

# **A Framework of Privacy Assessment for Smart Airport Passenger Interaction Architecture**

**by Maha Ibrahim A Alabsi**

Thesis submitted in fulfilment of the requirements for  
the degree of

**Doctor of Philosophy (C02029)**

under the supervision of:

Prof. Asif Gill

Dr. Madhushi Bandara

Dr. Bo Lui

Prof. Farookh Husain

University of Technology Sydney  
Faculty of Engineering and Information Technology School  
of Computer Science  
October 2023

## Certificate of Original Authorship

I, Maha Ibrahim A Alabsi, declare that this thesis is submitted in fulfilment of the requirements for the award of *Doctor of Philosophy in Information Systems*, in the School of Computer Science/ Faculty of Engineering and Information Technology at the University of Technology Sydney.

This thesis is wholly my own work unless otherwise referenced or acknowledged. In addition, I certify that all information sources and literature used are indicated in the thesis.

This document has not been submitted for qualifications at any other academic institution.

This research is supported by the Australian Government Research Training Program.

Signature:

Production Note:  
Signature removed prior  
to publication.

Date: 24/09/2023

## Acknowledgment

Foremost, I would like to express my deep gratitude to Allah for the guidance, strength, and inspiration provided throughout my academic journey.

I am delighted to acknowledge my deepest thanks and sincere gratitude to my supervisor, Dr. Asif Gill. His professional and invaluable guidance, feedback, expertise, and unwavering encouragement have been the cornerstones of this research. It is a great honour to work under his supervision. I am also grateful to Dr. Madhushi, Dr. Farookh, and Dr. Bo for their contributions during my supervision.

I extend my heartfelt thanks to my lovely family for their keen interest in my academic achievement. Their encouragement during challenging times has been greatly appreciated and noted. Special thanks go to my parents, Ibrahim and Nabeelah, for their countless prayers, constant love, and endless support, which guided me through every step of my academic journey. My heartfelt thanks to my caring, loving, and supportive husband, Osama, who is always here for me, even when he is away. Your unlimited engagement and support have extended beyond words. Your sacrifices and understanding have made it possible for me to pursue and achieve my dreams. To my little angels, Hisham and Elaf, I would not have found the strength to overcome the challenges, pains, and tough times during my academic journey without you as my inspiration. Your presence, laughter, and hugs have been a constant source of joy and support. I love you both more than words can express, and I am immensely proud to be your mother. Lastly, I would like to express my deep gratitude to my brothers, Saud, Abdulaziz, Abdulwahab, and my sisters, Seba, Reem, Heba, and Shahad, for their emotional support, love, and understanding during my challenging times.

I want to acknowledge the kindness and support of my friends in Sydney. Your practical and emotional support and encouragement have been invaluable. Each one of you has played a unique role in shaping my journey, and the memories we have created will forever hold a special place in my heart, reminding me of the importance of real friendships.

Finally, I am thankful to Taibah University for their scholarship, and to my country for funding my education.

## Research Contribution and Publication

The research components of this thesis have been presented in a rigorously reviewed international conference and two scientific journals. The publication of these papers provided a valuable opportunity to review the work before incorporating it into this thesis.

Publication	State	Reference	Source
Publication 1	Published	ALABSI, M. I. & GILL, A. Q. 2021. A Review of Passenger Digital Information Privacy Concerns in Smart Airports. <i>IEEE Access</i> , 9, 33769-33781.	<a href="https://ieeexplore.ieee.org/document/9360741">https://ieeexplore.ieee.org/document/9360741</a>
Publication 2	In review	A systematic review of personal information sharing in smart cities: risks, impacts, and controls	Springer
Publication 3	Accepted	Integrated Interaction Journey and Privacy Risk Assessment: A Graph Model	CENTERIS



## Table of Contents

Certificate of Original Authorship .....	ii
Acknowledgment .....	iii
Research Contribution and Publication .....	iv
Table of Contents .....	v
List of Tables .....	x
List of Figure.....	xiii
List of Abbreviations .....	xv
Abstract .....	xvi
1 Chapter 1: Introduction .....	17
1.1 Research context .....	17
1.1.1 Smart airports.....	19
1.1.2 Personal information.....	20
1.1.3 Privacy .....	21
1.2 Research problem.....	22
1.2.1 Research gap .....	23
1.3 Research questions, aims, and objectives.....	24
1.4 Significance and scope .....	25
1.5 Contribution .....	27
1.5.1 The IJAPRA framework .....	27
1.5.2 Publication .....	29
1.6 Applications and users .....	29
1.7 Research strategy.....	29
1.8 Thesis outline .....	31
1.9 Summary .....	32
2 Chapter 2: Literature review .....	33
2.1 Literature review .....	33

2.1.1	Smart airports.....	33
2.1.2	Personal information.....	37
2.1.3	Privacy .....	40
2.1.4	Ontology .....	42
2.1.5	Knowledge graph.....	43
2.1.6	Graph-data models.....	45
2.1.7	Graph database.....	45
2.2	Systematic literature review .....	46
2.2.1	Passenger digital information privacy concerns in smart airports (Reported in (Alabsi & Gill 2021)).....	46
2.2.2	Personal information handling in smart cities: risks, impacts, and controls (SLR 2) 58	
2.3	Additional literature review .....	78
2.4	Research gaps.....	78
2.5	Summary .....	79
3	Chapter 3: Design science research .....	81
3.1	Background .....	81
3.2	Review of research methodologies .....	81
3.2.1	Action research .....	82
3.2.2	Grounded theory .....	82
3.2.3	Experimental research.....	82
3.2.4	Design science research (DSR).....	83
3.2.5	Rationale for choosing DSR .....	83
3.3	DSR: Methodology .....	84
3.4	Design guideline.....	85
3.5	Applying DSR in this research.....	87
3.5.1	Awareness of the problem.....	88
3.5.2	Suggestion.....	88

3.5.3	Development.....	89
3.5.4	Evaluation .....	91
3.5.5	Conclusion .....	96
3.6	Research ethics.....	97
3.7	Research validity and limitations .....	97
3.8	Summary .....	99
4	Chapter 4: The IJAPRA framework.....	100
4.1	The IJAPRA framework overview .....	100
4.2	The IJPRA ontology.....	103
4.2.1	Increment 1 - IJ ontology .....	105
4.2.2	Increment 2 - PR ontology.....	112
4.2.3	Increment 3 - integrated IJPRA ontology .....	117
4.3	The IJPRA architecture .....	125
4.3.1	Increment 4- IJ layer .....	126
4.3.2	Increment 5 - PR layer .....	132
4.4	Summary .....	139
5	Chapter 5: The IJAPRA framework evaluation.....	141
5.1	The IJAPRA framework evaluation overview .....	141
5.1.1	Iteration 1 .....	142
5.1.2	Iteration 2 .....	143
5.1.3	Iteration 3 .....	143
5.2	Iteration 1- IJAPRA framework alpha version.....	144
5.2.1	The IJPRA ontology alpha version .....	144
5.2.2	The IJPRA architecture alpha version.....	153
5.3	Iteration 2- IJAPRA framework beta version.....	154
5.3.1	IJPRA ontology beta version .....	154
5.3.2	Scenario 1: Individual adult passenger .....	156

5.3.3	Scenario 2: Teenage passenger .....	160
5.3.4	Scenario 3: Merchant passenger .....	162
5.3.5	Scenario 4: Special needs passenger.....	165
5.3.6	Scenario 5: Diplomatic passenger.....	168
5.3.7	Evaluation results in iteration 2 .....	171
5.3.8	The IJPRA architecture beta version.....	173
5.4	Analysis of the alpha and beta versions of the IJPRA framework. ....	175
5.5	Iteration 3- IJPRA framework Gamma version.....	179
5.5.1	Survey data collection.....	181
5.5.2	Survey data analysis.....	183
5.6	Summary .....	203
6	Chapter 6: Discussion and Conclusion .....	204
6.1	Research journey and main output.....	204
6.1.1	The research journey .....	205
6.1.2	Research output and insights .....	206
6.2	Implications.....	213
6.2.1	Implications for practice .....	213
6.2.2	Implications for the research.....	214
6.3	Key contributions and publications.....	214
6.4	Limitations and future work.....	215
6.5	Discussion of research validity .....	217
6.6	Conclusion and Summary .....	218
	Bibliography .....	219
	Appendices.....	232
	Appendix A- Second SLR selected studies.....	232
	Appendix B- Ethical approval .....	237
	Appendix C- Invitation letter .....	239

Appendix D- Online survey information sheet.....	240
Appendix E- Online field survey Questionnaire.....	242
Appendix F- Research data.....	248

## List of Tables

Table 1.1 Research questions, aims, and objectives .....	25
Table 2.1 Definitions of smart airport in the literature .....	35
Table 2.2 Definitions of privacy in the literature.....	42
Table 2.3 Graph model types .....	45
Table 2.4 Passenger journeys in the smart airport .....	48
Table 2.5 People involved in passenger's travel journey .....	49
Table 2.6 Processes which are implemented by passengers .....	50
Table 2.7 Passenger's digital information handled through the journey .....	51
Table 2.8 Enabling technology used for smart airport applications .....	52
Table 2.9 Privacy challenges for passenger information .....	53
Table 2.10 Current solutions.....	54
Table 2.11 Standards for passenger's information in the aviation industry .....	55
Table 2.12 GDPR and APPs privacy regulations in Australian and European airports .....	56
Table 2.13 Identified privacy threats .....	60
Table 2.14 Identified vulnerabilities .....	62
Table 2.15 Elements under AEA layers in smart health.....	63
Table 2.16 Elements under AEA layers in the smart grid .....	64
Table 2.17 Elements under AEA layers in the smart city.....	65
Table 2.18 Elements under AEA layers in smart business/Organisation .....	66
Table 2.19 Elements under AEA layers in smart government and smart transportation.....	66
Table 2.20 Identified privacy requirements .....	68
Table 2.21 Existing privacy controls .....	72
Table 2.22 Research Gaps.....	79
Table 3.1 DSR guidelines and their specific use in this research .....	85
Table 3.2 Evaluation criteria.....	92
Table 3.3 Survey rating.....	94
Table 3.4 Survey process .....	95
Table 4.1 Increments activities for developing the IJAPRA framework.....	101
Table 4.2 Adopted theoretical and practical lenses. ....	102
Table 4.3 IJ ontology concepts, sub-concepts, and their definitions (C is concept label; the SC label refers to sub-concept).....	106
Table 4.4 Mapping IJ concepts and sub-concepts with UFO concepts .....	109

