and use of IS (Santoro & Costa, 2021). The focus of this process to ensure ethics is built and embedded within systems to ensure the privacy, security, safety, transparency, and trust of technologies and systems thereof. Blair (2020) states that the use of technology is based on the pretence of trust, integrity, confidentiality, privacy, and security. All of which can be ensured by the integration of ethics within the design. This emphasises the importance of the need to integrate and adopt ethical principles with the system design of technologies.

According to Atlam and Wills (2020), ethics in the IoT discipline deals with regulating the correct behaviour of humans towards others. As ethics has had a great impact on the Information Systems discipline, it is evident that this concept has potential to affect the design of emerging technologies. This will in return lead to more socially responsible technologies and ethical outcomes (Baldini & Botterman, 2018).

1.6.6 Ethics by Design within the Logistic Environment

Ethics by design has become very prevalent in the design of IoT devices within the logistics industry. In fact, many logistics companies have found themselves investing in IoT devices to improve productivity, performance, and efficiency within various business processes. In addition to this, there is potential for IoT to accelerate data-driven logistics. With this advantage that IoT in logistics brings, the question arises: How should developers of these technologies design and act? (Chaudhuri, 2017). Hence, it is important to consider the ethical aspects that are prevalent in the design and development of these technologies. The greatest responsibility identified by many academics is to leverage the design of these technologies to bring about a positive impact on society. Consequently, Peters et al. (2020) state that integrating ethics by design and wellbeing into the design of logistics technologies can contribute to more successful and responsible outcomes.

1.7 Overview of Theoretical Framework

As this study focuses on Ethics by Design of IoT in the logistics industry, the study requires a design theory (or model) that can be used as guide when investigating ways of improving the embedding of ethics into IoT system designs. Designing systems that are private, secure, and safe requires an understanding of System Design as a discipline. However, it is imperative during the design to bring an ethical systems lens to simultaneously design systems that satisfy the ethical requirements expected of the system and allow the design of systems that are designed to be used ethically by end users. The use of an easy-to-understand design framework during the design of IoT systems would make it easier for designers to look at ethical considerations around a system and embed ethics therein during the development phases. A suitable framework that can be employed is that of Van Aken (2005). In this framework, a professional approach is used to guide the design of large and complex design processes. This approach can be used to embed the moral ground of privacy, security, and safety into the technology artefact (object), the implementation process (realization) and the environment in which the system exists (process) (Van Aken, 2005). In essence, these concepts can be identified as a representation of a system.

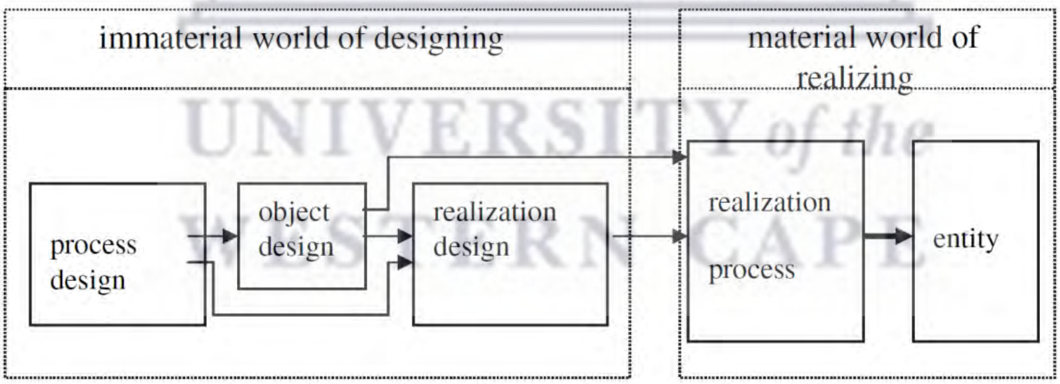


Figure 2: An object, realization, and process approach to system design (Van Aken, 2005)

Traditional approaches used in complex design processes have been proven no longer be sufficient (Van Aken, 2005). Many designers have, therefore, searched for a more professional approach to system design to guide the design process. A well-known and applicable framework that has satisfied these requirements is that of Van Aken (2005). This framework looks at providing a professional approach to design by categorising the process into object design, realization design, and process design.

1.7.1 Object, Realization, and Process Design

Object design can be defined as the design of the object or artefact, in this case the IoT devices. Once the design of the artefact has been created, the process of creating and producing said artefacts begins, namely realization design. Realization design is the act of configuring, drawing, and modelling the artefact. The last concept is process design, these are the activities involved with designing the process from the idea to realization to the responsibilities of each actor to execute this process. Van Aken's (2005) framework was, therefore, the most appropriate to guide the intentions of this study. This is because it provided a basis for dissecting "ethics by design" suggestions into the three main pillars. These offered a better means to gather and analyse the necessary information.

1.8 Research Design and Methodology

1.8.1 Research Design

The over-arching strategy used for this study was a survey. A survey can be defined as a design where data is collected from a sample of respondents to gain relevant information to compare, describe and explain their behaviour and attitude (Saunders et al., 2009). This design is classified as an empirical study as it utilises observations and measurements to arrive at the specified research outcomes. The reason for this choice of research design is because this study aimed to answer an exploratory question that can be linked to this research design. Additionally, this design was appropriate for this study as it intends to better understand individuals' perspectives towards ethics by design and this methodology was best to extract the relevant information and data.

The research paradigm that this study followed is that of interpretivism. Hence, this study is an interpretivist Information Systems study. This is a paradigm that focuses on how individuals understand and make meaning of information, especially if the data used for the investigation is respondents' qualitative perceptions (Sharma, 2009). This helps to reflect and identify the different aspects of a certain issue. Interpretivism was thus the most appropriate approach as it helped reveal the different interpretations from different individuals on this topic of study.

1.8.2 Unit of Analysis

According to Babbie and Mouton (2010) the unit of analysis can be defined as the what or whom that is to be studied. The unit of analysis for this investigation can be classified as individuals involved in the design of logistics related IoT devices, with expert knowledge of the privacy, security, and safety of such devices. These individuals, who were used in this study, are experts in the field of IoT and are employed at the case study organization, a private company in the logistics industry. Out of the 100 employees in the organization, 30 of them held positions as system designers, and I conducted surveys with 15 of these system designers. These selected individuals possess specialized knowledge in the domain of IoT and contribute actively to the design of logistics related IoT devices within the organization.

1.8.3 Research Instrument

A survey questionnaire was identified and selected as the best instrument to gather meaningful information from the participants. According to Saunders et al. (2009) a questionnaire can be defined as an instrument with a set of standardised questions used to collect data regarding a specific topic. Hence, the questionnaire utilised in this study consisted of qualitative, open-ended questions informed by the Van Aken (2005) theoretical framework. The design of the questionnaire was guided by the three main pillars of this framework, namely, object design, realization design, and process design. This framework guided the questions according to an individual's perceptions and attitudes towards the specific IoT technologies Ethics by Design approach. It will benefit this study by providing various interpretations of the different representations of the systems divided by the Van Aken (2005) framework.

1.8.4 Data Collection Technique

This study used a qualitative research method. Qualitative research is identified by the analysis of non-numeric data to gain an in-depth understanding of a social phenomenon (Saunders et al., 2009). With the adoption of this method, respondents are able to disclose their perspective and behaviour towards a concept without constraint (Palinkas et al., 2015). Hence, this was the appropriate method because the most relevant information from respondents was extracted to better understand their view on ethics by design. Furthermore, this study made use of survey questionnaires to gather the necessary information.

The survey instrument underwent meticulous development, iteratively identifying thematic domains guided by Van Aken's framework. Crafting questions followed, and a pilot survey with an Information Systems specialist ensured comprehensibility and assessed the instrument's consistency, validity, and replicability, enhancing its reliability and effectiveness.

1.8.5 Sampling Strategies and Techniques

This study used a non-probabilistic sampling method. This sampling entails a method where the researcher selects the intended sample dependent on the judgement of this researcher rather than a random selection (Babbie & Mouton, 2010; Saunders et al., 2009). This can also be defined as judgement sampling where the researcher selects cases based on judgement to answer the research question and objectives (Palinkas et al., 2015; Saunders et al., 2009). This sampling was used to gain a better understanding of specific individuals' perceptions pertaining to the topic. Using this sampling helped the researcher select the most appropriate candidates to provide the most relevant information for the study. In this study, the participants selected were experts within the organisation. These experts were information rich and had knowledge of the system design of the IoT technologies within their organisation.

1.8.6 Data Analysis

The qualitative data analysis approach employed in this study is content analysis, as recommended by Duriau et al. (2007). Content analysis involves coding qualitative information by identifying associations, links, and connotations. This methodology was deemed appropriate for the research, facilitating the identification and correlation of various themes and categories related to Ethical Design within the adoption of IoT. The choice of content analysis provided a systematic procedure to evaluate texts, offering insights into different perspectives on Ethical Design concerning privacy and security. In line with the suggestions by Zhang and Wildemuth (n.d.), the following steps were meticulously followed to analyze the data:

1. Preparation
   - Design and preparation of the survey instrument
   - Implementation of the survey for the Unit of Analysis (UoA)
   - Design of the coding procedure
2. Development of Categories, Themes, and Coding Scheme
   - Establishing categories, themes, and a coding scheme
   - Rigorous testing of the coding scheme
3. Data Coding Process
   - Coding of the collected data
   - Assessment of coding consistency
4. Drawing Conclusions and Reporting Findings

The data collected during this study underwent analysis using Atlas.ti, a robust research tool designed for coding and qualitative data analysis. Atlas.ti effectively manages, codes, organizes, and sorts through the collected data, enhancing the rigor and comprehensiveness of the analysis process.

1.9 Location of Study

For this study, the organisation's employees were used as the unit of analysis. This organisation is a global provider of fleet and mobile asset management solutions. It operates in Cape Town, South Africa. Within this company, the researcher selected multiple cases based on the judgement of the topic of Ethics by Design in Logistics. These participants are experts in their fields of study, hence ensuring that a well-rounded group of answers was collected.

1.10 Assumptions and Limitations

In this study, one of the main assumptions was the unit of analysis, specifically the individuals undertaking the survey. The assumption made was that the sample of individuals understood what ethics by design is and how it is utilised and applied in the system design. This was assumed during the collection of data and analysis thereof. Additionally, one of the limitations of this study was experienced during the collection of data. Due to the intent of the study, many individuals were afraid to provide their true insights towards concerns in their workplace. They did not want to expose any unnecessary issues within their organisation. This affected the data findings of this study. Hence, it is important for this study to acknowledge and be aware of these limitations and assumptions.

1.11 Ethical Considerations

In this study, data was collected through the use of a survey questionnaire. These questionnaires were administered online to the selected participants of this study. Before the surveys were undertaken, the researcher ensured that all participants were anonymous and consented to being a part of this study. Ethically, the researcher committed to upholding the values of integrity, honesty, confidentiality, openness, and objectivity throughout the collection and analysis of this data.

1.12 Chapter Outline

In this chapter, an introduction into the research problem was provided as well as the research question this thesis intends to answer. The following chapter will further provide a more intensive literature review interrogating all the main topics.

Chapter 2: Literature Review

2.1 Introduction

As discussed in Chapter 1, despite there being large societal impacts in the development of technologies, specifically IoT, there has been minimal academic literature on Ethics within IoT systems. However, there is a growing amount of literature regarding the areas of Information Ethics, Computer Ethics and Ethics itself. In Chapter 1 the literature review focused on definitions from literature, whereas this chapter delves deeper into the topic of this research study. This literature review will therefore, review further explains these concepts, as well as focus on how the ethical issues of privacy, security, and safety can be embedded in the design of systems in the logistics industry.

2.2 Ethics

The current adoption and utilisation of IoT and big data has been accompanied by the calls for the application of ethics within IoT design (Jurkiewicz, 2018). This has brought more attention to the concept of ethics as it relates to technology devices. However, there has been an ongoing debate within the field of ethics in research, especially surrounding the unified definition thereof. Hence, the literature regarding ethics is still maturing (Weinhardt, 2021). Ethics is a diverse notion that has conjured up various definitions in multiple fields. Ethics, as a discipline, is concerned with the moral philosophy of right and wrong behaviour (Allhoff & Henschke, 2018; Baldini & Botterman, 2018; Hagendorff, 2020; Jurkiewicz, 2018). It is concerned with the interest of society and what is deemed to be morally correct and incorrect (Hagendorff, 2020). Chatila and Havens (2019) go on to state that ethics go beyond the moral constructs of right and wrong, and also focuses on the issues of environmental sustainability, social fairness, and transparency. This concept is widely covered by various academics and has been identified in multiple disciplines, namely computer ethics and information system ethics.

2.3 Computer Ethics

As described in the previous section, Ethics is a concept that has multiple meanings according to the different application domains. There is a limited understanding of ethics in the world of technology. Computer ethics is a field where scholars start to create a better understanding of ethics more related to technology. Computer ethics is another domain that falls under ethics, that is concerned with the morals and ethics towards technology and computers. Masrom et al. (2011) describe computer ethics as ethical policies that govern the utilisation of computing technology. These policies guide individual actions towards what is morally right and wrong. They go on to state that there are multiple ways to incorporate the ethical approach into technology and computing. These ways consist of considering the concept of ethics as a continuous and dynamic enterprise, establishing and creating effective relationships between ethicists, scientist and technologists and developing and using more ethical analyses. Moor (1985) continues to describe computer ethics as the social impact of technologies and the consideration of social policies for the ethical use of these technologies. The ethics concerned in the discipline of computers can be technical. However, this study focuses more on ethics in systems – specifically Information Systems (IS).

Santoro and Costa (2021) argue that typical situations involving both system design and the use of IS should incorporate ethics through well-designed processes, ensuring the development of ethical systems as well as the utilisation of a more ethical approach. However, the acceptance and use of ethics in design is solely up to the IS designer. Hence there is a need for more designers in the IoT field to understand the fundamental role they play when designing and using IS to satisfy the diverse socio-cultural contexts. This is also known as ethics by design.

2.4 Information System Ethics

There is a new and more recent narrative about ethics as it relates to technology. This field of study is called Information Systems Ethics. Ethics is a process that has also been identified to be used in information systems. Similarly, to computer ethics, ethics in information systems is ethics incorporated in the design and use of IS (Santoro & Costa, 2021). The focus of this process to ensure ethics is built and embedded within systems to ensure the privacy, security, safety, transparency and trust of technologies and systems thereof. Blair (2020) states that the use of technology is based on the pretence of trust, integrity, confidentiality, privacy and security. All of which can be ensured by the integration of ethics within the design. Hence, the importance to integrate and adopt ethical principles with the system design of technologies.