Table 4.5 PR concepts, sub-concepts, and their definitions (C label refers to concept, SC is the sub-concept label). .....	112
Table 4.6 Mapping PR concepts and sub-concepts with UFO .....	114
Table 4.7 Emerged concepts for integrating IJ and PR ontologies and their definitions.....	117
Table 4.8 Mapping IJPRA emerged concepts with UFO concepts .....	118
Table 4.9 IJPRA – emerged relationships for integration purposes .....	118
Table 4.10 IJPRA ontology concepts used to design the IJ-Actor view.....	127
Table 4.11 IJPRA ontology concepts used to design the IJ-Technology view.....	128
Table 4.12 IJPRA ontology concepts used to design IJ-Process view .....	129
Table 4.13 Process stages and its activities .....	130
Table 4.14 IJPRA ontology concepts used to design the IJ-Information view.....	130
Table 4.15 IJPRA ontology concepts used to design the IJ-Factor view.....	132
Table 4.16 Description of privacy risk identification step.....	134
Table 4.17 Applicability Questions .....	135
Table 4.18 Description of privacy risk assessment process.....	138
Table 4.19 Description of the assessment level of each assessment component.....	139
Table 5.1 Summary of evaluation iterations methods and results .....	143
Table 5.2 IJ ontology (alpha) concepts and their definitions.....	144
Table 5.3 Emerged concepts and their definitions based on scenario results .....	148
Table 5.4 PR ontology (alpha) concepts and their definitions.....	149
Table 5.5 Emerged concepts for IJPRA ontology (alpha version) .....	151
Table 5.6 Scenario development process.....	154
Table 5.7 Description of persona types used in scenarios. ....	155
Table 5.8 Emerged concepts and their definitions based on scenario 1 results.....	158
Table 5.9 Emerged concepts and their definitions based on scenario 2 results.....	160
Table 5.10 Emerged concepts and their definitions based on scenario 3 results.....	163
Table 5.11 Emerged concepts and their definitions based on scenario 4 results.....	166
Table 5.12 Emerged concepts and their definitions based on scenario 5 results.....	169
Table 5.13 Description of the IJAPRA framework evaluation results in iteration 1 and 2 ...	176
Table 5.14 Participants’ years of experience .....	180
Table 5.15 Questionnaire set QS1-Applicability questions group.....	182
Table 5.16 Questionnaire set QS2-Understandability questions group.....	182
Table 5.17 Questionnaire set QS3- Usefulness questions group .....	182
Table 5.18 Questionnaire set QS4- Generalisability question group.....	182

Table 5.19 Questionnaire set QS6- Overall question group .....	182
Table 5.20 Questionnaire set QS5- Subjective feedback.....	183
Table 5.21 IJPRA applicability survey rating (CT1).....	185
Table 5.22 IJPRA applicability category rating (GT1).....	185
Table 5.23 IJPRA understandability survey rating (CT2) .....	186
Table 5.24 IJPRA understandability category rating (GT 2).....	187
Table 5.25 IJPRA usefulness survey rating (CT3) .....	188
Table 5.26 IJPRA Usefulness category Rating (GT 3).....	188
Table 5.27 IJPRA generalisability survey rating (CT4) .....	189
Table 5.28 IJPRA Generalisability category rating (GT 4).....	190
Table 5.29 Overall IJPRA framework rating (ORT 1) .....	191
Table 5.30 Subjective feedback on IJPRA (ST1) .....	193
Table 5.31 Participants' suggestions, their categories, and the responses (ST2).....	198
Table 6.1 IJPRA ontology output .....	208
Table 6.2 IJPRA architecture output.....	210
Table 6.3 Key contributions of this thesis .....	215



## List of Figure

Figure 1.1 Research context.....	19
Figure 1.2 Research gaps .....	23
Figure 1.3 IJAPRA framework overview .....	27
Figure 1.4 Research strategy.....	30
Figure 1.5 Research outline .....	31
Figure 2.1 Evolution of the airport industry .....	37
Figure 2.2 The stages of passenger journey.....	47
Figure 2.3 Mapping CFIP dimensions with AEA layers in smart health .....	63
Figure 2.4 Mapping CFIP dimensions with AEA layers in the smart grid.....	64
Figure 2.5 Mapping CFIP dimensions with AEA layers in smart city .....	65
Figure 2.6 Mapping CFIP dimensions with AEA layers in smart business/Organisation.....	65
Figure 2.7 Existing privacy controls.....	69
Figure 3.1 DSR Methodology.....	84
Figure 3.2 Awareness of the problem step.....	88
Figure 3.3 Suggestion step.....	89
Figure 3.4 Development step.....	90
Figure 3.5 Evaluation Step.....	92
Figure 3.6 Scenario development and documentation.....	93
Figure 3.7 Conclusion step .....	97
Figure 4.1 High-level conceptual view of the IJAPRA framework.....	100
Figure 4.2 IJPRA ontology conceptual view .....	104
Figure 4.3 IJ ontology concepts-relationships matrix.....	110
Figure 4.4 IJ graph-based model.....	111
Figure 4.5 PR ontology concepts-relationships matrix.....	115
Figure 4.6 PR graph-based model.....	116
Figure 4.7 IJPRA ontology structure .....	117
Figure 4.8 IJPRA concepts- relationships matrix .....	120
Figure 4.9 Organising the IJPRA concepts into metamodel layers (M2, M1, M0).....	122
Figure 4.10 IJPRA graph-based model.....	123
Figure 4.11 IJPRA architecture conceptual view .....	125
Figure 4.12 IJ-Actor view .....	127
Figure 4.13 IJ-Technology view .....	128

Figure 4.14 IJ-Process view .....	129
Figure 4.15 IJ-Information view .....	131
Figure 4.16 IJ-Factor view .....	132
Figure 4.17 Input and Output of PRIdentification tool.....	133
Figure 4.18 Process of privacy risk identification .....	134
Figure 4.19 Input and output of PRAssessment tool .....	137
Figure 4.20 Process of privacy risk assessment.....	137
Figure 5.1 IJAPRA evaluation iterations and methods.....	142
Figure 5.2 IJ graph-based model (alpha version).....	146
Figure 5.3 Scenario 1 implementation – iteration 1.....	147
Figure 5.4 Scenario 1 results- iteration 1 .....	148
Figure 5.5 IJPRA graph-model (alpha version).....	152
Figure 5.6 IJPRA architecture (alpha version) .....	153
Figure 5.7 Scenario 1 implementation – iteration 2.....	157
Figure 5.8 Scenario 1 results- refined IJ graph-based model (alpha version) .....	159
Figure 5.9 Scenario 2 implementation – iteration 2.....	161
Figure 5.10 Scenario 2 results- refined IJPRA graph-based model (alpha version).....	162
Figure 5.11 Scenario 3 implementation- iteration 2 .....	164
Figure 5.12 Scenario 3 results- refined IJPRA graph-based model (alpha version).....	165
Figure 5.13 Scenario 4 implementation- iteration 2 .....	167
Figure 5.14 Scenario 4 results- refined IJPRA graph model (alpha version) .....	168
Figure 5.15 Scenario 5 implementation- iteration 2 .....	170
Figure 5.16 Scenario 5 results- refined IJPRA graph model (alpha version) .....	171
Figure 5.17 IJPRA ontology beta version.....	172
Figure 5.18 IJPRA architecture beta version .....	173
Figure 5.19 IJPRA applicability rating graph (CF1) .....	185
Figure 5.20 IJPRA understandability rating graph (CF 2).....	187
Figure 5.21 JPra Usefulness Rating Graph (CF3).....	188
Figure 5.22 IJPRA Generalisability rating (CF 4).....	190
Figure 5.23 Overall IJPRA architecture overall rating Graph (ORF 1).....	192
Figure 6.1 Research journey .....	206

## List of Abbreviations

<b>Abbreviation</b>	<b>Description</b>
GDPR	General Data Protection Regulation
PDPL	Saudi Arabia's Personal Data Protection Law
PII	Personally Identifiable Information
PNR	Passenger's Name Record
API	Advanced Passenger Information
AI	Artificial Intelligent
IoT	Internet of Thing
RFID	Radio-Frequency Identification
CFIP	Concerns for Information Privacy
EU	European Union
ICAO	International Civil Aviation Organisation
PETs	Privacy Enhancing Technologies
ICT	Information and Communication Technology
PbD	Privacy by Design
CIA	Confidentiality, Integrity, availability
IAAA	Identification, Authentication, Authorisation, Accounting
NIST	National Institute of Standards and Technology
DSR	Design Science Research
CJM	Customer Journey Map
AEA	Adaptive Enterprise Architecture
UFO	Unified Foundational Ontology
LINNDUN	Threat modelling framework
IJAPRA	Interaction Journey Architecture and Privacy Risk Assessment
IJPRA	Interaction Journey and Privacy Risk Assessment
IJ	Interaction Journey
PR	Privacy Risk

## Abstract

Privacy of information has become a critical concern in the contemporary complex digital ecosystems or environments. Smart airport is an example of a digital ecosystem or environment, in which its digitally interconnected systems play a key role in facilitating and improving the quality of service provided to passengers. In smart airport, actors interact with technologies to handle several types of personal passenger information at each stage of their interaction journey. However, passengers' information in smart airport may result in passengers suffering from serious privacy risks that may compromise their information and affect their privacy. This research conducted a comprehensive review that revealed a lack of common understanding and assessment of privacy risks associated with passenger information in the context of smart airport. Thus, this thesis aims to address this important research gap by proposing an Interaction Journey Architecture and Privacy Risk Assessment (IJAPRA) framework. The proposed framework provides new knowledge and understanding of privacy risks linked to the personal information of passengers in smart airports and assists in assessing privacy risks relevant to passenger information in smart airport. This research applied a well-known design science research (DSR) method for developing and evaluating the IJAPRA framework in short increments.

The proposed IJAPRA framework consists of the following 2 main components: (1) Interaction Journey and Privacy Risk Assessment (IJPRA) ontology, and (2) IJPRA architecture. The IJPRA ontology is developed to conceptualise and capture the knowledge of the complex passenger interaction journey and associated privacy risks in the smart airport. The IJPRA architecture comprises the Interaction Journey (IJ) and Privacy Risk (PR) layers, which are designed based on the IJPRA ontology concepts. The IJPRA architecture offers a set of elements and their relationships involved in the passenger interaction journey. This will facilitate the identification, understanding and assessment of privacy risks arising during the passenger journey.

The evaluation of the proposed framework is conducted using two DSR evaluation methods: illustrative scenarios and expert evaluation via field survey through three iterations where each iteration resulted in an updated version of the IJAPRA framework based on the evaluation results. The results of this thesis indicate that the proposed IJAPRA framework is applicable and appropriate to capture the knowledge relevant to the domain of passenger interaction journey and associated privacy risks in smart airport. In conclusion, overall results indicate that the proposed framework addressed the identified research question and gap in hand.