2.4.1 Information Systems Ethics Concerns

Through the analysis of literature, there has been various questions raised regarding the ethics and moral aspects of the design of information systems technologies and artefacts. These questions can be divided into two aspects namely the extent to which information systems embed moral values which have an impact on the society and designing systems that will embody positive standards and avoid moral dilemmas (Paradice et al., 2018). These topics can be illustrated in the works of Brey (2017) and Introna (2005). Paradice et al. (2018) concludes by stating there are various debated list of issues concerning the application of ethics in information systems namely intellectual property, privacy and personal information, freedom and censorship, safety and security and globalization. However, this study we purely focus on that of privacy, security and safety.

2.5 Privacy

The public awareness of privacy risks within various technologies has increased due to the digital working and living spaces general citizens find themselves in. According to Karale (2021), privacy focuses on the freedom from interference and limitations of admittance to one’s space. In relation to information and technology, privacy is defined as the right of users to have control of how their data is used and collected (Lei Xu et al., 2014). Many of the major data privacy concerns are focused and related to data collection, data storage, data usage, and data access (Gimpel et al., 2018). The violation of a user’s privacy can lead to potentially adverse effects, hence it is important to mitigate these risks.

Various academics mention recommendations to reduce the risk of data privacy concerns, but the most commonly identified recommendation is protecting customers privacy through laws and regulations. Examples of this include the Protection of Personal Information Act (PoPIA) and General Data Protection Regulation (GDPR). (Gimpel et al., 2018; Lee & Hess, 2022; Lei Xu et al., 2014). The PoPIA is legislation designed to regulate and protect how personal information is stored, processed and transmitted by both public and private bodies (Kandeh et al., 2018). The main goal of this Act is to ensure the privacy of users' personal information, additionally preventing the loss, damage, and theft thereof.

2.6 Security

The security of devices can be considered one of the greatest concerns when designing and implementing new technologies. Securing these technologies should be considered a priority when guaranteeing the secure nature of these devices. Hence, this insurance can ensure the users trust that their data is well and effectively secured (Karale, 2021). Security in relation to IoT can be defined as the safeguarding and securing of devices to protect against any threats and breaches (Allhoff & Henschke, 2018). Additionally, it can also be defined as the implementation of protocols, strategies and technologies aimed at safeguarding IoT devices, networks, data, and applications from unauthorized access, cyberattacks, and breaches (Azam et al., 2019). Security measures in IoT include authentication, encryption, access controls, intrusion detection, and secure communication protocols, all of which contribute to protecting IoT ecosystems from potential threats (Azam et al., 2019; Zanella et al., 2014).

2.7 Safety

As with privacy and security, safety is a factor that has been in the spotlight when talking about ethical concerns of newer technologies. According to Atlam and Wills (2020), the safety of IoT can prevent physical damage and the risk of damage to the system and its components. Safety is the prevention of undesirable threats and protection against the surrounding environment. The concept of safety extends beyond the protection of devices and data; it also includes the prevention of unintended behaviour, system failures, and the safeguarding of the overall environment. Allhoff and Henschke (2018) add to this definition by stating the biggest factor of safety is the prevention and mitigation of physical harm. In fact, it is important to note that safety and security work hand-in-hand and are integrated together. Hence, any solutions to these challenges can positively impact both safety and security. An example of safety in IoT systems is the monitoring of the conditions of machinery to prevent accidents or utilizing sensors to detect and mitigate hazardous conditions (Atlam & Wills, 2020).

2.8 Privacy, security, and safety in Information Systems

The field of ethics is very broad and can span across various disciplines. However, this study focuses mainly on how the study of moral values applies to systems. The systems being described is that of Information Systems. Information Systems, in its wholeness, focuses on system components that collect, process, store and distribute information (Stahl et al., 2014). This field of academic research has considered the importance of ethical principles needed to ensure the satisfaction of users and what is considered right and wrong. In fact, the main goal of ethics in Information Systems is to embed ethical principles to improve the social impact of technology. Hence, the users of these technologies have a great impact on the acceptance thereof. The social acceptance of any technology is strongly dependent on the trustworthiness and protection of data (Atlam & Wills, 2020). Due to the complexity of these technologies, they face various challenges of security, safety, and privacy. The purpose of addressing these technologies is to instil trust within the users.

2.9 Privacy, security, and safety in Internet of Things

This study focuses specifically on privacy, security, and safety as it relates to Internet of Things. The rapid growth seen in the adoption and use of IoT has brought about various changes within multiple industries. This fast-paced change has brought to light several factors; factors which should be priority to those designing this technology. Some these factors consist of privacy, security, and safety as mentioned above (Allhoff & Henschke, 2018). These are ethical issues raised by users thereof.

2.9.1 Internet of Things

The Internet of Things (IoT) can be described as the system of interrelated devices and technologies connected and exchanging data over the internet (Burhan & Rehman, 2018). The main goal of these technologies is to automate work and connect devices via the internets to communicate with each other. These technologies can also be identified as an enabler that increases efficiency within various areas namely manufacturing, logistics, health and transport (Maple, 2017). The complex scale of this technology has led to the awareness of various issues and challenges faced by developers.

Due to the intricacy of technologies, various architecture frameworks exist. These architecture frameworks vary slightly amongst academics. However, they agree when it comes to three main layers namely the application layer, the network layer and the perception layer (Burhan & Rehman, 2018). According to Sethi and Sarangi (2017), this is the most basic architecture introduced in the early stages of research. This study used this architecture to gather information regarding privacy, security, and safety issues within each layer of IoT.

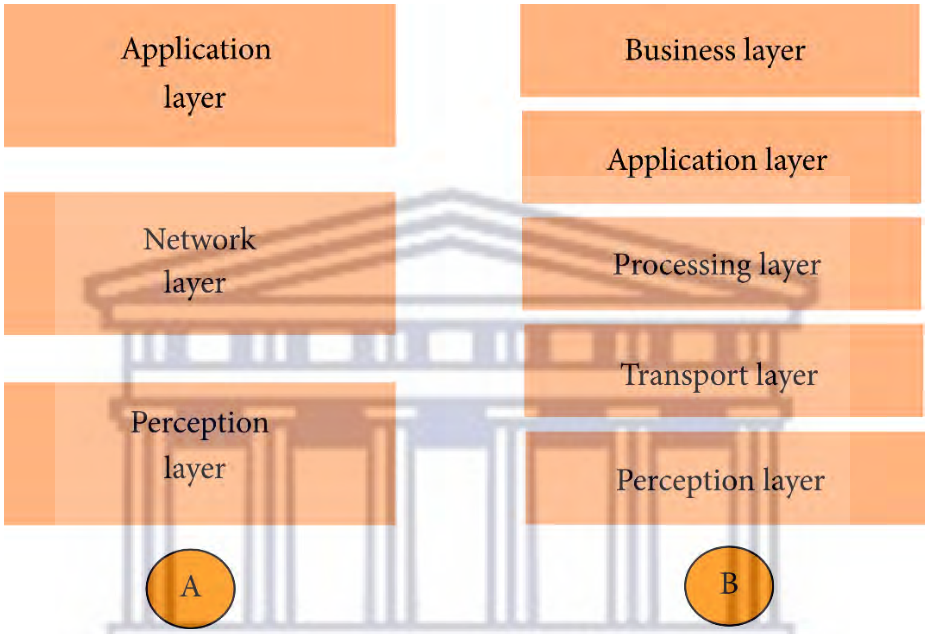


Figure 3: IoT architecture layers (Sethi & Sarangi, 2017)

2.9.2 IoT Privacy

The last few years has seen the growth in technology and integration of IoT devices in various organisations. This growth has led to more and more companies investing in IoT to connect to broader networks and achieve extensive functionalities. However, this growth has brought attention to multiple challenges and concerns about securing the data and protecting systems. Due to the disruption in technologies, there has been an increase in hackers, cyber criminals and system attacks. Atlam and Wills (2020) state that IoT privacy can be divided into four main elements: information, territory, body, and communications. The greatest threat relates to information and the risk of losing control over personal data (Alfandi et al., 2021).

Some common privacy threats listed by Atlam and Wills (2020) consist of profiling, localisation and tracking, inventory attacks, linkage and identification. These threats are mainly concerned with the vulnerability of users' identity and location and the disclosure of private information. According to Alfandi et al. (2021) these threats boil down to the main concepts of availability, confidentiality, integrity and authentication. This is the case for security threats as well.

As these threats are concerning for the users, there are solutions that can be implemented to preserve the privacy of IoT devices. In fact, these concerns are not only alarming for the users but also for the designers as it could impact the development and adoption of these technologies. Some of these approaches consist of Privacy by Design techniques – privacy awareness, data minimisation, access control, data anonymisation and cryptographic techniques (Atlam & Wills, 2020). In addition to these approaches, Seliem et al. (2018) state that utilising a framework or architecture in the design of IoT technologies can preserve the privacy. Frameworks mentioned consist of that of Langheinrich (2002) – the privacy aware System, a privacy preserving framework for smart homes courtesy of Bagüés et al. (2007), and a decentralised architecture by Seong et al. (2010).

2.9.3 IoT Security

The privacy and safety of IoT are concepts that are interlinked and closely related. These concepts have the common features of availability, confidentiality, integrity, and authentication. Additionally, Atlam and Wills (2020) make mention of the need for IoT security to instil trust in users. The way in which this can be achieved is by ensuring the common features mentioned above are integrated into the design.

There are numerous security threats and dangers throughout the various layers of IoT. The layers being the Sensing layer, Network layer, Middleware layer and the Application layer (Azam et al., 2019). These layers of IoT all have the potential to be attacked through loss and theft, physical damage, unauthorised access and integral loss of information. Mena et al. (2018) state that some of these threats include eavesdropping, booting attacks, phishing, access attacks, routing attacks, data theft, node catching and RF Jamming (Alfandi et al., 2021; Atlam & Wills, 2020; Azam et al., 2019; Mena et al., 2018).

Securing IoT is a practise that all designers should be incorporating into the early stages of their system design processes. The security of these technologies, can help protect, identify, and monitor risks. Some of the best practises of security IoT consist of strong authentication, firmware updates, tamper resistant hardware, device identity spoofing and dynamic testing (Atlam & Wills, 2020). In addition, one of the commonly used concepts regularly used by academics to practise securing IoT is that of Security by design. This concept is concerned with providing principles and approaches to make systems free of vulnerabilities to attacks (Guggenmos et al., 2022). Guggenmos et al. (2022) states that the early introduction of this approach in system design can create a widespread understanding of security requirements to help effectively integrate into IT project management and IS Strategic alignment. In return, this ensures safe IoT devices.

2.9.4 IoT Safety

IoT safety is one of the highest contributors to the prevention of physical damage and undesirable threats to the IoT system (Atlam & Wills, 2020). Just as the privacy and security of IoT's main goal is to impart trust in the users, the same goes for the safety. In fact, many academics argue that trust is reliant on the ethical issues of privacy, security and physical safety (Allhoff & Henschke, 2018; Atlam & Wills, 2020; Karale, 2021). The safety in IoT is mainly concerned with the detection and prevention if unintended or unexpected behaviour (Agarwal & Dey, 2016). Safety and security are integrated together in the product life cycle, hence the improvement of IoT security can enhance the security of IoT.

Various academics have created a correlation between the concepts of trust and safety (Atlam & Wills, 2020; Karale, 2021). The social acceptance of IoT technologies is highly dependent on the trustworthiness of data and the protection thereof. Hence, there is great demand to satisfy the requirements of trust. A survey by Allhoff & Henschke (2018) concluded that the issue of trust, security and safety exist in concatenation and are integrated together. Additionally, Chatterjee (2020) hypothesises that if the trust in users grows, so will the safety of IoT devices, thus positively impacting the adoption of IoT. Resultantly, there is a potential for trustworthiness in data and IoT to ensure safety and security.

2.10 Privacy, security, and safety in IoT logistics

2.10.1 IoT in Logistics

IoT has greatly impacted the logistics industry. Many organisations have found numerous benefits in the adoption of these technologies. As mentioned above, there are great risks that lie in the adoption and utilisation of IoT, primarily related to privacy, security, and safety. The researcher discussed these ethical concerns in IoT devices and will now discuss how privacy, security, and safety are related to IoT used in a logistics environment.

However, it is important to first understand the concept of logistics and how IoT can be used to improve productivity within. Logistics can be defined as the science of managing the mobility of people and the flow of production and distribution (Greenblatt & Hart, 2012). Within this logistics production flow, there are new possibilities for IoT to improve performance (Witkowski, 2017).

Due to the complexity of logistics processes, there are benefits associated with the extensive implementation of IoT devices. These devices can significantly impact the storage, warehousing, transportation and inventory management of these processes (Tu et al., 2018). With these benefits, comes challenges and risks namely the privacy, security, and safety. Mentioned below are the concerns related to IoT specifically, however there are more specific risks and threats related to the logistics environment.

The digitisation of logistics processes and services has been advanced through the application of IoT. IoT, used throughout the whole process of logistics, has made it easier to monitor each phase and automate processes for more efficiency. These technologies have impacted various parts of the logistics cycle, but this study was purely focused on the devices used within cargo and fleet management. Some technologies used in cargo and fleet are remote sensors monitoring temperature and humidity, and Global Positioning Systems (GPS) monitoring and locating cargo, fuel usage controls, sensors detecting driver behaviour and trackers for the detection of fluid levels (Tu, 2018). The table below provides a description of each of these IoT devices with a diagram.

Table 2: IoT devices

IoT Devices	Image	Definition
Sensors	Rugged IP-67 rated Perfect for large and small non-powered assets Self-install battery powered device Long battery life up to 5 years	The smaller devices are utilised and installed in the necessary asset to determine and monitor humidity, temperature, driver behaviour (Tu et al., 2018)
Global Positioning System		This a satellite based system that provides navigation, timing services and positioning. (Tu, 2018)
Drone-based delivery system		These drones are created to speed up and automate deliveries by navigating and delivering packages to the defined location (Tu, 2018)

2.10.2 IoT in e-Logistics

Literature provides us with various definitions of the term e-Logistics. e-logistics can be defined as the digitalization and automation of logistics processes through the integration of advanced technologies such as the Internet of Things (Burhan & Rehman, 2018). E-logistics can also be defined as management of physical flows for organizations engaged in online sales, involving not only the delivery processes for products purchased online to customers but also the utilization of web-based technologies and cloud computing infrastructures to optimize operations (Burak, 2022). In this study, our working understanding of the term e-logistics spans broader than supply chain applications and include the digitization and automation of non-retail related logistics activities. This approach with e-logistics provides various benefits to organizations namely improved efficiency, real-time tracking, and enhanced decision-making. However, along with these benefits comes significant concerns regarding privacy, security, and safety. Privacy concerns arise from the extensive collection and sharing of sensitive data among various stakeholders in the supply chain, potentially leading to unauthorized access, misuse, or breaches (Kandeh et al., 2018). Security issues include the vulnerability of interconnected systems to cyberattacks, data breaches, and unauthorized tampering, potentially disrupting operations (Azam et al., 2019).