# 1 Chapter 1: Introduction

Information privacy has become an important and critical concern in increasingly sophisticated digital environments, such as smart airports, to protect personal information (Avancha, Baxi & Kotz 2012; Bélanger & James 2020). This complex, interconnected digital system utilises advanced technologies to enhance the passenger's experience and provide high quality services (European Union Agency for Network and Information Security 2016; Straker & Wrigley 2018). In a smart airport, several types of passenger information are handled because of the interaction between the several actors and technologies involved in the passenger journey (Bouyakoub et al. 2017; Kalakou, Psaraki-Kalouptsidi & Moura 2015). Thus, understanding the privacy risks that may arise during information-handling activities is needed in interconnected digital systems, such as smart airports (Makhdoom et al. 2020). This research aims to address this important issue by presenting an Interaction Journey Architecture and Privacy Risk Assessment (IJAPRA) framework. The proposed framework provides new knowledge and assists in understanding the privacy risks linked to the personal information of passengers which is digitally handled in smart airports.

This chapter presents an introduction to the research area and a preview of the whole of the research in this thesis. In Section 1.1, the research context is presented. Section 1.2 explains the research problem and research gaps, followed by the research questions, aims, and objectives in Section 1.3. Sections 1.4 and 1.5 provide an explanation of the significance and scope, and the contribution of this research, respectively. Section 1.6 outlines the application and uses of IJAPRA. Section 1.7 discusses the research strategy used in this thesis and Section 1.8 presents the thesis outline. Finally, Section 1.9 overviews the structure of the remaining chapters in this thesis.

## 1.1 Research context

The research presented in this thesis is conducted in the field of information technology, particularly in the area of information privacy management, and architecture. According to Orlikowski & Barley (2001), information technology (IT) research aims to develop practical solutions that have a positive impact on people's lives and on various industries, addressing real-world problems similar to how design-oriented fields such as engineering and architecture approach their challenges. Information technology generally refers to the use of computers, software, and other digital technologies to process, store, and transmit information (Orlikowski & Barley 2001; Velliari & Coleman-George 2016, p. 324). Information privacy management

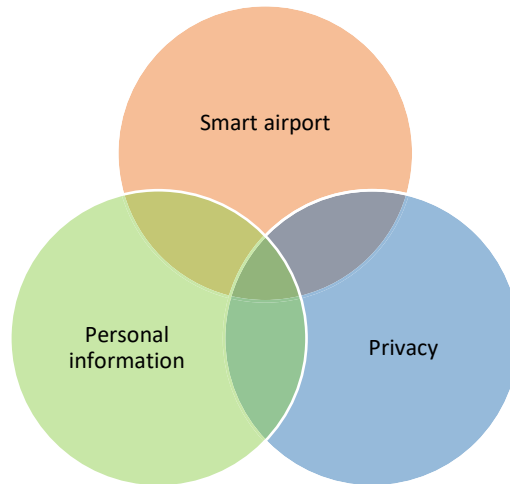
encompasses various strategies, policies, and procedures that aim to manage and protect information and ensure privacy (Duncan et al. 2022; Papamartzivanos et al. 2021). Architecture refers to the key concepts and properties of a system that are represented in its components, relationships, and principles to reflect its environment and the way it has developed and improved (Dumitriu & Popescu 2020; Gill 2022).

Smart airports represent a revolutionary paradigm in the aviation industry, seamlessly merging IT and emerging technologies to reimagine the way airports operate and cater to passengers (Kılıç, Üçler & Martin-Domingo 2021; Straker & Wrigley 2018). A typical smart airport comprises five stages in the passenger journey each of which is supported by different emerging technologies, such as self-service, biometrics, and automated services technologies, which are enabled by many underlying technologies to enhance passenger convenience (Bogicevic et al. 2017; Karakuş, Karşıgil & Polat 2019; Rajapaksha & Jayasuriya 2020). During this journey, different types of passenger information are collected and handled by various stakeholders, including airlines and government agencies. They play vital roles at each stage of the journey, for instance, airlines handle check-in, bag drop, and boarding, while government agencies manage security and border control (Bogicevic et al. 2017; Chang-Ryung, McGauran & Nelen 2017).

The handled information includes identity information such as biographic or biometric, and travel information (Khi 2020; Labati et al. 2016).

Based on the preceding discussion, it is clear that passengers interact with many elements at each stage of their journey through a smart airport. During this interaction journey, diverse types of passenger personal information are collected and handled by several stakeholders, using different technologies. However, handling passengers' personal information in interconnected digital systems, such as a smart airport, may result in passengers facing serious privacy risks that compromise their personal information and impact their privacy (Martinez-Balleste, Perez-Martinez & Solanas 2013; Sharma et al. 2020).

As studies lack a common understanding of the privacy risks associated with passenger information in smart airports, this research addresses the issue of privacy risk in such settings with a primary focus on the privacy of personal information. The research context is developed by conceptualising the related major elements such as smart airports, personal information, and privacy, as shown in Figure 1.1.



*Figure 1.1 Research context*

### 1.1.1 Smart airports

The continuous development in the airport industry is a result of the progressive growth in global passenger traffic. In 2022, total passenger traffic increased by 76.2% compared to 2021, exceeding the long-run industry average rate (International Air Transport Association 2022). Air traveller numbers are projected to hit 8.2 billion by 2037 (Coleman 2018). Accordingly, there is a massive strain on existing airport facilities, requiring airport operators to rethink their traditional structures to optimise their operations, increase capacity, expand revenues, and improve the passenger experience, while ensuring physical and digital cybersecurity (Nau & Benoit 2017). As such, technology offers a mechanism for cooperation between airport facility design and digital innovation and automation to help personalise customer experiences; hence the concept of the smart airport emerges. The modern airport uses a range of technologies such as self-service, flight information systems, baggage tracking, and smart parking within the overall context of smart airports (AlMashari et al. 2018; Bouyakoub et al. 2017; Nau & Benoit 2017; Shehieb et al. 2017).

A smart airport leverages information and communication technologies (ICT) to facilitate efficient, rapid, and high-quality services for passengers by utilising networked, data-driven responses and automated features, ultimately enhancing the overall passenger experience throughout the journey (European Union Agency for Network and Information Security 2016; Straker & Wrigley 2018). It offers a portfolio of automated services with regard to check-in, baggage management, flight bookings, and security checks. The digitisation process in the airport industry arose in the 1980s from the need to share IT facilities between ground handlers and airlines across the airport (Nau & Benoit 2017). Hence, in this research, the smart airport definition is adopted from the literature (European Union Agency for Network and Information

Security 2016; Straker & Wrigley 2018) and is defined as an interconnected complex digital system (or a system of systems) that uses digital technologies, information, and processes to improve the passengers' travel experience.

The primary objective of the majority of smart airports is to enhance passenger journeys by offering efficient processes and technologies for handling passenger information (Fattah et al. 2009; International Air Transport Association 2018). Consequently, as digital interactions increase, the experience of both passengers and operators is likely to improve. Given that most airports adopt this strategy, the smart airport concept envisioned for the future is rapidly becoming a present-day reality. However, the handling of passengers' personal information in smart airports may result in passengers experiencing serious privacy risks that could compromise their personal information and negatively impact their privacy (Martinez-Balleste, Perez-Martinez & Solanas 2013; Sharma et al. 2020). The following discusses personal information, one of the main terms used in this research.

### 1.1.2 Personal information

Recently, advances in interconnected systems and a growing dependence on technology have made personal information more vulnerable than ever before (Holender, Sutton & De Simoni 2018). The use of technology amplifies the risk to privacy, as personal information is now collected, handled, and easily linked across various platforms and technologies, which has led to heightened privacy concerns regarding personal information (Leonard 2014).

Personal information encompasses all details regarding individuals that could enable their identification, either directly from the information itself or through the amalgamation and additional information that is under the control or anticipated control of the individual managing the information (Herrera et al. 2021; Milne et al. 2017). Hence, this research focuses on personal information in a digital format.

Personal information encompasses many different types of information. The categories of personal information have been presented by many scholars. For instance, Ambrose (2012); Veghes et al. (2012) classified personal information as: demographic, psychometric, and identity. According to a comprehensive review conducted by Chua, Ooi & Herbrand (2021), the selected studies discussed various types of personal information, including medical, biometric, financial, demographic, and Personally Identifiable Information (PII). According to Chuleeporn (2008), PII is the heart of personal information and requires specific protection considerations. These are only a few of the many categories that fall under the general umbrella



of personal information. More details about personal information categories are discussed in Chapter 2.

In the context of the smart airport, most of the aforementioned personal information types are handled during the interaction journey in smart airports and shared among different stakeholders. This clearly demonstrates the complexity around the handling of personal and sensitive information of passengers in smart airports, and how passengers can be put at risk of privacy breaches.

In order to solve the complex privacy concerns surrounding personal information in interconnected systems and to ensure the privacy rights of both individuals and businesses are respected, ongoing research and a dedication to data protection procedures are required. The following discusses privacy as one of the main terms used in this research.

### 1.1.3 Privacy

Privacy is a common topic discussed in the literature (Krishnamurthy & Wills 2010; Norberg, Horne & Horne 2007; Pavlou 2011; Smith, Milberg & Burke 1996). Numerous studies have explored various facets of privacy, which is indicative of the importance of privacy in contemporary digital interconnected systems (Tlacuilo Fuentes 2020).

The concept of privacy is multifaceted and can be studied from various perspectives including economics, management, law, and information systems. It encompasses different dimensions such as bodily, territorial, communications, and information privacy (Corcoran 2017; Martinez-Balleste, Perez-Martinez & Solanas 2013; Panahi Rizi & Hosseini Seno 2022). However, other forms of privacy include privacy of location, state of body and mind, social life, behaviours and action, and media (Eckhoff & Wagner 2018; Finn, Wright & Friedewald 2012). These categories highlight the complexity of privacy and the need for nuanced protection mechanisms across various domains and activities. Concerns for information privacy gained traction after the widespread processing of digital information began in the 1960s (Li & Palanisamy 2018). This research focuses on information privacy which pertains to the protection of individual personal information (Panahi Rizi & Hosseini Seno 2022). This emphasis on information privacy reflects a growing concern in the digital age, where the proliferation of interconnected systems and technologies has led to increased privacy risks associated with personal information. The concept of information privacy refers to an individual's power to regulate their personal information (Fried 1970, p. 209; Hoffman 1973; Martinez-Balleste, Perez-Martinez & Solanas 2013). Conversely, information privacy concern indicates individuals worry about an

Organisation's activities related to the acquisition and utilisation of personal data (Smith, Milberg & Burke 1996; Xu et al. 2011).

This research addresses the matter of information privacy, which is a significant issue that can be associated with smart airports and their underlying technologies to comprehend passengers' concerns about the handling of their personal information in the smart airport.

## 1.2 Research problem

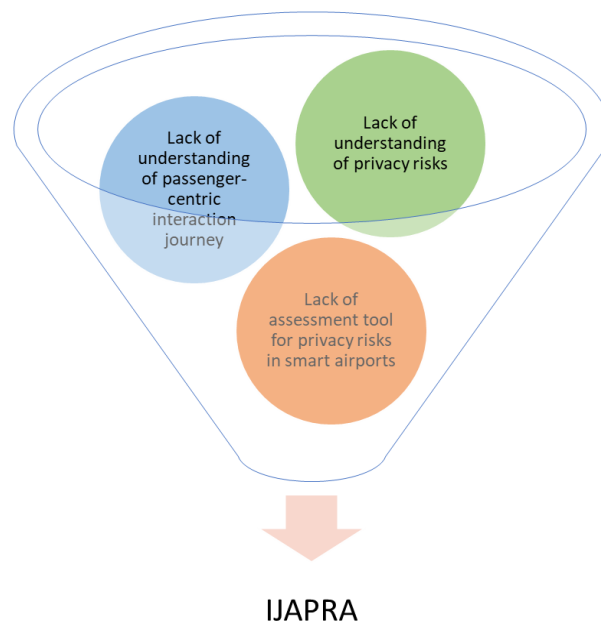
A smart airport is defined as an interconnected digital system that implements efficient solutions and processes to provide an efficient and convenient travel experience for passengers during their journey (European Union Agency for Network and Information Security 2016; Gill 2015b; Straker & Wrigley 2018). By using these technologies, passenger information is collected, processed and stored by airport and airline systems, and also shared by various stakeholders, including airline companies, government agencies, and service providers (Anand et al. 2017; Bogicevic et al. 2017; Chang-Ryung, McGauran & Nelen 2017; Labati et al. 2016). This information includes personal and sensitive information about passengers, such as PII, medical, financial, and biometric information (Alabsi & Gill 2021; Anand et al. 2017; Chua, Ooi & Herbland 2021). If passenger information is revealed as a result of accidental and intentional threats, such as unauthorised access, misuse, and secondary uses, this raises a unique set of concerns related to information privacy and data protection (Alabsi & Gill 2021; Chang-Ryung, McGauran & Nelen 2017). These threats pose several privacy risks that affect passengers and their information. From time to time, there is news about airlines and airport information being compromised, putting the privacy of passengers and their information at risk. For example, in 2018, British Airways suffered a massive cyberattack, which led to the theft of the credit card information of nearly 380,000 passengers. As a result, passengers suffered significant financial losses, and the company lost its reputation and customers' trust (Vivek Kumar 2019). Another example occurred in 2021, when Société Internationale de Télécommunications Aéronautiques (SITA), a leading provider of airline technology that manages various passenger processes from ticket booking to boarding in smart airports, announced a significant cyberattack on its servers, affecting major airlines and potentially compromising the personal information of more than 2 million passengers. Most victims were part of frequent flyer programs, and the basic passenger information at risk included personal information such as program card numbers and their names. SITA took immediate action by notifying affected PSS customers and related Organisations (CnSight 2021). The majority of passengers are concerned about the privacy of their information during their journey through a smart airport, as their personal information can

be revealed from different sources, including their e-travel documents (Kenn Anthony Mendoza 2023). Privacy threats, including unauthorised access and improper use, can exploit passenger information and lead to privacy risks that can have serious consequences for passengers and their information. Thus, it is vital for airports, airlines, service providers, and regulatory bodies to collaborate to understand the potential privacy risks impacting passengers and their information and implement best practices to reduce the impact of the risks.

The research problem to be addressed in this research underscores the research gaps regarding the need to understand the privacy risks associated with passenger information in the context of smart airports.

### 1.2.1 Research gap

As a result of our comprehensive review (see Chapter 2), we found that the existing studies lack an understanding of the privacy risks in smart airports. The research gaps are presented in Figure 1.2.



*Figure 1.2 Research gaps*

- There is a lack of a research-based systematic conceptualisation and understanding of the elements involved in complex passenger-centric interaction journeys in smart airports.
- There is a lack of a common, systematic understanding of the privacy risks associated with passenger information in smart airports.
- There is a lack of research-based assessment tools to help assess the privacy risks associated with passenger information in smart airports.

As airports continue to embrace digital transformation, the concerns of passenger information privacy is increasing. This study aims to address this critical problem and fill the gaps by offering insights and solutions that could shape the future of smart airport design and operation and ensure a balance between convenience and privacy.

### 1.3 Research questions, aims, and objectives

This section includes the research questions, aims, and objectives of this research. In Design Science Research (DSR), "design" signifies a purposeful, iterative process for creating and assessing artifacts to solve real-world problems (Hevner et al. 2004). These artifacts encompass frameworks, models, methods, architectures, constructs, and instantiations (Vaishnavi & Kuechler 2015). Architecture, a key artifact in DSR, refers to high-level structures representing key concepts and relationships within a system's environment (Dumitriu & Popescu 2020; Gill 2022; Vaishnavi & Kuechler 2015). In the context of this research, the main problem is the lack of understanding of privacy risks related to passenger information in smart airports. This problem is addressed by the designated artifact, which is the architecture focused on depicting the concepts and relationships of the passenger interaction journey within the smart airport. Consequently, the main research question is formulated as follows:

**RQ: How to design the passenger interaction journey architecture and assess the associated information privacy risks in the context of the smart airport?**

The following sub-questions were devised to address the main research question:

RQ1: How to model the knowledge of the domain of privacy risk associated with passenger information during their interaction journey in a smart airport?

RQ2: How to design the passenger interaction journey architecture in a smart airport?

RQ3: How to assist in the assessment of privacy risks associated with passenger's information during their interaction journey in a smart airport?

The main aim of this research derived from the aforementioned main research question is to develop a consolidated framework, the IJAPRA framework, which assists in understanding the passenger interaction journey and analysing the associated privacy risks relevant to passenger information. Table 1.1 maps the research questions with the corresponding aims and objectives.

The aims of this research in light of the aforementioned research questions are:

RA1: To capture knowledge of the domain of the passenger interaction journey and associated privacy risks in the smart airport context.

RA2: To design the passenger interaction journey architecture in the smart airport context.

RA3: To assist in assessing the privacy risks associated with passenger information in the smart airport context.

This study sets the following objectives to achieve the aforementioned research aims:

RO1: Conduct a systematic literature review (SLR) to identify the elements involved in the passenger interaction journey in a smart airport.

RO 2: Conduct an SLR to identify the privacy risks associated with personal information under different smart city themes, including smart airports.

RO 3: Represent the knowledge of the domain of the passenger interaction journey and associated privacy risks in the smart airport context.

RO 4: Develop a passenger interaction journey architecture for a smart airport.

RO 5: Assess the privacy risks associated with passenger information in a smart airport.

*Table 1.1 Research questions, aims, and objectives*

<b>Research Q</b>	<b>Research Aim</b>	<b>Research O</b>
How to model the knowledge of the domain of privacy risk associated with passenger information during their interaction journey in a smart airport?	To capture the knowledge of the domain of the passenger interaction journey and associated privacy risks in the smart airport context.	<ul style="list-style-type: none"> <li>- Conduct an SLR to identify the elements involved in the passenger interaction journey in smart airports.</li> <li>- Conduct an SLR to identify the privacy risks associated with personal information under different smart city themes including smart airports.</li> <li>- Represent knowledge of the domain of the passenger interaction journey and associated privacy risks in the smart airport context.</li> </ul>
How to design the passenger interaction journey architecture in a smart airport?	To design the passenger interaction journey architecture in the smart airport context.	Develop the passenger interaction journey architecture in a smart airport.
How to assist in the assessment of the privacy risks associated with passenger's information during their interaction journey in a smart airport?	To assist in assessing the privacy risks associated with passenger information in the smart airport context.	Assist in assessing the privacy risks associated with passenger information in a smart airport.

## 1.4 Significance and scope

This section summarises the research significance and scope. The protection of personal information during digital interactions and upholding an individual's fundamental rights in

digital environments are crucial for ensuring that personal data are handled with care and integrity, making information privacy a complex and important concern (Li & Palanisamy 2018). The research started with a broader topic on the importance of information privacy in smart airports. As the research progressed, the focus narrowed to the passenger interaction journey and the privacy risks associated with a passenger's personal information. The scope of this research includes the development of a consolidated framework to design the passenger interaction journey architecture and assist in assessing the privacy risks associated with passengers' personal information in smart airports. The scope of this research is limited to identifying and analysing privacy risks associated with passengers' personal information during their interaction journey on the departure side of domestic and international travel at a smart airport, and the risks associated with non-personal information are beyond the scope of this research. The passenger journey on the arrival side as well as risk mitigation and compliance analysis are outside the scope of this research. This research adopts the method of DSR (Hevner et al. 2004; Vaishnavi & Kuechler 2015) to develop and evaluate the proposed framework. This research is not restricted to a particular geographical area.

The scope of this research is as follows:

1. An Interaction Journey and Privacy Risk Assessment (IJPRA) ontology:
  - a. To identify relevant key concepts and relationships with the elements involved in the passenger interaction journey.
  - b. To identify key concepts and relationships of privacy risks affecting passenger information during their interaction journey in a smart airport.
2. The IJPRA architecture:
  - a. To design an interaction journey architecture based on the concepts in the IJPRA ontology.
  - b. To develop privacy risk tools:
    - i. to assist in identifying the privacy risks associated with passenger information in the smart airport context.
    - ii. to assist in analysing the identified privacy risks.

This research provides new knowledge and a holistic understanding of the passenger interaction journey and privacy risks associated with passenger information in the smart airport context by developing the novel IJAPRA framework consisting of two components: IJPRA ontology and IJPRA architecture.

## 1.5 Contribution

This section summarises the key contributions of this research. As shown in Figure 1.3, this research proposes an IJAPRA framework as the main contribution of this research.

The proposed IJAPRA framework is developed based on the relevant existing studies and theoretical and practical lenses, as well as expert evaluation feedback. The framework will assist privacy experts in identifying and analysing the privacy risks which will assist in designing the best privacy solutions relevant to passenger information in the smart airport. The proposed framework is unique because it provides new knowledge and an understanding of the privacy risks associated with passenger information in a smart airport, which contributes to the body of knowledge on information privacy management and architecture. The proposed IJAPRA framework consists of the following components: the IJPR and the IJPR architecture (as discussed in Chapter 4). The proposed framework addresses the research problem and the aforementioned research gaps (see Section 1.2). The contribution of this research is discussed in the following subsection.