Additionally, safety risks involve the physical and operational well-being of human resources, assets, and goods, as system failures or cyberattacks could compromise the safe operation of logistics processes (Somasundaram, 2019). As the e-logistics industry continues to evolve, it is essential for organizations to address these concerns to ensure the successful implementation and sustainable growth of digitalized logistics systems.

The integration of the Internet of Things (IoT) into e-logistics has completely changed the landscape of supply chain management, altering how we interact with and optimize logistics processes. The greatest benefit of IoT lies in its ability to connect and communicate with multiple devices and systems via the internet, facilitating the interchange of real-time insights and data (Burhan & Rehman, 2018). This means that assets, trucks, warehouses, and even goods can be equipped with sensors, cameras, and tracking devices, creating a interconnected network that enables precise monitoring, predictive maintenance, and increased decision-making (Somasundaram, 2019). However, as IoT adoption expands, so do worries about privacy, security, and safety. The data generated by IoT devices can be sensitive, raising privacy issues, while the connectivity of devices opens the door to potential cyber threats and unauthorized access (Kandeh et al., 2018).

2.10.3 IoT in Cargo and Fleet

Fleet and cargo management is a practice that is concerned with the coordination and management of vehicles and cargo (Monnerat et al., 2019). Many e-logistics organisations practise fleet management to maximise efficiency, improve safety and drive productivity. This practice is optimised by the utilisation and adoption of IoT technologies to improve these processes. In fact, IoT promotes machine to machine communications by ensuring connected vehicles. Some of these technologies used in this case are sensors, cameras and GPS (Killeen et al., 2019). However, the privacy, security, and safety of these devices are issues of concern. Ensuring the privacy of drivers anonymity when driving vehicles, the safety against theft of cameras and sensor on the vehicles, and securing private data against attacks and thefts are a few of these concerns (Akram et al., 2017).

2.10.3.1 Use cases of IoT in cargo and fleet

Monitoring and measuring the fuel spent, condition of the vehicle and driver behaviour are a few use cases of IoT in fleet management. These devices monitor the condition of vehicles like the coolant level, tire pressure and suggested failures (Somasundaram, 2019). Having this data makes it easier for organisations to plan and prepare for scheduled maintenance on their assets. However, there are plenty of risks that can be associated with these devices namely privacy, security, and safety. Another common use for IoT in cargo and fleet is that sensors track goods. Some of these sensors consist of Automatic Identification and Data Capture (AIDC) and Radio Frequency Identification (RFID). These sensors use radio waves to determine the positioning of the cargo/goods.

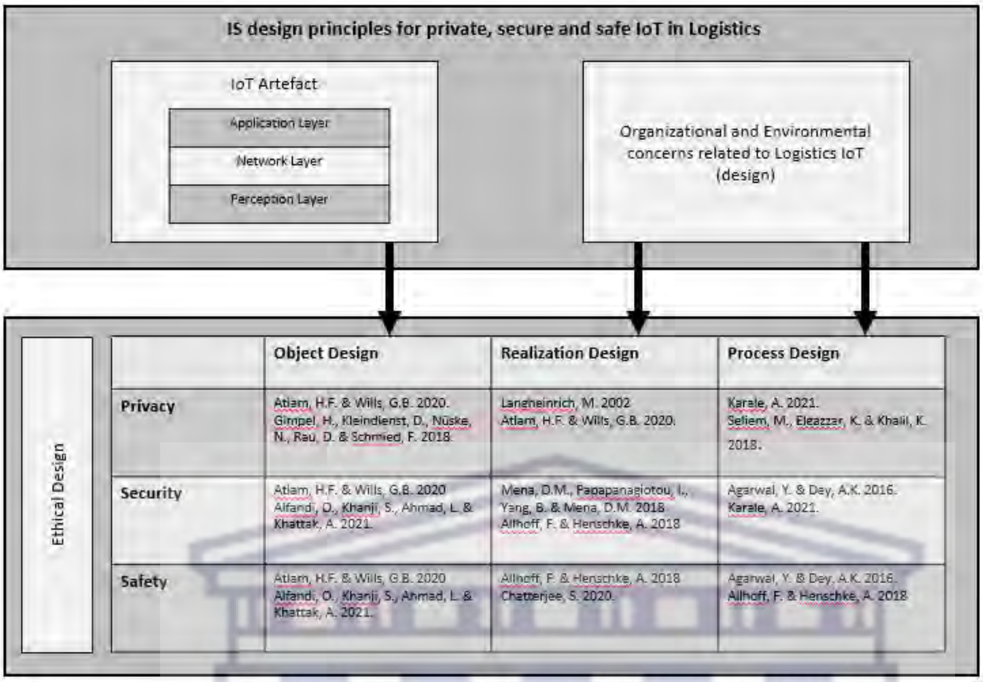
2.10.3.2 Typical privacy, security, and safety concerns in cargo and fleet

Whilst fleet and cargo management can greatly benefit various industries, there are multiple concerns regarding the privacy, security, and safety thereof. Specifically within the wide array of functions it involves namely the safety of vehicles, financing, maintenance, telematics and managing fuel, speed, and drivers (Somasundaram, 2019). Due to the large amount of data being generated by this practise, there are typically great concerns regarding cybercrimes and cyber threats. These concerns are particularly regarding the data getting in the wrong hands. These crimes can have serious consequences for the business, customer accounts, asset locations, confidential information and shipments (Somasundaram, 2019). Additionally, the vulnerability of IoT in fleet management practises to hacking has also seen a lot of growth (Rane et al., 2021).

2.11 A Framework for Designing IoT Logistics devices that are private, secure, and safe

As argued in this study, ethics and system design are two factors that need to work together in order to satisfy social morality and moral boundaries. This is the thinking behind the requirement to incorporate Ethics by Design into the development of systems and technologies. However, when incorporating Ethics by Design into the design of systems, a framework is necessary to guide this process. The framework that has been utilised is that of Van Aken (2005).

The framework of Van Aken (2005) is appropriate for this study as it helps to separate the development of a system into categories, to better help integrate the ethical concerns of privacy, security, and safety. Through the analysis of the literature, it has been identified that these concerns can be seen in each of these categories, namely object, realization, and process. It is therefore essential to classify recommendations that can be made on how ethical design can be utilised to improve the privacy, security, and safety standards within logistics IoT. To summarise, this study has utilised the knowledge of Van Aken and bridged the gap between IS, ethics and system design by creating a conceptual framework that is visualised below.


IS design principles for private, secure and safe IoT in Logistics
IoT Artefact
Application Layer
Network Layer
Perception Layer
Organizational and Environmental concerns related to Logistics IoT (design)
Ethical Design

	Object Design	Realization Design	Process Design
Privacy	Atlam, H.F. & Wills, G.B. 2020. Gimpel, H., Kleindienst, D., Nüske, N., Rau, D. & Schmied, F. 2018.	Langheinrich, M. 2002 Atlam, H.F. & Wills, G.B. 2020.	Karale, A. 2021. Seliem, M., Elgazzar, K. & Khalil, K. 2018.
Security	Atlam, H.F. & Wills, G.B. 2020 Alfandi, O., Khanji, S., Ahmad, L. & Khattak, A. 2021.	Mena, D.M., Papapanagiotou, I., Yang, B. & Mena, D.M. 2018 Allhoff, F. & Henschke, A. 2018	Agarwal, Y. & Dey, A.K. 2016. Karale, A. 2021.
Safety	Atlam, H.F. & Wills, G.B. 2020 Alfandi, O., Khanji, S., Ahmad, L. & Khattak, A. 2021.	Allhoff, F. & Henschke, A. 2018 Chatterjee, S. 2020.	Agarwal, Y. & Dey, A.K. 2016. Allhoff, F. & Henschke, A. 2018

Figure 4: Conceptual framework

2.12 Chapter Summary

This chapter provided an intensive review of privacy, security and safety in Information Systems, Internet of Things and logistics. This literature review discusses and interrogates previous studies on this topic and highlights the gaps in literature this research aims to address. The following chapter will provide more insight into the methodology utilised to conduct this study.

Chapter 3: Research Methodology

3.1 Introduction

The following chapter provides and describes the methods and approaches used in this study to answer the main research problem. This provision of data is organised according to the image provided below.

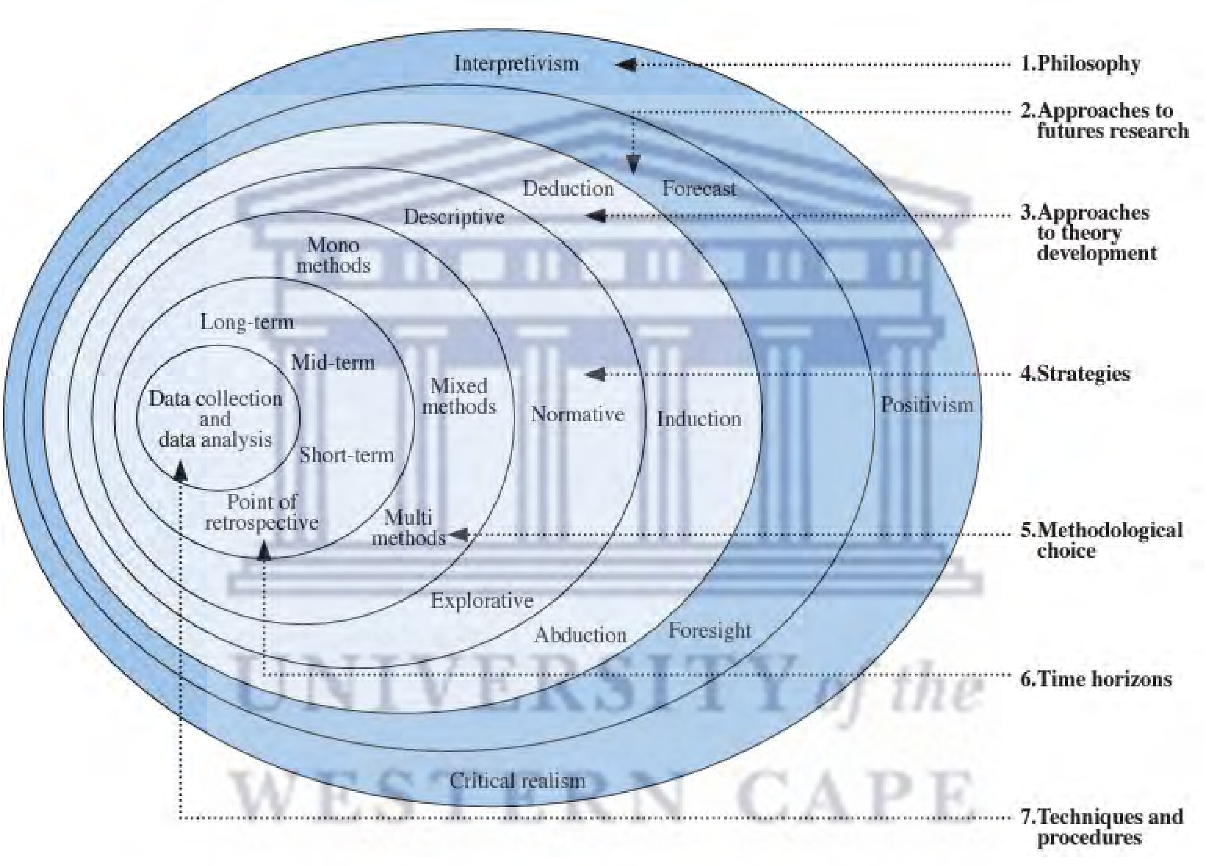


Figure 5: The research onion (Saunders et al., 2009)

3.2 Philosophy

It is important to identify the research philosophy of a study to better understand the development of knowledge during the study itself. It can be defined as the nature of a study or development thereof. The importance of this concept is to reveal the assumptions and choices made during the research. There are multiple philosophies in the research environment, namely positivism, realism, interpretivism, pragmatism.

Positivism can be defined as an approach where the knowledge is solely dependent on empirical evidence. In other words, this theory's positioning can be classified as a natural scientist. Additionally, this theory focuses on observing social reality to develop a hypothesis for the production of credible data (Saunders et al., 2009).

Realism is similar to positivism as it relates to scientific enquiry. This theory focuses on a scientific approach to the development of knowledge where the reality is independent of the mind (Saunders et al., 2009). This theory is split into two categories, namely direct and critical realism.

Pragmatism is another philosophy that can be defined as a theory where beliefs and actions are judged against the outcomes. This theory focuses on practical considerations and knowledge rather than theoretical ones.

However, the philosophy this study undertook was that of interpretivism. Interpretivism can be defined as a theory where knowledge is gained from collecting and interpreting social actors' thoughts, understandings and meanings (Saunders et al., 2009). This interpretation of the social roles of actors will contribute to a larger set of knowledge. This philosophy is appropriate for this study as the truth of this study's research problem lies within the minds of IoT experts who work with these technologies, specifically, individuals who work in and with fleet and cargo management technologies. This study interpreted these individuals' thoughts towards how privacy, security, and safety of IoT devices used in e-logistics could be improved.

3.3 Approach

There are two approaches that can be taken in research namely deductive and inductive. Deductive research can be associated with scientific research. This approach looks at deducting from existing knowledge. A theory and hypothesis are created in which the result is deducted from existing knowledge and research. On the other hand, inductive research focuses on collecting data and creating and developing theory and knowledge. In this study, a deductive approach was used to further expand the knowledge of privacy, security, and safety of IoT devices based on existing research and literature. Due to the vast knowledge on this particular research topic, this study will further contribute to the body of information by providing recommendations on how Ethical Design can be utilised to improve the privacy, security, and safety within logistics implementations of IoT.

3.4 Strategy

The research strategy is a well-organised plan a researcher takes to give direction towards conducting research (Saunders et al., 2009). The choice of a strategy is dependent on the research question and objectives. Due to this study focusing on improving privacy, security, and safety in IoT logistics environments, and this being classified as an exploratory question, the most appropriate strategy is that of surveys (Babbie & Mouton, 2010). Surveys can be described as studies that are either qualitative or quantitative in nature and aim to collect relevant knowledge to represent a sample of a larger population. This strategy is most appropriate for this study as a smaller sample of experts in the IoT Logistics field were questioned and the results gathered helped describe the characteristics of the larger population. Additionally, the results gathered helped provide recommendations of how to improve privacy, security, and safety to the larger population working with similar IoT devices.

3.4.1 Instrument development

The development of the survey instrument aimed to optimize the extraction of data from participants and underwent a comprehensive iterative development process. The initial phase encompassed the identification of the thematic domains in relation to the research objectives. The construction of these questions was guided by the framework of Van Aken. Once the questions were crafted, a pilot survey was administered to an independent specialist in the Information Systems field, aimed at ensuring its comprehensibility and ease of response. This pilot phase served to evaluate the instrument's consistency, validity and replicability as a data collection method.

3.4.2 Sampling

The sample surveyed consisted of individuals recognized as experts of IoT in the Logistics environment. The reason for this choice of sample, was that they were most representative of the larger population or closely aligned to the broader population of interest. The sampling approach adopted in this study was that of purposive sampling. This is a method where sampling in on the basis of the researcher's knowledge of the population (Babbie & Mouton, 2010). Through this method, a selection of 15 participants were chosen based on the researcher's informed understanding of the population. This entailed the careful evaluation of IoT experts against predefined criteria, leading to the inclusion or exclusion of individuals as participants.

The sample selection incorporated the principle of data saturation, which refers to the point in a study where gathering fresh data ceases to yield distinctive insights. Within the scope of this research, it has been observed that attaining data saturation typically necessitates around 15 in-depth surveys, indicating that conducting additional surveys pertaining to the same implementation beyond this point is unlikely to yield different findings. (Guest, Bunce & Johnson, 2006)

By utilizing this purposive sampling technique, which is commonly employed in applied research, the study aimed to enhance the validity and reliability of the gathered data. The selection of this sampling technique is grounded in the context of applied research, which is characterized by its emphasis on addressing real-life applications and challenges. According to Riege (2003), validity refers to how well an instrument measures what it is intended to measure. Additionally, Riege (2003) refers to reliability as the consistency of findings across various studies and researchers. By focusing on the identified experts in the information systems field, this contributed to the content validity. Additionally, the deliberate selection process of the sample strengthens the construct validity, as the identified participants possesses the necessary expertise to provide accurate and informed responses.

Additionally, to ensure content validity, the survey instrument underwent a review process by IoT experts. The survey questions were carefully aligned with the research objectives and existing theoretical frameworks of Van Aken. Furthermore, a pilot study was conducted with a IoT expert to assess the clarity and comprehensibility of the survey items. In the data analysis phase, any discrepancies or outliers were carefully examined and cross-referenced with existing literature to mitigate potential threats to construct validity.

In relation to the reliability, it is important to note that the choice of participants was targeted and deliberate. It is credible that if different individuals were chosen as respondents for the questionnaire, the underlying themes and insights highlighted may still have been consistent. This suggests that the results of this study are not solely dependent on the specific participants but are more likely reflective of the IoT within the Logistics domain.

In order to facilitate replicability of the study, the research design and data collection procedures were documented. The primary data collection method employed was a survey questionnaire distributed among a purposively sampled group of experts in the field. The questionnaire items were adapted from established scales and validated instruments in the IoT field, ensuring a standardized approach. Furthermore, the qualitative content analysis process followed a systematic coding procedure, guided by recognized coding schemes, which enhances the potential for future replication

3.5 Choices

When conducting a research study, it is important to identify the method or choice to guide the way in which the data is collected and analysed. There are three choices that can be chosen from, namely mixed method, mono method, and multi-method. These choices are dependent on whether the study will be using a single data collection technique or more than one data collection technique to answer the research question (Saunders et al., 2009). Due to this study collecting and analysing qualitative data, the method utilised was the mono method. That was the best method when answering the research question and objectives via the analysis of qualitative data.

3.6 Time Horizons

Time horizons in research answers the question of whether the researcher wants their research to be a snapshot of time or a representation of various events over a longer period (Saunders et al., 2009). According to Melnikovas (2018), time horizons can also be defined and described as the time frame of the specific research. For this research study, the time horizon was cross sectional. Cross-sectional studies can be described as the study of an event or phenomenon over a period of time (Saunders et al., 2009). It can also be described as studying a population at a single point in time and not over time. The reason for this choice of study was due to time limitations and the idea that the most accurate data and knowledge gathered would be from collecting data from IoT logistics experts in a single point of time.

3.7 Techniques and Procedures

As mentioned in previous chapters, this study collected qualitative data. This research instrument consisted of various qualitative open-ended questions, and well as a few quantitative questions. The qualitative data was analysed using qualitative content analysis. This approach can be described as a method for searching across qualitative data to analyse, identify and report on identified repeated themes (Kiger & Varpio, 2020). Additionally, this approach focuses on identifying themes that address the research problem and question. The reason for this choice of analysis was because of the flexibility in interpreting the data as well as the identification of themes to coincide with Van Aken's framework. Hence this approach allowed for the analysis of data into the main pillars of Van Aken's framework, namely object design, process design, and realization design.

The application of qualitative content analysis to the data followed a dynamic and iterative process. Initially, the data underwent a stage of comprehensive preparation, involving familiarising the data to gain an overall understanding of the content. This data was then prepared and organized for analysis. This was followed by the coding phase of the data, during which significant segments of information were labelled using key concepts, themes, and ideas. Following the completion of coding, this coded data was grouped into categories based on shared attributes. This categorization process laid the groundwork for the identification of overarching themes and patterns, all of which was managed within the software framework of Atlas.ti. Within Atlas.ti, the data was organized and presented into the necessary mind maps according to the overarching themes. Upon the conclusion of the analytical work within Atlas.ti, the findings were developed through drawing connections between the research objectives and the pivotal subjects underpinning the study.

3.8 Chapter Summary

In this chapter, the research methodology utilised was discussed. This can be summarised into the below table 3. The following chapter will present the finding collected and propose design principles to answer the research question.

Table 3: Research Methodology

Research Methodology	
Philosophy	Interpretivism
Approach	Deductive Approach
Strategy	Survey
Choices	Mono Method
Time Horizon	Cross Sectional
Techniques and Procedures	Qualitative Content Analysis
Research Instrument	Survey Questionnaire
Sampling Strategy	Judgement Sampling

Chapter 4: Data Findings and Discussion

4.1 Introduction

This chapter focuses on answering the main research question of how the design of privacy, security, and safety of IoT devices used in e-logistics can be improved. The following data provides insight into IoT experts' perspectives towards what they believe and identify as privacy, security, and safety concerns. It also sheds light on the ways it can be improved in the technology (object design), internal business (process design) and external environment (realization design). The findings presented below ,established through the content analysis process described in Chapter 3, have been categorised into the three groupings of system design according to Van Aken (2005), namely object design, realization design and process design. Additionally, the following data is captured in a network diagram and matrix to provide a more comprehensive view of the responses collected with the research instrument.

Discussed in the findings below are the design principles derived from the matrix of codes categorised into privacy, security, and safety. These design principles provide insight into recommendations that can be made on how Ethical Design can be utilised to improve the privacy, security, and safety standards within logistics implementations of IoT. Resultantly, this answers the research sub-question mentioned in Chapter 1.

4.2 IoT Knowledge

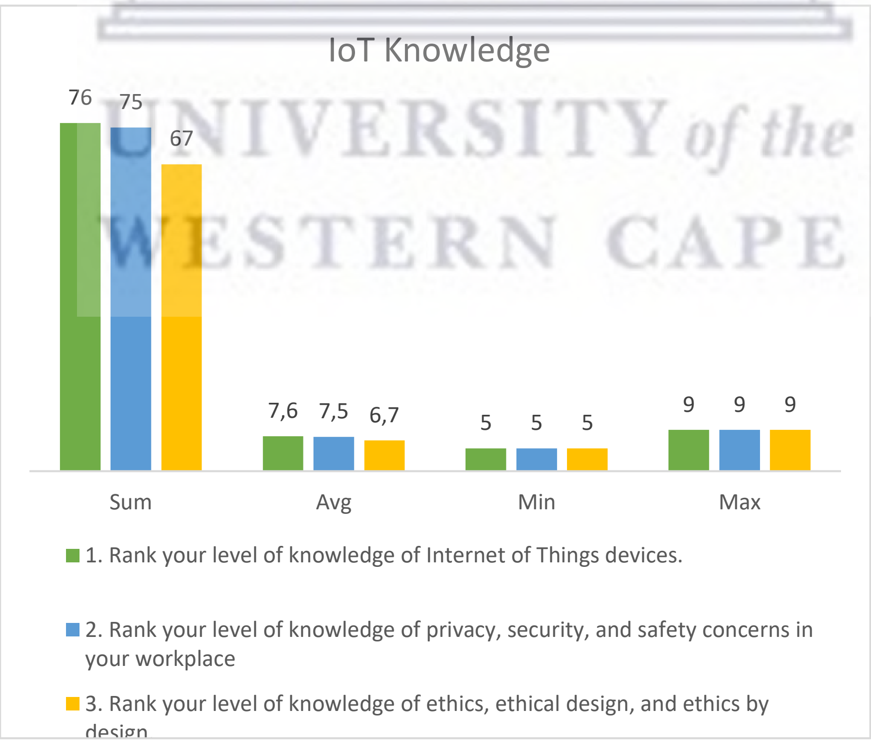


Figure 6: IoT knowledge of respondents

Figure 6 above represents the perceived IoT knowledge levels of the interviewees dependent on their knowledge of the following: the devices, the privacy, security, and safety concerns of these devices and ethics, Ethical Design, and ethics by design. The analysis of this data proves that these interviewees participating in this survey questionnaire perceived themselves to have a good understanding of the IoT devices in their workplace and the concerns thereof. However, their perceived knowledge of ethics, Ethical Design and ethics by design was below that of their knowledge of the other topics. This might indicate that within the sample workspace, ethics, and Ethical Design in the workplace, are concepts that still need further defining, understanding, and interpreting.

4.3 Object Design

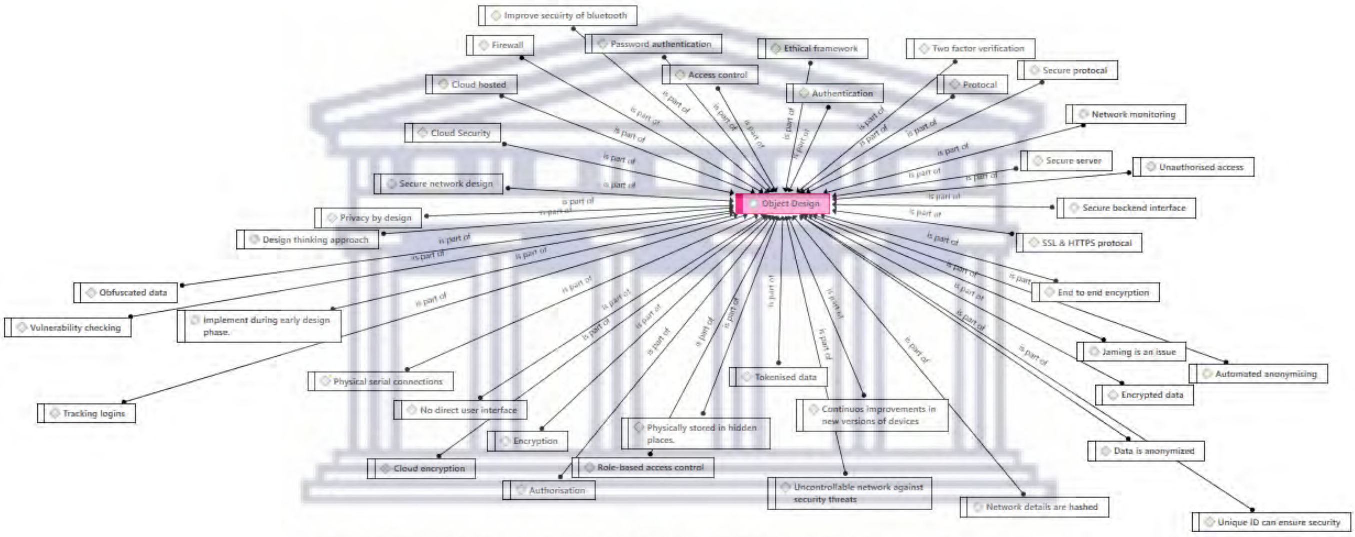


Figure 7: Object design network diagram

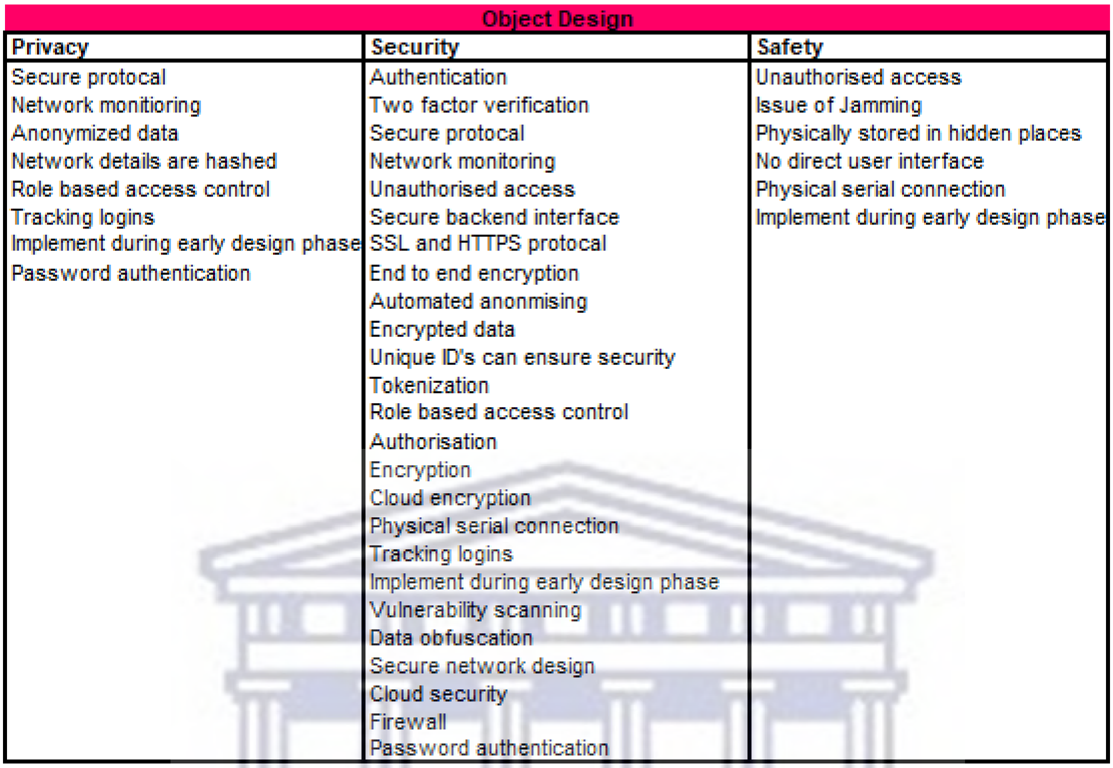
Object design can be described as the design of technology artifacts itself. This concept speaks to everything involved in building and maintaining the technology. This includes the infrastructure network, physical connections/ports, protocols, hardware, and software. This design concept also concerns the various layers of technology namely the application layer, network layer and perception layer. It is quite evident, through the analysis of the data, that most concerns, suggestions, and recommendations for bettering ethics concerned the technology artifact itself. In fact, the greatest security concern identified was that of authentication and encryption. This was a common theme in the data; a theme that most of the interviewees mentioned. This aligns with Agarwal & Dey (2016) who emphasizes the need for robust authentications mechanisms in IoT infrastructure to prevent unauthorised access. The findings state that having these in place can ensure the privacy, security, and safety of logistics IoT devices.