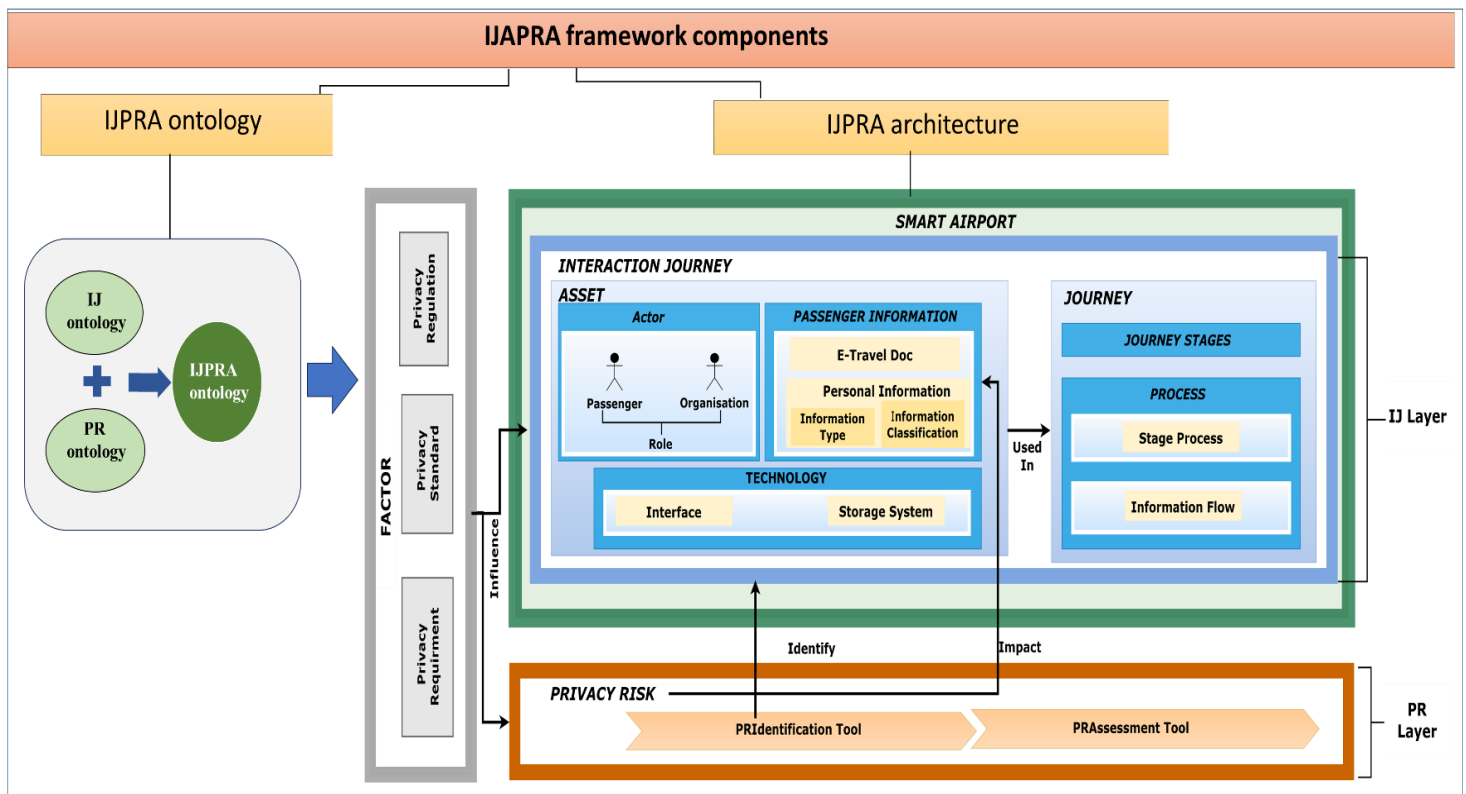


Figure 1.3 IJAPRA framework overview

### 1.5.1 The IJAPRA framework

As previously discussed, the development of the IJAPRA framework is the main contribution in this research. A brief description of the framework component presented in Figure 1.3 is as

follows. The details of the development of the final version of the framework are discussed in Chapter 4.

### ***IJPRA ontology***

The IJPRA ontology is a crucial component of the IJAPRA framework, as depicted in Figure 1.3. The IJPRA ontology is the outcome of the integration of two main components: the Interaction Journey (IJ) and Privacy Risk (PR) ontology and is developed to capture the knowledge of the passenger interaction journey and associated privacy risks in the smart airport. The IJPRA ontology and its integrated components, the IJ and PR ontologies, are represented using a graph-based modelling approach and implemented using the Neo4j graph. The graph modelling approach is appropriate as it provides a flexible structure to model elements relevant to the interaction journey and privacy risks, and their connections (Gill 2022). The IJPRA ontology can be utilised as a tool to conceptualise, analyse, and communicate the privacy risks in smart airports.

### ***IJPRA architecture***

The IJPRA architecture is the second component of the IJAPRA framework, as illustrated in Figure 1.3. The IJPRA is an architecture comprising IJ and PR layers and designed based on IJPRA ontology concepts. The IJ layer in a smart airport offers a comprehensive overview of assets and journey elements, encompassing the various stages and activities involved in the passenger interaction journey. This layer is primarily composed of two essential components, assets and journeys, which are organised into five views: IJ-Actor, IJ-Technology, IJ-Process, IJ-Information, and IJ-Factor. These views illustrate and provide details regarding the components within the IJ layer to facilitate the identification of privacy risks that arise during the journey and the development of effective privacy solutions. The PR layer involves two components: the PRIdentification and PRAssessment tools, which guide the identification and assessment of the privacy risks associated with passenger information in the smart airport.

The evaluation of the IJAPRA framework underwent three iterations using two well-known DSR evaluation methods: an illustrative scenario and expert evaluation via a field survey. The development and documentation of the illustrative scenario evaluation method (see Chapter 3) were used to evaluate the proposed artifact as another contribution of this research. The evaluation of the IJAPRA framework is covered in detail in Chapter 5.



### 1.5.2 Publication

A publication in a peer-reviewed journal is one of the contributions of this research (Alabsi & Gill 2021). In addition, one publication has been accepted in a conference, while another paper has been submitted to high-ranking journal and it is currently under review.

## 1.6 Applications and users

This section outlines the IJAPRA framework applications and its users. The IJAPRA framework is intended to be used by privacy experts, including privacy architects and solution designers, as well as researchers interested in the privacy area. The framework, comprising ontology and architecture, serves as a robust tool for systematically understanding the types of passenger information being handled, how it is collected, stored, and used during the journey, and managing the privacy risks associated with passenger information in the context of smart airports. Privacy experts and researchers can use the IJAPRA ontology to define and understand the complex relationships between various concepts within the smart airport domain. This foundational understanding is crucial for identifying who and what is involved during the passenger-centric journey. This understanding helps to identify potential privacy risks impacting passengers and their information. In addition, privacy experts and researchers can leverage the ontology to define and understand the intricate relationships between various privacy domain concepts. On the other hand, the IJAPRA architecture provides a systematic approach for mapping the passenger interaction journey and identifying and analysing privacy risks in the smart airport context. Privacy experts can also use the IJAPRA architecture to evaluate the likelihood of measuring the probability of a potential privacy threat affecting passenger information and causing privacy risks, and the potential impact of each identified risk. This can include physical, material, and moral damage as well as their consequences. Then, the overall risk level is prioritised to help manage privacy risks in a way that is tailored to the smart airport context and needs, balancing the need to protect passenger information within the smart airport operational and strategic requirements. Based on risk identification and analysis, targeted controls and measures can be designed and implemented to mitigate the prioritised risks. This can include technological solutions, policy changes, training, and awareness programs.

## 1.7 Research strategy

This section provides a summary of the research strategy employed to develop and evaluate the IJAPRA framework. The main research question of this thesis is: **How to design the passenger interaction journey architecture and assess the associated information privacy risks in the context of a smart airport?** This research question is divided into three sub-

questions to fill the gaps highlighted in Section 1.2.1. To address this question, this research presents the IJAPRA framework, the main research contribution, which has been briefly explained in Section 1.5. Figure 1.4 illustrates an overview of the research strategy in this research.

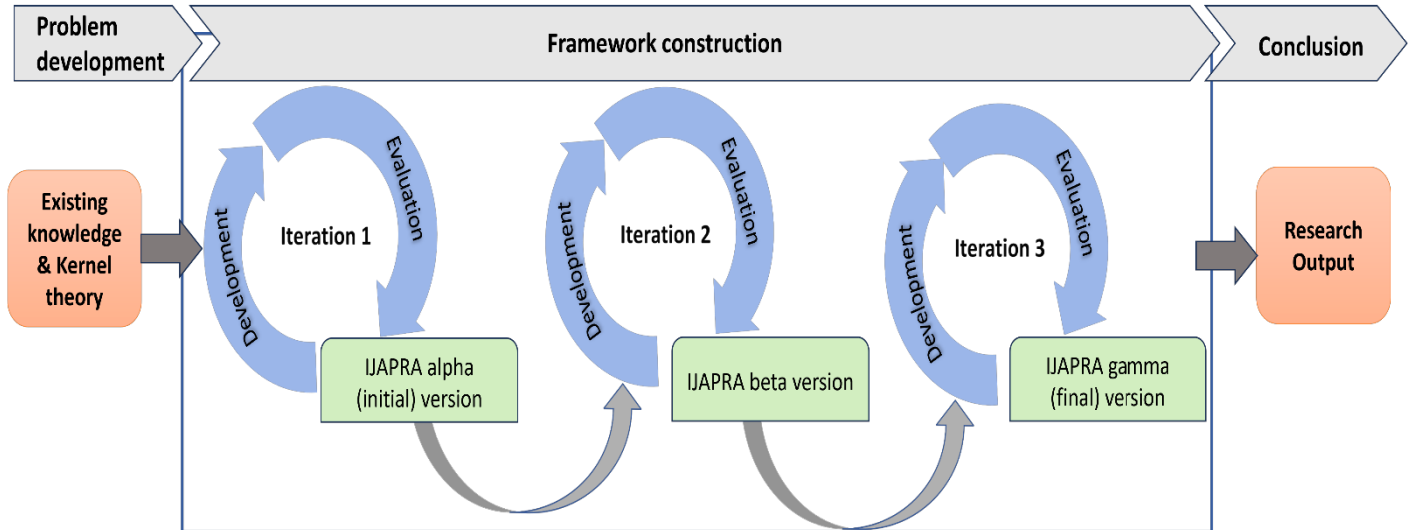


Figure 1.4 Research strategy

The DSR is selected as the most suitable approach for developing and evaluating the IJAPRA framework proposed in this research. The reason for using DSR in this research is that it offers an iterative process that assists and facilitates the development and evaluation of the proposed solution to solve the research problem in hand, relying on theories grounded in kernel theories and existing knowledge (Hevner et al. 2004; Kotzé, van der Merwe & Gerber 2015; Peffers et al. 2012). The DSR process adopted in this thesis is that presented by Vaishnavi & Kuechler (2015) along with the guidelines proposed by Hevner et al. (2004) to assist in conducting and evaluating the DSR process. As shown in Figure 1.4, the DSR methodology implemented in this research consists of three phases: problem development, framework construction, and conclusion. Phases One and Two (problem development and framework construction) are drawn from existing studies, relevant kernel theories, and well-known standards relevant to privacy. To generate awareness of the research problem, an SLR was conducted to comprehensively understand the research domain and to analyse the relevant studies to identify the research gaps and formalise the research problem (see Chapters 1 and 2). This was followed by proposing the initial design as a problem solution and choosing the appropriate tool to develop the proposed solution under the suggestion process. In this research, the IJAPRA framework was proposed to provide a practical solution to the research questions in hands. The IJAPRA framework consists of two components: the IJPRA ontology and the IJPRA