Authentication in IoT devices is concerned with permitting users to perform specific actions and gain access to specific resources in the device. Selecting and monitoring these users has been identified as a contributing factor to higher privacy and security in devices, hence the frequent occurrence of this theme. Additionally, interviewees stated that the authentication was configured in their APNs to ensure privacy.

Furthermore, the data analysis process found that a frequently mentioned theme was that of utilising cloud services, privacy, security, and safety protocols to protect their own data and devices. The codes mentioned in conjunction with this was cloud security, cloud-hosted services and cloud encryption. It can therefore be concluded that most IoT businesses utilise third party cloud hosted services to ensure their own privacy, security, and safety. Some of these cloud-hosted backend environments provide standard password authentication and role-based access control mechanisms. A common example is that of Amazon Web Services (AWS). Businesses that use vendors like AWS can be protected against any threats due to implemented privacy, security, and safety protocols. This theme identified resonates with the literature of Blair (2020) where the integration of cloud services and security protocols to protect data and devices are mentioned.

A common theme identified was that of implementing privacy, security, and safety standards during the design stage of a business's development lifecycle. Multiple interviewees mentioned the need to implement any concerns or standards early, as it become more difficult later in the development lifecycle. This corresponds with the literature's call for embedding ethical principles into system design from the outset to create a more secure and trustworthy technology (Allhoff & Henschke, 2018). This is evident in the statement made below by interviewee A.

"Privacy and intrinsic security are not layers that can necessarily be easily added to a product after its initial design and implementation. It should be part of the design philosophy and fundamental design of the product from the outset" (Interviewee A, 2022).



Object Design		
Privacy	Security	Safety
Secure protocal	Authentication	Unauthorised access
Network monitoring	Two factor verification	Issue of Jamming
Anonymized data	Secure protocal	Physically stored in hidden places
Network details are hashed	Network monitoring	No direct user interface
Role based access control	Unauthorised access	Physical serial connection
Tracking logins	Secure backend interface	Implement during early design phase
Implement during early design phase	SSL and HTTPS protocal	
Password authentication	End to end encryption	
	Automated anonmising	
	Encrypted data	
	Unique ID's can ensure security	
	Tokenization	
	Role based access control	
	Authorisation	
	Encryption	
	Cloud encryption	
	Physical serial connection	
	Tracking logins	
	Implement during early design phase	
	Vulnerability scanning	
	Data obfuscation	
	Secure network design	
	Cloud security	
	Firewall	
	Password authentication	

Figure 8: Privacy, security, and safety in object design

4.3.1 Privacy

Privacy concerns of the device itself (object design) are usually focused on building the freedom from interference into the technology and controlling how the data is stored, managed, collected, used, and accessed. One of the biggest privacy concerns among participants was that of passwords, specifically the monitoring and authentication thereof. Most passwords policies are that of third parties. Hence, organisations are harnessing the password authentication protocols from third parties. Otherwise, these organisations ensure they have password policies in place that focus on protecting and safeguarding the data and devices from outside threats, being the first line of defence. Moreover, changing passwords frequently was also listed as a recommendation to more private data and devices. This evidently reduces the risk of outside threats and privacy and security dangers.

4.3.2 Security

Security is a great concern within the technology of IoT devices. Safeguarding devices against security threats, vulnerabilities and cyber-attacks is an important factor when designing devices. Hence, the great concern for security in logistics industries identified in the data. As mentioned above, encryption was a cause for concern in the findings. Many mentioned the need for and use of encryption to ensure their devices are secure. Below interviewee B states how encryption can be used in data management to form a security barrier:

“Data is transmitted with encrypted binary stream as a form of security” (2ee B, 2022).

Another theme identified from the data analysis was that of access. Some of these themes identified are namely unauthorised access to the system and role-based access control. The access explained is that of access to the system and data generated. Allocating and maintaining access is a task that is required to secure data and systems against any threats. In fact, role-based access control mechanisms can ensure the correct users as seeing the necessary data. The practice of role-based access control aligns with the literature's emphasis on access management to secure IoT data and systems (Chatterjee, 2020). Interviewee C supports this argument by stating the following:

“*It is easy for authorised persons to access data, but virtually impossible for unauthorised persons to gain access*” (Interviewee C, 2022).

4.3.3 Safety

The safety concerns related to object design focuses on protecting and safeguarding the technology itself against risks, threats, and physical damage. The role of safety in IoT devices is also aligned with the literature's focus on preventing physical harm and undesirable threats (Atlam & Wills, 2020). Some of the concerns mentioned were jamming, physical serial connections, the user interface, and storage of the technology itself. These concerns can be categorised into the creation, maintenance, and storage of the technology. A recommended way of improving the safety of logistics IoT technologies was to install the devices out of reach of the public. This will ensure the devices are not tampered with or stolen.

Additionally, one case study interviewee mentioned that their devices did not have a direct user interface. This means that all changes, settings, and firmware installations are updated via the backend communication server on their SaaS platform. Hence, this organisation has full control over their devices and what is entered, stored, and managed. This protects the technology against any risk and threats. These statements are supported by the interviewees’ responses below:

“No physical ports or remote login capabilities through which the internal data is exposed” (Interviewee D, 2022).

“The data on the internal flash is encrypted to protect against physical disassembly and direct reading of the flash” (Interviewee E, 2022).

Contrary to these statements, interviewee C mentioned that the effective design of networks and applications determine the safety and security thereof and not the devices itself. This shows the importance of design and the incorporation of Ethical Design within the design phases. This shows that the initial stages in the development lifecycle that focuses on planning the network, interface and application can be considered very important to ensuring privacy, security, and safety.

“Network architecture and application design determine the security, not the devices” (Interviewee F, 2022).

4.3.4 Design Principles

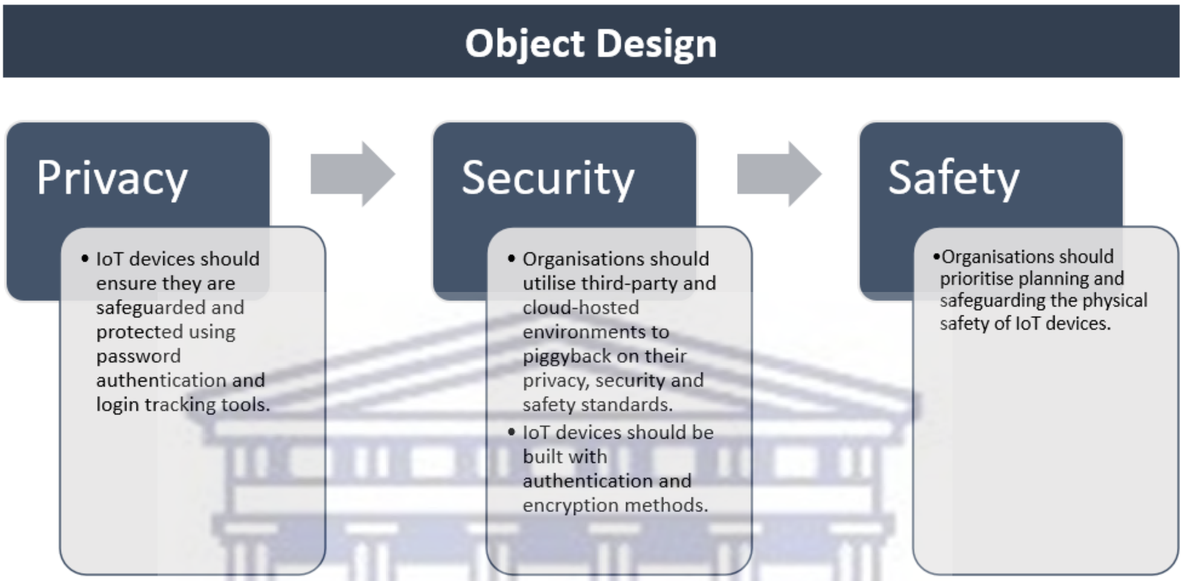

Object Design
Privacy
IoT devices should ensure they are safeguarded and protected using password authentication and login tracking tools.
Security
Organisations should utilise third-party and cloud-hosted environments to piggyback on their privacy, security and safety standards.
IoT devices should be built with authentication and encryption methods.
Safety
Organisations should prioritise planning and safeguarding the physical safety of IoT devices.

Figure 9: Design principles for object design

In Figure 9, design principles have been derived from the analysis of data found in the object design category. These principles were compiled from the codes mentioned in Figure 3. These principles focus on the main stages of the system's development lifecycle which includes planning, designing, testing, and deploying. These stages are considered the main focus of designing IoT devices, hence the mention of prioritising planning, utilising cloud-hosted environments, and safeguarding and building privacy logic into the devices. From analysis of the data, it can be concluded that object design focuses on the stages of the system development lifecycle thus ensuring that privacy, security, and safety are built within.

4.4 Process Design

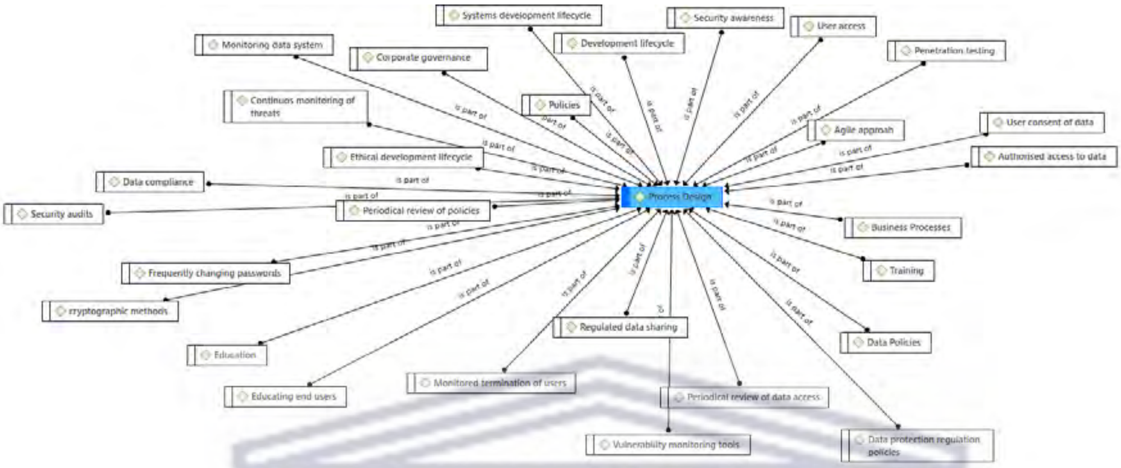


Figure 10: Process design network diagram

Process design, in conjunction with system design, can be defined as the design of "internal business" processes that are essential to the functioning of the technology. These are all the activities focused on internal business and the processes within. This includes data management, business policies, governance, and the development lifecycle related to the technology being designed. One of the biggest contributors to privacy, security, and safety concerns in IoT is that of the data generated and how it is managed. This was a common theme when analysing the data. Ensuring the privacy, security, and safety of the data can ensure that the privacy, security, and safety of IoT devices are taken care of as well. As illustrated in Figure 2, the common codes relating to data management were that of authorising access to data, ensuring data policies are being followed, regulating data sharing, and monitoring the data system. This is supported by the comments made by interviewee G, H, and I below:

> *"Data is transmitted with encrypted binary stream as a form of security" (Interviewee G, 2022).*

> *"Data is persisted to a cloud-hosted backend environment that provides standard password authentication and role-based access control mechanisms" (Interviewee H, 2022).*

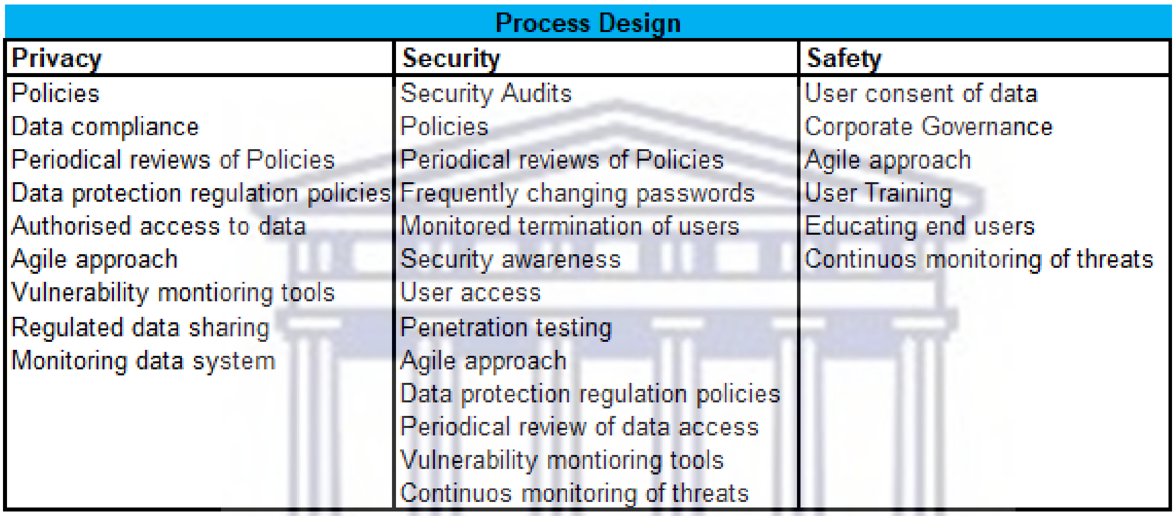
> *"Monitoring of the data reporting system has been implemented to detect and revoke access where users are inactive for periods" (Interviewee I, 2022).*

With reference to Figure 11, the data analysis highlighted another common theme relating to the development lifecycle of the IoT devices. It is quite evident through the data collected that the incorporation of privacy, security, and safety in early stages of the development lifecycle can ensure private, safe, and secure devices. Interviewee J states that it is in fact easier to build this ethical consideration in the beginning of the process:

"It is easier to build in privacy and security from the design phase that trying to add these at the end of the process" (Interviewee J, 2022).