architecture. Then, the IJAPRA framework was developed incrementally to answer the research questions (RQ1, RQ2, and RQ3) identified in Section 1.3. The development involved a review of the relevant kernel theories, well-known privacy standards, and existing studies to develop a rigorous solution or artifact for the intended purpose. The development of the IJAPRA framework was organised in five increments: three increments for the development of the IJPRA ontology, and the remaining two increments for IJPRA architecture development. The development of the IJAPRA framework is discussed in Chapter 4 of this thesis.

The proposed framework is evaluated using two DSR evaluation methods: illustrative scenario and expert evaluation via a field survey. An evaluation was implemented to determine whether the proposed framework met the predetermined evaluation criteria, including applicability, usefulness, understandability, and generalisability. During the evaluation process, each iteration resulted in an updated version of the IJAPRA framework: alpha (initial), beta, and gamma (final), based on the evaluation results. The gamma version is the final version of the IJAPRA framework, discussed in Chapter 4. Finally, the research contribution, limitations, and future works are outlined in the conclusion.

## 1.8 Thesis outline

This section presents an overview of the thesis outline. As illustrated in Figure 1.5, this thesis is organised into six chapters.

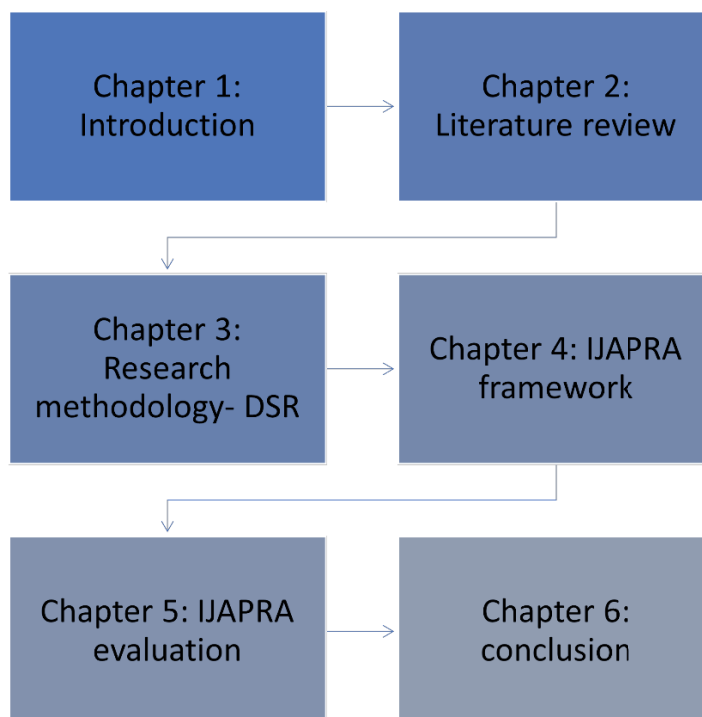


Figure 1.5 Research outline

Chapter 1 introduces the thesis by covering the research context, research problem and gaps, research questions, research aims and objectives, research significance and scope, research contributions, research applications and users, research strategy, and research outline. Chapter 2 presents a literature review to gain a deeper understanding of the research topic and discusses the analysis and results of the two systematic literature reviews (SLRs) conducted to identify the research gaps. Chapter 3 presents DSR as the research methodology adopted in this research. Chapter 4 discusses the development of the gamma (final) version of the IJAPRA framework, which is the main thesis contribution. Chapter 5 presents the evaluation methods used to evaluate the IJAPRA framework. Chapter 6 highlights the research output and insights, theoretical and practical implications, publications, limitations, and directions for future research. The appendices include selected studies (Appendix A) for the second SLR discussed in Chapter 2, ethical approval forms (see Appendices B, C, and D), online survey questionnaire (Appendix E), and research data (Appendix F).

## 1.9 Summary

This chapter provided an overview of the research conducted in the field of information privacy in digital environments, such as smart airports. This chapter presented the research problem and identified the gaps in the existing research. In addition, it identified the research questions and relevant aims and objectives. It also provided an overview of the research in this thesis, including the IJAPRA framework and the research strategy followed in conducting this research. The IJAPRA framework was proposed to address the main research question: How to design the passenger interaction journey architecture and assess the associated information privacy risks in the context of the smart airport? In addition, this chapter outlined the main research theoretical and practical contributions. The IJAPRA framework is covered in detail in Chapters 3-5. The next chapter discusses the comprehensive review of existing literature related to this research

## 2 Chapter 2: Literature review

This chapter delivers a thorough review of the existing literature associated with the research topic. This chapter is divided into five sections. In section 2.1, a literature review is presented to offer a detailed and rigorous understanding of the contextual backdrop encompassing smart airports and its interconnected subjects. By critically reviewing the existing work, this section lays a solid foundation for the subsequent research and outlines the key themes and findings of previous studies. Section 2.2 focuses on the specific research methodology employed to gain deeper insights into passenger interaction journeys within the smart airport context and the associated concerns regarding information privacy. To achieve this, two systematic literature reviews (SLRs) were conducted, following the well-established method proposed by Kitchenham & Charters (2007). These SLRs involved an extensive analysis of articles published in renowned academic databases, emphasising topics related to smart airports and privacy risks. Furthermore, the findings from these SLRs serve as the initial stage of the DSR method adopted in this thesis (Vaishnavi & Kuechler 2015) to develop the proposed framework. In section 2.3, an additional review via manual search is presented to cover the most recent studies relevant to the scope of this research. Finally, the research gaps are presented in section 2.4, followed by a chapter summary in section 2.5.

### 2.1 Literature review

This section offers an in-depth review of the existing literature on the research topic, aiming to provide rich and rigorous information to enable an understanding of the context of smart airports, personal information, privacy, ontology, and knowledge graphs. The section begins with a review of smart airports as a main domain addressed in the thesis, followed by review of personal information and privacy as a main concern within this domain. The subsequent reviews of ontology and knowledge graphs provided a deep understanding of concepts employed in the proposed solution to the research problem. Through summarizing key points and highlighting insights, this section offers an overview of scholarly findings, offering clarity and coherence in navigating the topic at hand.

#### 2.1.1 Smart airports

The airport industry is in constant flux in response to changing travel requirements and digital technologies, such as the cloud, Internet of Thing (IoT) and mobile computing. It seeks to improve the quality of services provided to enhance the passengers' experience when travelling (Siddiqui & Ieee 2019). Digital technologies have facilitated connections between airport

facilities, data, and applications, with the aim of customising customer experiences (Halpern et al. 2021), leading to the emergence of the smart airport concept, also referred to as Airport 4.0. The following presents various definitions of smart airport and identifies the most appropriate one for this research scope. Following this, a discussion is presented about the evolution and development of the airport industry until the emergence of the smart airport concept.

### ***Smart airport definitions***

The term "smart airport" has gained widespread recognition in the global aviation industry, as airports are becoming increasingly connected and digitised, with passengers showing a growing desire for greater control and a wider range of self-service technologies that a smart airport can provide (Hirsh 2016). This calls for a more in-depth comprehension of passengers in terms of demographics, behaviours, attitudes, and a more robust cooperation between airlines and airports (Graham 2000). Generally, smart airports prioritise enhancing the passenger experience by providing a more seamless and efficient flow of information through various touchpoints. This results in a better experience for all parties involved, and as the majority of airports are embracing this strategy, the smart airport of the future appears to be quickly becoming a present-day reality (International Air Transport Association 2018).

The concept of smart airports, also known as Airport 4.0, is continuing to evolve. A smart airport can be considered a subsystem of a smart city, where urban life and aviation are seamlessly integrated, and information is readily shared between airline and air traffic management and control. This interconnectedness not only streamlines individual processes and overall airport operations but also significantly elevates customer satisfaction (Nagy & Csiszar 2016). According to Qi & Pan (2018), the concept of a smart airport involves integrating man and machine through the reconfiguration of service processes that utilise big data, IoT, and networks. Furthermore, AlMashari et al. (2018) introduced the concept of an airport solution that enables remote control and monitoring of multiple systems to improve safety for both passengers and personnel, ensuring that any issues are addressed promptly. The smart airport utilises networked data-driven responses and automated services to enhance the travel experience for passengers (European Union Agency for Network and Information Security 2016). According to Koenig, Found & Kumar (2019), Airport 4.0 refers to the application of Industry 4.0 technology to airport operations to improve efficiency and the passenger experience. Smart airports leverage the potential of cutting-edge and maturing technologies equipped with advanced and pervasive response capabilities. These digital

systems allow for the efficient and fast flow of broadband traffic in the entire system, encompassing the facilities and stakeholders (Fattah et al. 2009).

Straker & Wrigley (2018) describe smart airports as those that leverage information and communication technologies (ICT) to facilitate interactions that strive to provide efficient, timely, and exceptional services to passengers. Some Information and Communication Technology (ICT) examples are self-service technologies, automated technologies, biometric technologies, Radio-Frequency Identification (RFID), and mobile applications (Alabsi & Gill 2021; Bogicevic et al. 2017; Kalakou, Psaraki-Kalouptsidi & Moura 2015; Labati et al. 2016; Shehieb et al. 2016). These technologies allow customers to interact with software without any employee involvement during their journey which can increase both efficiency and the timelines of services (Chen, Batchuluun & Batnasan 2015; Kılıç, Üçler & Martin-Domingo 2021; Lin & Hsieh 2007). Table 2.1 includes a summary of the various definitions of smart airports.