Interviewee K states that these ethical considerations should be a part of the design as well:

"It should be part of the design philosophy and fundamental design of the product from the outset" (Interviewee K, 2022).



Process Design		
Privacy	Security	Safety
Policies	Security Audits	User consent of data
Data compliance	Policies	Corporate Governance
Periodical reviews of Policies	Periodical reviews of Policies	Agile approach
Data protection regulation policies	Frequently changing passwords	User Training
Authorised access to data	Monitored termination of users	Educating end users
Agile approach	Security awareness	Continuos monitoring of threats
Vulnerability montioring tools	User access	
Regulated data sharing	Penetration testing	
Monitoring data system	Agile approach	
	Data protection regulation policies	
	Periodical review of data access	
	Vulnerability montioring tools	
	Continuos monitoring of threats	

Figure 11: Privacy, security, and safety in process design

4.4.1 Privacy

One of the greatest concerns within the process design category is that of data management. The practice of ensuring the privacy, security, and safety of the data generated by the devices was considered of upmost importance. Some of these data management privacy related codes are: data compliance, data protection regulation policies, authorised access to data, regulated data sharing and monitoring the data system.

One of the data privacy concerns mentioned was that of data sharing within the organisation. This was identified as a concern by interviewee F, as seen below. Sharing data in an organisation can be seen as a risk when it is not regulated. Hence, informal sharing of data can mean risks of confidentiality and privacy breaches. Informal and unregulated data sharing can mean the wrong data in the hands of the wrong person.

"Sharing within a structured process is fine. Informal sharing of confidential information by staff and students poses a huge risk" (Interviewee L, 2022).

4.4.2 Security

As mentioned above, data management was one of the greatest concerns. The security of data has been a concern within logistics IoT devices. Specifically, these IoT experts mentioned users access to data, data protection regulation properties, periodical review of access, monitored termination of data access of users. Through analysis of the findings, it is clear that access to the organisation and IoT data is a cause for concern. Additionally, this correlates with the concern of monitoring data access and terminating access to data when required.

Deductions state that allocating the correct access to the correct data is very necessary to ensure data remain confidential, private, and secure. Alongside allocating user access, terminating this access when it is inactive or not needed is a considered recommendation for future logistics IoT experts. This can be identified in the statement made by interviewee M below:

> *"Monitoring of the reporting system has been implemented to detect and revoke access where users are inactive for periods" (Interviewee M, 2022).*

Additionally, another suggestion towards a more private, secure, and safe IoT device is the need to frequently change passwords. The changing of passwords is necessary to prevent cybercriminal and hacker access to confidential data in the system. Inevitably, this minor task of changing passwords in an organisation can led to more private and secure data and systems. The suggestion to frequently change passwords as a security measure also corresponds to the literature's recommendations for proactive security practices (Guggenmos et al., 2022).

4.4.3 Safety

One of the most identified themes to ensure the safety of devices in the internal business is through educating and training users within the organisation. Educated users are one of the biggest keys to safe devices. Users who are aware of phishing, cyber-attacks and related threats are more prone to understanding and reacting in the safest manner. The reaction to these threats can greatly impact the safety of users' data. Additionally, human vulnerabilities like phishing can be remedied through constant training and educating of users.

4.4.4 Design Principles

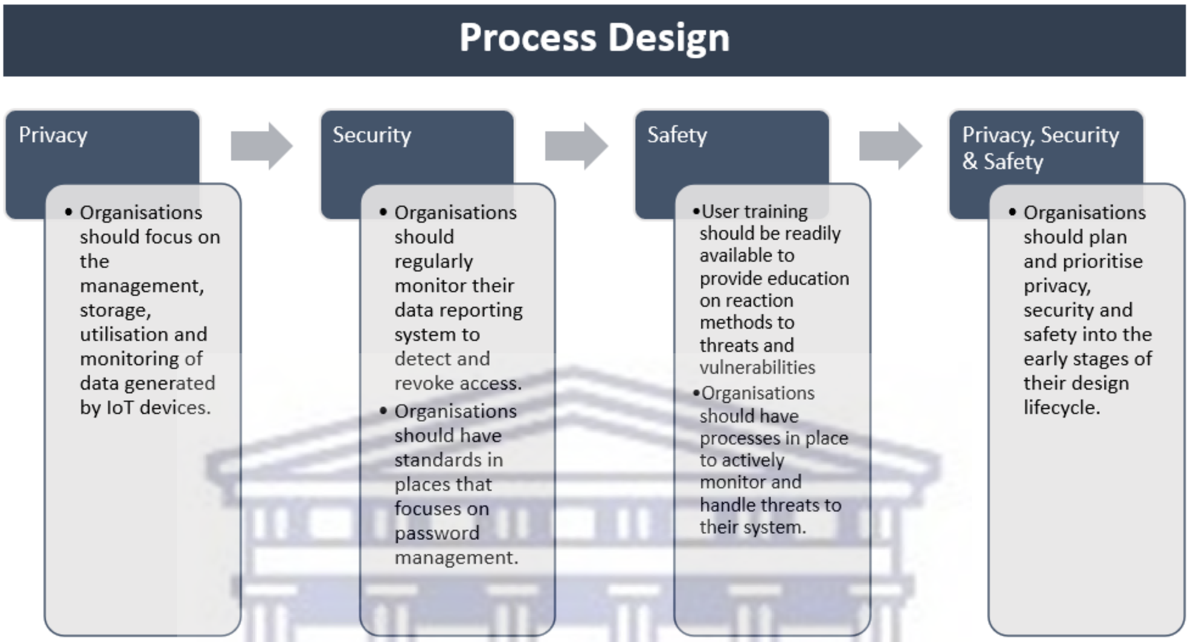

Process Design
Privacy
• Organisations should focus on the management, storage, utilisation and monitoring of data generated by IoT devices.
Security
• Organisations should regularly monitor their data reporting system to detect and revoke access.
• Organisations should have standards in places that focuses on password management.
Safety
•User training should be readily available to provide education on reaction methods to threats and vulnerabilities
•Organisations should have processes in place to actively monitor and handle threats to their system.
Privacy, Security & Safety
• Organisations should plan and prioritise privacy, security and safety into the early stages of their design lifecycle.

Figure 12: Design principles for process design

In Figure 12, design principles have been derived from the analysis of data and the matrix of thematic codes displayed above. The privacy and security design principles are mostly concerned with the data generated from the IoT device. These principles provide recommendations on how the data can be protected and secured. Due to most of the concerns primarily focusing on the data management in the organisation, these design principles are essential to ensure private and secure data. The emphasis on protecting and securing data aligns with the concept of "Privacy by Design" and "Security by Design" discussed in the literature (Allhoff & Henschke, 2018; Atlam & Wills, 2020).

It can be concluded from the research demonstrated, that organisations striving to ensure their IoT devices are private, secure, and safe need to ensure that the data management, user training and user access are themes incorporated into their objectives and Key Performance Indicators (KPIs). These themes have been highlighted in the analysis of data and show potential for increasing privacy, security, and safety in the process design of IoT Logistics devices.

4.5 Realization Design

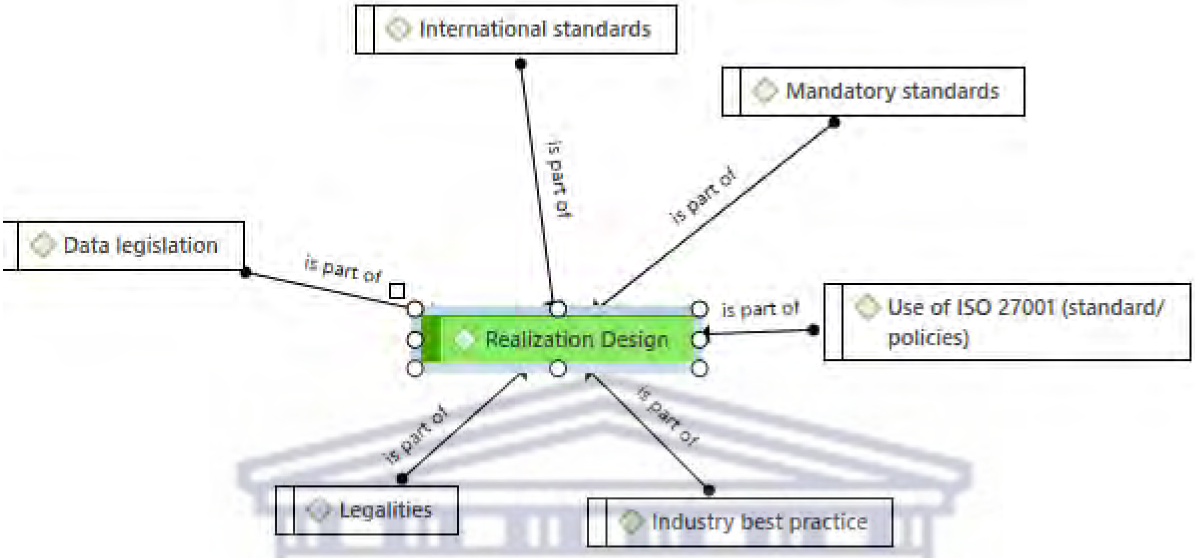
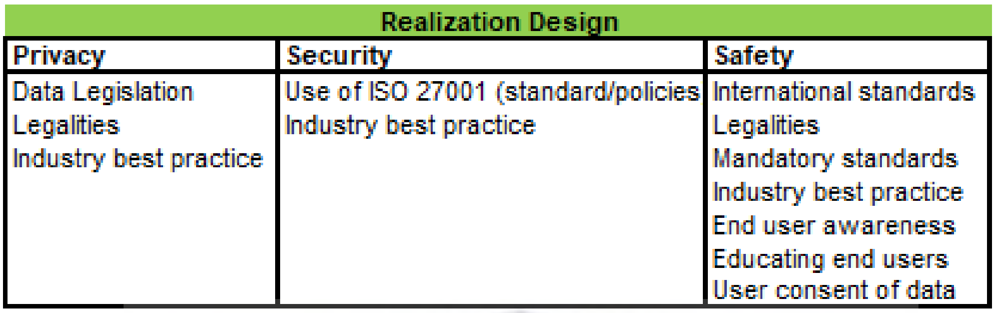


Figure 13: Realization network diagram

Realization design can be defined as the part of system design that focuses on being sensitive to the requirements (legal, environmental, etc.) of the external environment that the technology will be implemented in. This concept purely attends to all the external factors and regulations influencing the business. During the analysis of the data, it was quite evident that the privacy, security, and safety of realization design was minimally elaborated or discussed. This could either mean that there are minimal privacy, security, and safety concerns in the external environment, or that there are few discussions regarding how this part of system design could be improved.

After analysing the data collected, the most identified theme within realization design was that of ensuring business use and following all standards, policies and legislation needed by the external environment. Just by following and abiding by these standards, the privacy, security, and safety of system design is ensured. This can be supported by the following statement made by interviewee N:

"Best practice encapsulated in process and policies. It can always be improved, but this is need based" (Interviewee N, 2022).



Realization Design		
Privacy	**Security**	**Safety**
Data Legislation Legalities Industry best practice	Use of ISO 27001 (standard/policies Industry best practice	International standards Legalities Mandatory standards Industry best practice End user awareness Educating end users User consent of data

Figure 14: Privacy, security, and safety in realization design

4.5.1 Privacy

The privacy within realization design focuses on the considerations required to protect the external environment seen as the realization category of system design. After categorising the findings into the conceptual framework, the main privacy concerns identified by interviewees was that of data legislation, legalities and industry best practice. Many interviewees mentioned being compliant with the legislation thus ensuring the privacy and security of their users. Additionally, their users' privacy was a big consideration as there are various legal implications.

"Generally, industry best practice is used to ensure that the devices are secure, private and safe to use" (Interviewee O, 2022).

According to the above statement made by interviewee B, the industry best practice dictated by the external environment can ensure that IoT devices are secure, private, and safe. Organisations that ensure that they follow these best practices are almost guaranteed private, secure, and safe devices.

4.5.2 Security

After analysis of the data, the only security concern repeatedly mentioned was that of utilising the specifications mentioned by the ISO0 27001. This is a framework of policies dictated by the information security management system. This was a common theme mentioned by most interviewees. Additionally, it was mentioned that this framework is used within the organisation to govern the data privately, securely, and safely.

4.5.3 Safety

Safeguarding IoT devices and business data from external threats and environmental forces can be seen as a large task. However, through analysis of this data set, being upfront with end users of the technology can help to safeguard them against any threats or unauthorised access to their data. Due to the users being a part of the external environment, namely realization design, it is important for organisations to protect users against privacy, security, and safety concerns with their data and IoT devices. Interviewee P states that utilising legal frameworks can better govern the use of information which in return can ensure the safety of users. This use of legal frameworks like PoPIA and GDPR is aligned with the literature's recommendations to reduce safety risks(Kandeh et al., 2018). Below Interviewee P states the importance of user's safety:

"Users are required to authorise the use of their information with respect to POPIA and GDPR. Being upfront with users in terms of the intended use of the data is absolutely key" (Interviewee P, 2022).

"The end user is responsible to handle threats within their own environment" (Interviewee Q, 2022).

Above, Interviewee Q, states the importance of user awareness and training. They state the need for end users to handle their own threats in their environment. This means that the awareness of threats and how to handle them is necessary knowledge for end users to be able to safeguard themselves. Users being aware of their environments and the threats that may occur can prevent risks to their privacy, security, and safety. The literature mentions trust, integrity, confidentiality, and protection of data as crucial for user acceptance. Designing ethical systems with these principles aligns with the literature's recommendations mentioned by Blair (2020).