*Table 2.1 Definitions of smart airport in the literature*

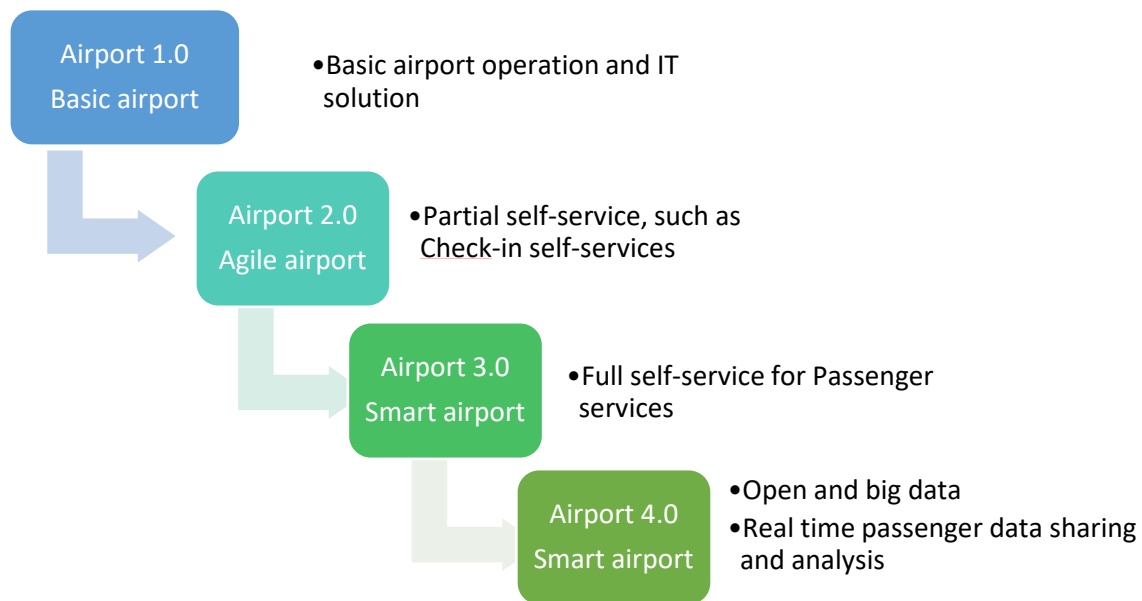
<b>Ref</b>	<b>Smart airport definition</b>
Nagy & Csiszar (2016)	A smart airport is a subsystem of a smart city, where aviation and urban life are connected, and information is shared between airlines and air traffic control to optimise processes and airport operations and improve customer satisfaction.
Qi & Pan (2018)	An airport that is smart integrates both human and machine through the rearrangement of service processes that utilise big data, the IoT, and networks.
AlMashari et al. (2018)	The smart airport provides solutions to remotely monitor and control multiple systems to improve safety for passengers and workers and address any issues quickly.
European Union Agency for Network and Information Security (2016)	The smart airport uses networked data-driven responses and automated services to improve the travel experience for passengers.
Fattah et al. (2009)	The Smart airports are digital systems that use advanced maturing technologies with pervasive response capabilities to enable fast broadband traffic throughout the airport and its stakeholders.
Straker & Wrigley (2018)	Airports that utilise ICT to enhance passenger interactions and provide efficient, timely, and exceptional services are considered smart airports.
Koenig, Found & Kumar (2019)	Airport 4.0 refers to the application of Industry 4.0 technology in airport operations to enhance efficiency and the passenger experience.

### ***Airport industry evolution***

Over time, airports have undergone notable transformations in their procedures and offerings, shifting from solely facilitating transportation to focusing on improving the quality of service

and offering a pleasing and engaging experience for travellers, via the rise of self-service, big data, biometric, and automated technologies (Lykou, Anagnostopoulou & Gritzalis 2018; Nau & Benoit 2017). Alansari, Soomro & Belgaum (2019); Koroniotis et al. (2020); Rajapaksha & Jayasuriya (2020) discussed the evolution of the airport industry at four levels: Airport 1.0, 2.0, 3.0, and 4.0 (Figure 2.1), as follows. Traditional airports, often labelled as Airport 1.0, heavily relied on basic IT solutions and manual procedures. Operations like take-off, refuelling, and landing were particularly underscored with a focus on safety. While passengers received standard services for boarding and disembarking the aircraft, communication channels between different services and stakeholders in these airports remained underdeveloped. Airport 2.0, also known as the "Agile airport," refers to airports that have embraced partial self-service technologies in the check-in process, network-enabled systems, and video surveillance, enhancing their efficiency and improving customer experience compared to Airport 1.0. These airports are flexible and can adapt to demand changes. A key characteristic of Airport 2.0 is the seamless data sharing and collaboration made possible by a single network that connects all parts of the airport under a single administration system. In Airport 3.0, also referred to as a smart airport, the defining features are the comprehensive implementation of self-service facilities for passengers, covering automated processes and transportation. Airport 4.0 owes its existence to Industry 4.0 and is powered by advanced technologies such as big data, biometric technology, and artificial intelligence. It generates value through real-time passenger flow and profile analysis by utilising open and big data, IoT, leveraging a unified network that includes airports, aircrafts, and airlines to provide services that enhance the passenger experience and improve the functionality of airports by facilitating smooth coordination between various subsystems and enabling real-time data exchange and analysis. Figure 2.1 presents the airport industry evolution up to the point of Airport 4.0.





*Figure 2.1 Evolution of the airport industry*

To conclude, there has been an evolution from the basic airport to the smart airport, making use of automation and other available technologies to enhance efficiency and the passenger experience. The advantages of smart airports are evident; however, it is critical to focus on security, privacy, and sustainability to ensure their continued success in enhancing passenger experience and operational efficiency.

### 2.1.2 Personal information

Information comes in a wide variety of forms and meanings. Various explanations can be connected to it, depending on the viewpoint used and the needs and ideals one has in mind (Floridi 2010). Data that has been processed and formatted in a manner that provides meaningful value to the recipient is referred to as information (Davis & Olson 1999; Zins 2007). A combination of characteristics or data items for a specific context is often referred to as information (Gill 2021a; Liew 2013).

In the interconnected digital world, personal information is collected, handled, and easily linked across several technologies (Anwar et al. 2021; Leonard 2014). “Personal information” is the term for information is linked to an individual person and may be used to identify them, particularly through specific identifiers such as a name, ID, location information, or a combination of data relating specifically to that individual (Herrera et al. 2021; Milne et al. 2017; Tlacuilo Fuentes 2020). In other words, personal information can be used to identify a specific individual, either alone or in conjunction with additional information known or expected to be possessed by the information controller.

Different regulators have applied their respective definitions of personal information. For example, the Privacy Act defines personal information as: "*Information or an opinion about an identified individual, or an individual who is reasonably identifiable*" (Office of the Australian Information Commissioner n.d). Another definition applied by the General Data Protection Regulation (GDPR) is: "*any information relating to an identified or identifiable natural person (data subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;*" (GDPR.ED 2023).

A broad review of the categories of personal information is necessary to comprehend the scope and sensitivity of personal information in various professions. This review examines the literature and privacy laws to provide a broad overview of the various categories of personal information. A review by Chua, Ooi & Herbland (2021) categorised personal information presented in the literature. According to this work, medical information, biometric data, financial information, demographic information, and PII are a few of the many distinct types of data that come under the general category of personal information.

Ambrose (2012); Veghes et al. (2012) categorise personal information as demographic (such as gender, age, education, and family status and members); psychometric (such as hobbies, interests, religious beliefs, political opinions); and identities (such as name, ID, biometric data, nationality, and gender). According to Chuleeporn (2008); Schwartz & Solove (2011), PII is information that might be used alone or in combination with other data, such as email address, name, phone number, and ID number, to identify a specific person. Due to the risk of abuse, identity theft, and unauthorised access, PII is regarded as the heart of personal information and needs specific security (Chuleeporn 2008). Medical information is defined as a person's health state, medical history, treatments, and diagnoses (Nosowsky & Giordano 2006). Biometric data is unique to a person and includes identifiable physical or behavioural characteristics, such as voiceprints, iris scans, fingerprints, or facial recognition and DNA profiles (Patel 2018). Financial information includes details on a person's financial transactions, bank account information, credit card information, and income, according to various financial legislation (Chua, Ooi & Herbland 2021).

Different countries and regions have their own specific privacy laws that may categorise personal information differently. For example, sensitive information, credit information, health information, online identifies, and biometric information are categorised under personal information in GDPR, and the Privacy Act 1988 in Australia, and the United States Privacy Law (Burdon & Telford 2010; Schwartz & Solove 2014). However, the GDPR also recognises special categories of personal information, , such as demographical or genetic or a person's sexual orientation information, political views, sexual activities, religious beliefs, and membership of a trade union (Schwartz & Solove 2014).

According to Islam (2009); (Peter H.Gregory 2021); Pingo (220), in order to classify personal information, it must be divided into groups based on how private, sensitive, and publicly available it is. Islam (2009); Pingo (220) defined public, private, and sensitive information under the personal information classification as: Public information which represents personal information that could be available to anyone without the owner's permission such as website and social media profiles, and first name; Private information which requires a high level of protection once the owner has granted permission based on their privacy preferences. Although the owner's permission is the legitimate right of the data subject, in some cases and under certain services agreements, providers are considered to be the owner and can use the information. Individual information includes ID numbers, biometric data, purchase history, and insurance and medical record numbers; Sensitive information includes ethical, political, and religious beliefs, sexual preferences, biometric, medical, and genetic information. The disclosure of personal information affects the owners and this is considered a privacy breach if it occurs without the person's consent(Gailloux & King 2020) .

In the realm of digital interconnected systems, the term digital information has gained significant prominence. The world has become increasingly connected through various technologies, and the role of digital information has become central to communication. Data which are processed, stored, or sent digitally or electronically are referred to as digital information (Burdon 2020). This includes any type of information in digital form, including text, pictures, audio, and video, that is produced, used, or shared in digital systems (Burdon 2020). In the context of this research, digital information refers to the handling of a passenger's personal information using smart airport technologies that support each stage of their journey.