4.5.4 Design Principles

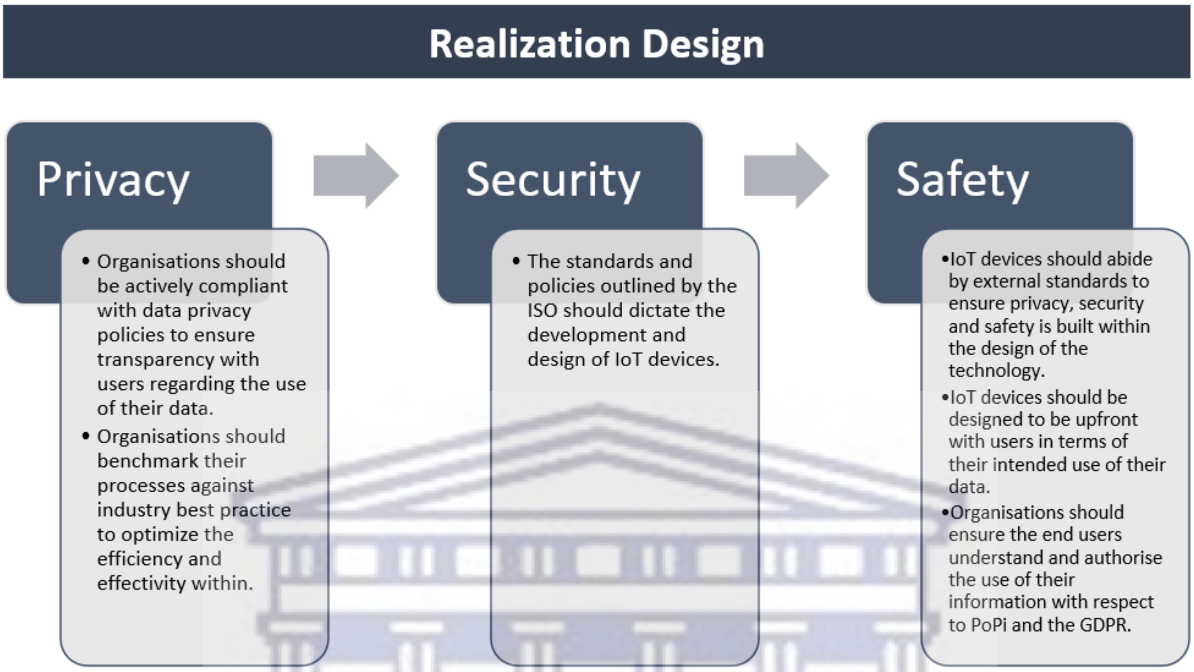

Realization Design
Privacy
Organisations should be actively compliant with data privacy policies to ensure transparency with users regarding the use of their data.
Organisations should benchmark their processes against industry best practice to optimize the efficiency and effectivity within.
Security
The standards and policies outlined by the ISO should dictate the development and design of IoT devices.
Safety
IoT devices should abide by external standards to ensure privacy, security and safety is built within the design of the technology.
IoT devices should be designed to be upfront with users in terms of their intended use of their data.
Organisations should ensure the end users understand and authorise the use of their information with respect to PoPi and the GDPR.

Figure 15: Design principles for realization design

In Figure 15 above, design principles have been identified to provide direction and recommendations for logistics IoT devices in the realization design stage. These design principles are focused on the external environment and how organisations can ensure they cater for and improve any concerns within privacy, security, and safety. All the above principles have demonstrated that they to abide by, benchmark and comply with the industry's policies, standards, and best practices. Compliance with these external policies shows potential to improve the devices privacy, security, and safety standards.

4.6 Chapter Summary

The chapter offers comprehensive insights into the research question, probing how the design of privacy, security, and safety of IoT devices used in e-logistics can be improved. The chapter focuses on the IoT interviewee's viewpoints towards the privacy, security and safety concerns and their potential resolutions within the logistics industry. Utilizing the framework by Van Aken (2005), this chapter explores the object design, process design, and realization design.

In Section 4.2, the data scrutinizes participants' perceptions of their knowledge domains, identifying the degrees of familiarity with IoT devices, their related concerns, and ethical design principles. This highlights the need for a deeper comprehension of ethics and its integration into workplace.

In Section 4.3, the data delves into the technology artifact's design, known as object design. This section emphasizes the pivotal role of authentication and encryption in securing IoT devices. Additionally, this section underscores the merit of embedding privacy, security, and safety standards in the designs of technology artifacts. Password policies, encryption strategies and the management of user access are highlighted as approaches to more private, secure, and safe devices

In Section 4.4, the data focuses on the internal business processes, known as process design. This section highlights that the utilisation of data management policies and processes, user training, and access regulation ensures the safeguarding of IoT devices. The chapter underscores the significance of ethical considerations in the development lifecycle. Training and education are spotlighted as potential tools to enhance safety.

In Section 4.5, the data showcases the resonance of best practices and compliance in preserving privacy, security, and safety within realization design. This confirms the sentiment that adherence to external standards equips IoT devices to thrive within e-logistic environments.

In summary, the Data Findings and Discussion chapter navigates a variety of opinions, originating from the voices of IoT experts. These finding reveal information regarding object design, process design and realization design, helping to better understand how the privacy, security and safety are connected with the industry of e-logistics IoT devices.

Chapter 5: Conclusion

5.1 Introduction

This chapter concludes the study by providing answers to the primary research question as well as the sub-questions identified in Chapter 1. Following this, it presents a summary of the key findings, to provide more insight into the problem clearly stated in this study. This conclusion is focused on the privacy, security, and safety improvements that have been suggested to improved IoT logistics devices. The final section discusses the study's limitations and provides recommendations for future research.

5.2 Primary Research Question

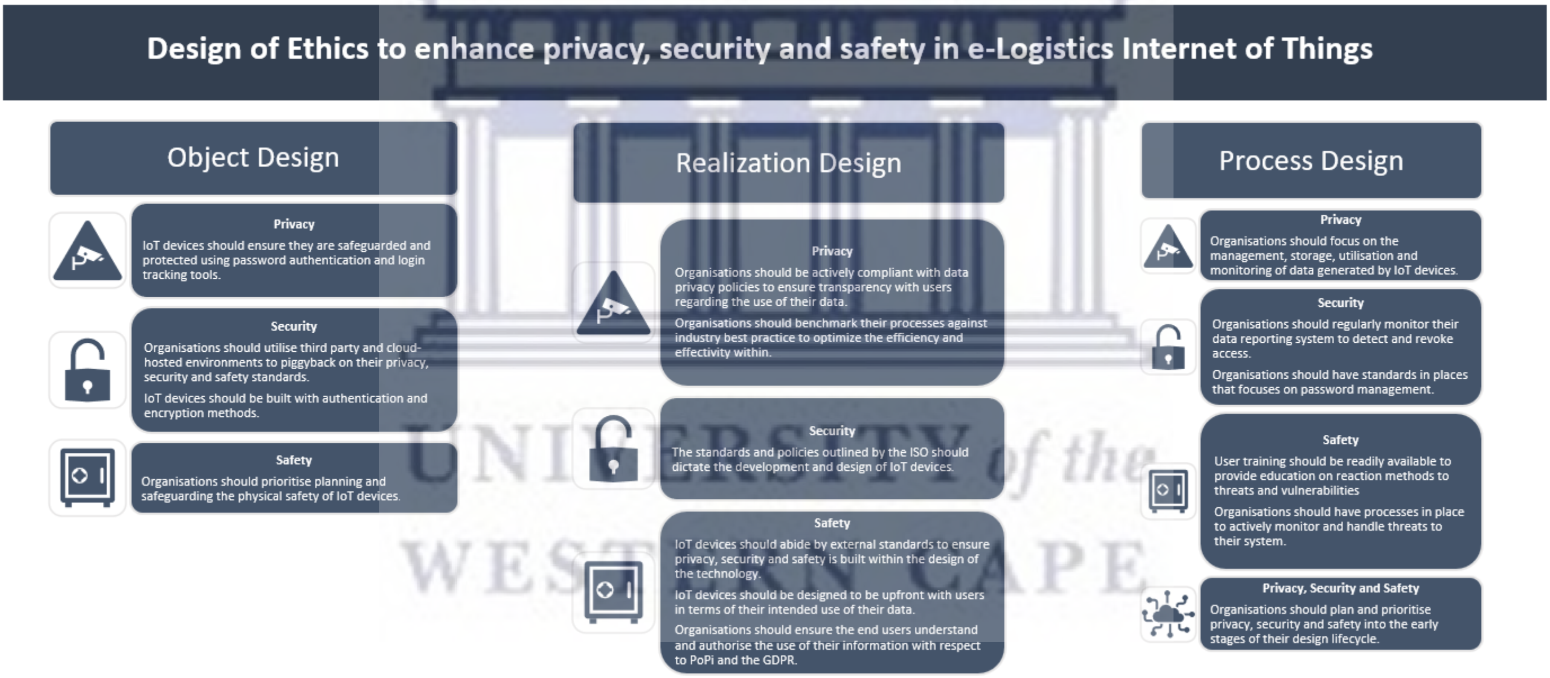
This research aimed to answer the primary research question about how the design of privacy, security, and safety of IoT devices used in e-logistics could be improved. The data collected was gathered using a questionnaire that was guided by Van Aken's framework. With the guidance of this framework, the study was able to categorise the concerns into the three main stages of system design, namely object, process, and realization. This framework provided context to the data that was collected and analysed. Based on the qualitative data collected using a questionnaire, this study concluded with design principles to best safeguard, protect and secure the physical device, the internal environment, and the external environment. These results highlight the main themes of the system development lifecycle, the physical protection of the device, the external standards and policies, and the concerns regarding the end user, their access to the device and protection of their data.

5.3 Summary of Key Findings

The data findings in the previous chapter provided insight into the data collected from IoT logistics experts and how they perceived privacy, security, and safety in relation to object design, process design, and realization design. This study answered the following sub-questions during the literature review, data analysis, and discussion of findings:

- What are the operational definitions of ethics and Ethics by Design within Information Systems?
- How can ethics be incorporated into the design of IoT?
- Can ethics by design be employed to ensure privacy, security, and safety?
- What are the perspectives of logistics experts towards the utilisation of ethics by design within IoT devices in the logistics industry?
- What recommendations can be made on how Ethics by Design can be utilised to improve the privacy, security, and safety standards within logistics implementations of IoT?

The data collected highlighted a few common themes that are necessary to note when answering the above research questions. During the conception of an IoT device, it is vital to consider any concerns that may impact the privacy, security, and safety thereof. The early identification thereof, should be added during the initial design and implementation stages of the device. Hence, the implementation of a well thought out system development cycle that organisations use to plan, build and maintain the IoT devices can potentially contribute to a more private, secure, and safe device. Ethically considering the end users of the devices has been identified as a contributing factor to a more private, secure, and safe device. Ensuring users are aware of how their data is being utilised and understanding the intended use of their data in relation to PoPIA and GDPR can ensure the safety of the devices as well as the users themselves. Additionally, a common and recurring theme was identified in the object and process design of these devices, namely authentication, authorisation and encryption. These methods have shown to improve the privacy and security of devices. Figure 16 provides a summarised view of the design principles for each category of Van Aken's design framework. This visual is derived from the conceptual framework created in Chapter 2 (see Figure 3). This visuals provides a summarised view of the data collected in terms of Van Akens framework, as well as answering the research question posed by this study.



Design of Ethics to enhance privacy, security and safety in e-Logistics Internet of Things

Object Design

Privacy

IoT devices should ensure they are safeguarded and protected using password authentication and login tracking tools.

Security

Organisations should utilise third party and cloud-hosted environments to piggyback on their privacy, security and safety standards.

IoT devices should be built with authentication and encryption methods.

Safety

Organisations should prioritise planning and safeguarding the physical safety of IoT devices.

Realization Design

Privacy

Organisations should be actively compliant with data privacy policies to ensure transparency with users regarding the use of their data.

Organisations should benchmark their processes against industry best practice to optimize the efficiency and effectivity within.

Security

The standards and policies outlined by the ISO should dictate the development and design of IoT devices.

Safety

IoT devices should abide by external standards to ensure privacy, security and safety is built within the design of the technology.

IoT devices should be designed to be upfront with users in terms of their intended use of their data.

Organisations should ensure the end users understand and authorise the use of their information with respect to PoPi and the GDPR.

Process Design

Privacy

Organisations should focus on the management, storage, utilisation and monitoring of data generated by IoT devices.

Security

Organisations should regularly monitor their data reporting system to detect and revoke access.

Organisations should have standards in places that focuses on password management.

Safety

User training should be readily available to provide education on reaction methods to threats and vulnerabilities

Organisations should have processes in place to actively monitor and handle threats to their system.

Privacy, Security and Safety

Organisations should plan and prioritise privacy, security and safety into the early stages of their design lifecycle.

5.4 Future Research

Based on the conclusions deducted from this study, future research is needed to determine and identify a unified definition of IoT ethics. In most cases ethics is a common concept that has been defined by many academics. However, the definition of ethics in relation to IoT deserves a spotlight in the Information Systems field. This concept is continually growing and requires further research to better understand the different perspectives on ethics in the field of Internet of Things. This need for future research can benefit researchers, academics, scholars and IoT experts. This would be necessary for further studies looking at the impact it can have on business processes, strategy, operations, and technology.

5.5 Research Limitations

The focus of this study was to collect IoT experts' perspectives on how the privacy, security, and safety of IoT devices used in logistics could be improved. However, this research was limited to a single case study. This limitation contributed to an insufficient sample size. Due to the way this questionnaire was built, there were only a few individuals who had insight and knowledge into all areas of the devices. Hence, the data collected was minimal and only driven by a few experts in this case study. A study focused on multiple cases would have potential to reach a wider audience and potentially offer more insightful feedback.

5.6 Conclusion

In conclusion, the findings collected in this study have provided design principles that can be utilised in the different categories of system design namely object design, process design and realization design. Additionally, providing a basis on which privacy, security and safety can be embedded in the design of systems in the logistics industry. The recommendations for future research have been provided to ensure more comprehensive research into specifically IoT in logistics in a South Africa context.

References

Agarwal, Y. & Dey, A.K. 2016. Toward building a safe, secure, and easy-to-use Internet of Things infrastructure. *IEEE Computer Society*, 49(4):88–91.

Akram, R.N., Markantonakis, K., Mayes, K., Group, S., Card, S., Holloway, R. & Kingdom, U. 2017. Security, privacy and safety evaluation of dynamic and static fleets of drones. arXiv e-prints, pp.arXiv-1708.

Alfandi, O., Khanji, S., Ahmad, L. & Khattak, A. 2021. A survey on boosting IoT security and privacy through blockchain: exploration, requirements, and open issues. *Cluster Computing*, 24(1):37–55. DOI: 10.1007/s10586-020-03137-8.

Allhoff, F. & Henschke, A. 2018. The Internet of Things: foundational ethical issues. *Internet of Things*, 1–2:55–66. DOI: 10.1016/j.iot.2018.08.005.

Atlam, H.F. and Wills, G.B., 2020. IoT security, privacy, safety and ethics. Digital twin technologies and smart cities, pp.123-149.Azam, F., Munir, R., Ahmed, M., Ayub, M., Sajid, A. & Abbasi, Z. 2019. Review article Internet of Things (IoT). *Security Issues and its Solutions*, 3(2):18–21.

Azam, F., Saeed, M. A., & Shafiq, M. 2019. Internet of Things (IoT) applications to fight against COVID-19. In EAI/Springer Innovations in Communication and Computing (pp. 45-54). Springer.

Babbie, E. & Mouton, J. 2010. Qualitative data analysis: the practice of social research. Cengage learning.

Badii, C., Bellini, P., Difino, A. & Nesi, P. 2020. Smart city IoT platform respecting GDPR privacy and security aspects. *IEEE Access*. 8:23601–23623. DOI: 10.1109/ACCESS.2020.2968741.

Bagüés, S.A., Zeidler, A., Valdivielso, F. & Matias, I.R. 2007. Sentry@Home - Leveraging the smart home for privacy in pervasive computing. *International Journal of Smart Home*, 1(2):129–146.

Baldini, G., Botterman, M., Neisse, R. and Tallacchini, M., 2018. Ethical design in the internet of things. Science and engineering ethics, 24, pp.905-925.Blair, P.D. 2020. Ethics in Technology.

Botterman, M. 2017. Ethical IoT: a sustainable way forward. *Building Blocks for IoT Analytics Internet-of-Things Analytics*. pp.239–248.

Brey, P. 2017. Method in computer ethics: towards a multi-level interdisciplinary approach. *Computer Ethics*, 233–237. DOI: 10.4324/9781315259697-24.

Burhan, M. & Rehman, R.A. 2018. IoT elements, layered architectures and security issues: a comprehensive survey. sensors, 18(9), p.2796.

Burhan, N., & Rehman, A. 2018. An overview of Internet of Things (IoT) and data analytics in agriculture: Benefits and challenges. In 2018 4th International Conference on Control, Automation and Robotics (ICCAR) (pp. 265-271). IEEE.

Chatila, R. & Havens, J.C. 2019. The IEEE global initiative on ethics of autonomous and intelligent systems. *Intelligent Systems, Control and Automation: Science and Engineering*, 95:11–16. DOI: 10.1007/978-3-030-12524-0_2.

Chatterjee, S. 2020. The safety of IoT-enabled system in smart cities of India: do ethics matter? *International Journal of Ethics and Systems*, 36(4):601–618. DOI: 10.1108/IJOES-05-2019-0085.

Chaudhuri, A. 2017. Philosophical dimensions of information and ethics in the Internet of Things (IoT) technology. *Edpacs*, 56(4):7–18. DOI: 10.1080/07366981.2017.1380474.

Dignum, V., Baldoni, M., Baroglio, C., Caon, M., Chatila, R., Dennis, L., Gonzalo, G., Kließ, M., et al. 2018. Ethics by design: necessity or curse? Proceedings of the AAAI/ACM Conference on Artificial Intelligence, Ethics, and Society. Available from: http://tinyurl.com/GDPREU2016.

Dubey, R., Altay, N., Gunasekaran, A., Blome, C., Papadopoulos, T. & Childe, S.J. 2018. Supply chain agility, adaptability and alignment: empirical evidence from the Indian auto components industry. *International Journal of Operations and Production Management*, 38(1):129–148. DOI: 10.1108/IJOPM-04-2016-0173.

Duriau, V.J., Reger, R.K. & Pfarrer, M.D. 2007. A content analysis of the content analysis literature in organization studies. *Organizational Research Methods*, (February 2005):5–34.

Fang, W., Wen, X.Z., Zheng, Y. & Zhou, M. 2017. A survey of big data security and privacy preserving. *IETE Technical Review*, 34(5):544–560. DOI: 10.1080/02564602.2016.1215269.

Gimpel, H., Kleindienst, D., Nüske, N., Rau, D. & Schmied, F. 2018. The upside of data privacy – delighting customers by implementing data privacy measures. *Electronic Markets*, 28(4):437–452. DOI: 10.1007/s12525-018-0296-3.

Gotterbarn, D.W., Brinkman, B., Flick, C., Kirkpatrick, M.S., Miller, K., Vazansky, K. and Wolf, M.J., 2018. ACM code of ethics and professional conduct.

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

Guggenmos, F., Häckel, B., Ollig, P. & Stahl, B. 2022. Computers & security security first, security by design, or security pragmatism – strategic roles of IT security in digitalization projects. *Computers & Security*, 118:102747. DOI: 10.1016/j.cose.2022.102747.

Hagendorff, T. 2020. The ethics of AI ethics: an evaluation of guidelines. *Minds and Machines*, 30(1):99–120. DOI: 10.1007/s11023-020-09517-8.

Introna, L.D. 2005. Disclosive ethics and information technology: disclosing facial recognition systems. *Ethics and Information Technology*, 7(2):75–86. DOI: 10.1007/s10676-005-4583-2.

Jurkiewicz, C.L. 2018. Big data, big concerns: ethics in the digital age. Public Integrity, 20(sup1), pp.S46-S59

Kandeh, A.T., Botha, R.A., Futcher, L.A., Technology, I., Africa, S. & Kandeh, A. 2018. Enforcement of the Protection of Personal Information (POPI) Act: Perspective of data management professionals. South African Journal of Information Management, 20(1), pp.1-9.

Kandeh, J. M., Leenen, L., & Labuschagne, L. (2018). Data privacy concerns in smart cities: A survey. In Proceedings of the International Conference on e-Infrastructure and e-Services for Developing Countries (pp. 139-150). Springer.

Karale, A. 2021. The challenges of IoT addressing security, ethics, privacy, and laws. *Internet of Things*. 15:100420. DOI: 10.1016/j.iot.2021.100420.

Karr, A. n.d. Ethical design. *Interactions*. Available: https://interactions.acm.org/blog/view/ethical-design.

Kiger, M.E. & Varpio, L. 2020. Thematic analysis of qualitative data: AMEE guide No. 131. *Medical Teacher*, 42(8):846–854. DOI: 10.1080/0142159X.2020.1755030.

Killeen, P., Ding, B., Kiringa, I. & Yeap, T. 2019. IoT-based predictive maintenance for fleet management. *Procedia Computer Science*, 151(2018):607–613. DOI: 10.1016/j.procs.2019.04.184.

Langheinrich, M. 2002. A privacy awareness system for ubiquitous computing environments. InUbiComp 2002: Ubiquitous Computing: 4th International Conference Göteborg, Sweden, September 29–October 1, 2002 Proceedings 4 2002 (pp. 237-245). Springer Berlin Heidelberg.

Lapointe, C. & Fishbane, L. 2019. The blockchain ethical design framework. *Innovations: Technology, Governance, Globalization*, 12(3–4):50–71. DOI: 10.1162/inov_a_00275.

Lee, D. & Hess, D.J. 2022. Public concerns and connected and automated vehicles: safety, privacy, and data security. *Humanities and Social Sciences Communications*, 9(1):1–13. DOI: 10.1057/s41599-022-01110-x.

Lei Xu, Chunxiao Jiang, Jian Wang, Jian Yuan & Yong Ren. 2014. Information security in big data: privacy and data mining. *IEEE Access*, 2:1149–1176. DOI: 10.1109/access.2014.2362522.

Maple, C. 2017. Security and privacy in the Internet of Things. Journal of cyber policy, 2(2), pp.155-184.

Masrom, M., Ismail, Z., Hussein, R., Faragardi, H.R., Stahl, B.C., Eden, G., Jirotka, M., Coeckelbergh, M., et al. 2011. What is computer ethics? *Journal of Business Ethics*. 16(1):266–275. Available: http://dx.doi.org/10.1016/j.im.2014.01.001.

Melnikovas, A. 2018. Towards an explicit research methodology: adapting research onion model for futures studies. *Journal of Futures Studies*, 23(2):29–44. DOI: 10.6531/JFS.201812_23(2).0003.

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

Mercan, S., Akkaya, K., Cain, L. & Thomas, J. 2020. Security, privacy and ethical concerns of IoT implementations in hospitality domain. In 2020 International Conferences on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData) and IEEE Congress on Cybermatics (Cybermatics) (pp. 198-203). IEEE.

Monnerat, F., Dias, J. & Alves, M.J. 2019. Fleet management: a vehicle and driver assignment model. *European Journal of Operational Research*, 278(1):64–75. DOI: 10.1016/j.ejor.2019.03.021.

Moor, J.H. 1985. What is computer ethics? *Metaphilosophy*, 16(4):266–275. DOI: 10.1111/j.1467-9973.1985.tb00173.x.

Núñez-Merino, M., Maqueira-Marín, J.M., Moyano-Fuentes, J. & Martínez-Jurado, P.J. 2020. Information and digital technologies of Industry 4.0 and lean supply chain management: a systematic literature review. *International Journal of Production Research*, 58(16):5034–5061. DOI: 10.1080/00207543.2020.1743896.

Ogbuke, N.J., Yusuf, Y.Y., Dharma, K. & Burcu, A. 2020. The management of operations big data supply chain analytics: ethical, privacy and security challenges posed to business, industries and society. Production Planning & Control, 33(2-3), pp.123-137

Palinkas, L.A., Horwitz, S.M., Green, C.A., Wisdom, J.P., Duan, N. & Hoagwood, K. 2015. Purposeful sampling for qualitative data collection and analysis in mixed method implementation research. *Administration and Policy in Mental Health and Mental Health Services Research*, 42(5):533–544. DOI: 10.1007/s10488-013-0528-y.

Paradice, D., Freeman, D., Hao, J., Lee, J. & Hall, D. 2018. A review of ethical issue considerations in the information systems research literature. DOI: 10.1561/9781680833997.

Peters, M.A. 2017. Technological unemployment: educating for the fourth industrial revolution. *Educational Philosophy and Theory*, 49(1):1–6. DOI: 10.1080/00131857.2016.1177412.

Peters, D., Vold, K., Robinson, D. & Calvo, R.A. 2020. Responsible AI—two frameworks for ethical design practice. *IEEE Transactions on Technology and Society,* 1(1):34–47. DOI: 10.1109/tts.2020.2974991.

Rane, S.B., Potdar, P.R. & Rane, S. 2021. Data-driven fleet management using MOORA: a perspective of risk management. *Journal of Modelling in Management*, 16(1):310–338. DOI: 10.1108/JM2-03-2019-0069.

Riege, A.M. 2003. Validity and reliability tests in case study research: A literature review with "hands-on" applications for each research phase. Qualitative Market Research: An International Journal. 6(2):75–86. DOI: 10.1108/13522750310470055.

Santoro, F.M. & Costa, R.M.E.M. da. 2021. Towards ethics in information systems. *Journal on Interactive Systems*, 12(1):69–82. DOI: 10.5753/jis.2021.961.

Saunders, M., Lewis, P. & Thornhill, A. 2009. Research methods for business students. Fifth edition. Essex: Pearson Education limited.

Seliem, M., Elgazzar, K. & Khalil, K. 2018. Towards privacy preserving IoT environments: a survey. *Wireless Communications and Mobile Computing*, 2018(October). DOI: 10.1155/2018/1032761.

Seong, S.W., Seo, J., Nasielski, M., Sengupta, D., Hangal, S., Teh, S., Chu, R., Dodson, B., et al. 2010. PrPl: a decentralized social networking infrastructure. In *Proceedings of the 1st ACM Workshop on mobile cloud computing & services*. (MCS '10). ACM. 1–8.

Sethi, P. & Sarangi, S.R. 2017. Internet of things: architectures, protocols, and applications. *Journal of Electrical and Computer Engineering.* DOI: 10.1155/2017/9324035.

Sharma, U. 2009. Qualitative research in business & management. *Qualitative Research in Accounting and Management*, 6(4):292–296.

Somasundaram, D. 2019. Internet of Things (IoT) in Logistics and Supply Chain Management. In Encyclopedia of Big Data Technologies (pp. 1-8). Springer

Stahl, B.C., Eden, G., Jirotka, M. & Coeckelbergh, M. 2014. From computer ethics to responsible research and innovation in ICT: the transition of reference discourses informing ethics-related research in information systems. *Information and Management*, 51(6):810–818. DOI: 10.1016/j.im.2014.01.001.

Sutherland, E. 2020. The fourth industrial revolution - the case of South Africa. *Politikon*, 47(2):233–252. DOI: 10.1080/02589346.2019.1696003.

Tu, M. 2018. An exploratory study of Internet of Things (IoT) adoption intention in logistics and supply chain management a mixed research approach. *International Journal of Logistics Management*, 29(1):131–151. DOI: 10.1108/IJLM-11-2016-0274.

Tu, M., Lim, M.K. & Yang, M.F. 2018. IoT-based production logistics and supply chain system – part 2 IoT-based cyber-physical system: a framework and evaluation. *Industrial Management and Data Systems*, 118(1):96–125. DOI: 10.1108/IMDS-11-2016-0504.

Tu, Y. L. 2018. The Internet of Things in Logistics Management: A Literature Review. In Proceedings of the International Conference on Industrial Engineering and Operations Management (pp. 971-983). IEOM Society International.

United Nations Educational, Scientific and Cultural Organization (UNESCO). n.d. Ethics of artificial intelligence – UNESCO Member States adopt the setting instrument on the subject. Available: https://www.unesco.org/en/artificial-intelligence/recommendation-ethics#:~:text

Ustek-Spilda, F., Powell, A. & Nemorin, S. 2019. Engaging with ethics in Internet of Things: imaginaries in the social milieu of technology developers. *Big Data and Society*, 6(2):1–12. DOI: 10.1177/2053951719879468.

Van Aken, J.E. 2004. Management research based on the paradigm of the design sciences: the quest for field-tested and grounded technological rules. *Journal of Management Studies*, 41(2):219–246. DOI: 10.1111/j.1467-6486.2004.00430.x.

Van Aken, J.E. 2005. Valid knowledge for the professional design of large and complex design processes. *Design Studies*, 26(4):379–404. DOI: 10.1016/j.destud.2004.11.004.

Weinhardt, M., 2021. Big data: Some ethical concerns for the social sciences. Social Sciences, 10(2), p.36.

Witkowski, K. 2017. Internet of Things, big data, industry 4.0 - innovative solutions in logistics and supply chains management. *Procedia Engineering*, 182:763–769. DOI: 10.1016/j.proeng.2017.03.197.

Zhang, Y. and Wildemuth, B.M., 2009. *Applications of Social Research Methods to Questions in Information and Library Science*. Portland, OR: Book News.