In this research, PII is considered to be a type of personal information according to the GDPR regulation definition previously mentioned. All PII can be personal data but not all personal

data, including social media posts, preferences, and location, is considered personally identifiable. The reason for this is that in the smart airport context, PII is considered a limited scope definition and cannot capture the pseudonymous information which is commonly used in smart airports and considered personal information under GDPR (Psychoula 2020).

### 2.1.3 Privacy

The meaning of privacy varies and can be interpreted differently, even within a given context. However, there are central elements that are shared by most definitions of privacy. A very simple and early definition of privacy calls it "*the right to be let alone*" (Warren & Brandeis 1890, p. 193). In the decades since, many privacy definitions have been offered and have evolved, developed on societal changes, different views, and the rise of digital technology (Li & Palanisamy 2018; Peppet 2014). Before discussing the definitions of the term privacy, it is important to explain the dimensions of privacy discussed in the literature.

The privacy concept can be studied from several perspectives, such as economic, management, law, and information systems. Furthermore, privacy has various dimensions based on the information types. This includes information privacy, bodily privacy, territorial privacy, location privacy and communications privacy (Corcoran 2017; Martinez-Balleste, Perez-Martinez & Solanas 2013; Panahi Rizi & Hosseini Seno 2022). Information privacy refers to an individual's collected data including, identity, medical, and financial information and how to improve its protection level (Panahi Rizi & Hosseini Seno 2022). Bodily privacy involves the protection of a person's physical self, while territorial privacy focuses on the protection of an individual's attributes and space (Corcoran 2017; Panahi Rizi & Hosseini Seno 2022). Location privacy refers to the protection of a person's location against tracking (Martinez-Balleste, Perez-Martinez & Solanas 2013), and communications privacy involves the protection of communication channels in digital systems whether wireless or wired from recording and monitoring (Corcoran 2017).

Elmaghraby & Losavio (2014) argued that the privacy protection level relies on the following aspects. The first aspect is the place where personal activities are being conducted, as indoor activities need a higher protection level than outdoor activities. The second aspect is the activities with public regulations within services which affect the protection level when using those services. The final aspect is that the activities involving third parties usually have little or no protection level.

Finn, Wright & Friedewald (2012) described seven forms of privacy: customs and behaviour, personality, association, feelings and viewpoints, communication, location or area, and data or image. In contrast, Eckhoff & Wagner (2018) described the following five types of privacy: privacy of location involves protecting information of the locations a person has visited and when so a person's home location, workplace, habits, and social life can be protected. Privacy of state of body and mind involves protecting information concerning an individual's health, perspectives, ideas, fingerprints, and other biometric data. Privacy of social life involves protecting information on a person's social activities on social media applications and other platforms. Revealing private information surrounding a person's social life, such as their habits and opinions, or metadata, such as information concerning other persons with whom they have made contact via social applications, is a violation of that person's privacy. Privacy of behaviour and action refers to protecting information on a person's online purchase activities and habits. Often, a person's privacy in relation to their online shopping activities is violated for advertising purposes. Finally, the privacy of media includes protecting information concerning all the data a person has uploaded and shared via the internet, for example, photos, video, and audio. A violation of a person's privacy in relation to media occurs when an individual's use of media data is republished or reused without their permission.

Privacy is defined by Westin as *“the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others”* (Westin 1968, p. 166). According to Fried (1970, p. 209) *“Privacy is not simply an absence of information about us in the minds of others, rather it is the control we have over information about ourselves”* whereas, privacy is known as the individual prerogative to decide what kind of information is to be shared or accepted (Hoffman 1977). Solove describes privacy as an individual right to dictate the circumstances in which their personal information is obtained, shared, and utilised (Solove 2008). He also writes about the collection, processing, publication, and violation of personal information as dimensions of information privacy (Solove 2006). Information-specific privacy is defined as the connection between an individual's right to privacy and their ability to access and control their own information when it is held by different organisations (Hoffman 1973; Martinez-Balleste, Perez-Martinez & Solanas 2013).

Concerns about how an organisation collects and uses personal information are known as information privacy concerns (Mutimukwe, Twizeyimana & Viberg 2021; Xu et al. 2011). The interest in information privacy began following the rise in the processing of digital

information after 1960 (Li & Palanisamy 2018). Table 2.2 summarises the various definitions of privacy.

*Table 2.2 Definitions of privacy in the literature*

Reference	Privacy definition
Warren & Brandeis (1890)	“The right to be left alone.”
Hoffman (1977); Solove (2008); Westin (1968)	The right to decide what of one’s information is disclosed to others.
Fried (1970)	Control over individual information, not the absence of the information.
Hoffman (1973); Martinez-Balleste, Perez-Martinez & Solanas (2013)	Information-specific privacy is the connection between an individual’s right to privacy and their ability to access and control their own information across different organisations.

As shown in Table 2.2, the evolution of privacy definitions has transitioned from recognitions of individual claims to sophisticated understandings that encompass individual control, autonomy, and the complexities of information handling in digital environments. This reflects a growing concern in the digital age, where the appearance of interconnected systems has led to increased privacy risks associated with personal information.

In today's digital and connected world, privacy is deeply interconnected with the mechanisms of handling information using many technologies and sharing it with different parties for different purposes; accordingly, the privacy definitions proposed by Solove (2008) and Martinez-Balleste, Perez-Martinez & Solanas (2013) appears more relevant in today's digital world.

#### 2.1.4 Ontology

Ontology is defined as a discipline within the knowledge representation field (Omerovic, Milutinovic & Tomazic 2001; Sowa 1999). Knowledge representation is the process of creating a structured model of knowledge for reasoning about and solving problems. It includes representing knowledge for processing and understanding by a computer (Guarino 1995). Ontology refers to the process of conceptualising an abstract and simplified view to represent the world for a specific purpose, which involves explicitly defining the concepts and relationships that are relevant to a particular domain (Gruber 1995; Martin, Szekely & Allemang 2021). Ontology is key to various disciplines including computing (Boyce & Pahl 2007; Guizzardi 2005). In this context, ontology is a framework for knowledge representation

that captures the concepts and connections between them in a given domain (Nahar & Gill 2020; Uschold & Grüninger 1996).

Studies have classified ontology types by level of generality or dependency (Guarino 1998; Guizzardi 2005; Omerovic, Milutinovic & Tomazic 2001); the ontology level of dependency is categorised into independent, domain and task, and application ontologies. The independent ontology, also referred to as generic, foundation, core, or top-level ontology, represents general independent concepts (e.g., time, events, and space). Domain and task ontologies, such as medicine and diagnosis, specialise the ideas from a general ontology and record the vocabulary associated with a specific domain or activity. Application ontologies link the specialisations from both domain and task ontologies to define ideas derived from both. For example, domain entities can serve different purposes, such as replacing components, when performing a particular task (Guizzardi 2005).

Ontology development draws from fundamental ontological distinctions and is supported by knowledge representation formalisms and tools that have emerged in past decades (Fung & Bodenreider 2023). Ontological Organisation can be assembled through manual, or fully automated, and typically has classes, objects, attributes and their values, and semantic relationships as essential elements (Studer, Benjamins & Fensel 1998).

There are many benefits to using an ontology (Alrumaih, Mirza & Alsalamah 2020; Boyce & Pahl 2007; Hajmoosaei & Abdul-Kareem 2008; Sarraipa et al. 2008), for instance, ontology provides a universal definition of a domain in which multiple applications and groups can be reused. It facilitates computational comprehension and effortless compatibility between individuals and organisations, allowing the extraction and definition of crucial concepts and their relationships in a transparent and uncontested manner. Ontology plays a crucial role in promoting the exchange of knowledge by facilitating its use between people and Organisations, ultimately aiming to enhance the interoperability of intelligent systems. It has also been employed to address semantic discrepancies that may arise between various data sources. Furthermore, it serves as a valuable resource for direct design processes by providing a comprehensive knowledge base.

#### 2.1.5 Knowledge graph

The concept of a knowledge graph was initially introduced in 1972, but it gained widespread recognition after 2012, when Google launched its Knowledge Graph (Buchgeher et al. 2021; Hitzler 2021; Martin, Szekely & Allemang 2021; Schneider 1973). The introduction of

knowledge graph led to the increased utilisation and development of such representation in organisations (Buchgeher et al. 2021; Hubauer et al. 2018; Noy et al. 2019). Knowledge graphs are the graph-structured driven knowledge which are extensively employed to represent structured knowledge and deliver a range of Artificial Intelligent (AI) based tasks to handle complex dynamical large data (Hofer et al. 2023; Tamašauskaitė & Groth 2023). Subsequently, several definitions of knowledge graphs have been developed, either in research (Ehrlinger & Wöß 2016; Fensel et al. 2020; Hogan et al. 2021) or by companies using or supporting the use of knowledge graphs, such as OpenLink, Ontotext, Neo4J, or TopQuadrant (Hofer et al. 2023). According to Hogan et al. (2021, p. 3), a knowledge graph is defined as “*a graph of data intended to accumulate and convey knowledge of the real world, whose nodes represent entities of interest and whose edges represent potentially different relations between these entities.*”. A knowledge graph is a comprehensive network of entities and their corresponding instances, which accurately represents real-world objects and their interconnections within a specific domain or Organisation (Bellomarini et al. 2019). These definitions reflect that knowledge graphs are structured to represent a combination of knowledge and data of significance to a domain as one single graph.

Two types of knowledge graphs are discussed in research. The first type is generic knowledge graphs providing access to multiple domains (Tamašauskaitė & Groth 2023). The second type is domain-specific knowledge graphs focussing on a narrower domain, often pertaining to a specific problem or industry (Abu-Salih 2021).

According to Li et al. (2020); Tamašauskaitė & Groth (2023), There are two primary approaches to developing a knowledge graph: the top-down approach and the bottom-up approach. The top-down approach involves first defining an ontology and then extracting knowledge from the data, while the bottom-up approach involves extracting knowledge from the data and then defining the ontology of the knowledge graph. This research follows the bottom-up approach whereby the ontology is developed first to represent the conceptual knowledge relevant to the field of privacy risks in smart airports.

There are several significant justifications for and benefits of knowledge graphs ((Martin, Szekely & Allemang 2021), such as: 1. providing semantic context to data, enabling easier integration of data from multiple places and generating richer combined data sets for predictive purposes; 2. permitting representation of complex information domains which possess rich, connected structures; 3. providing a flexible data structure to store predictions along with the



pertinent data; 4. enabling modular knowledge, whereby knowledge can be treated as a discrete, reusable, modular resource throughout the data architecture of the endeavour; and 5. allowing for self-describing data, where metadata can be linked directly to the data, making the data both business-friendly and machine-readable.

### 2.1.6 Graph-data models

The fundamental principle underpinning knowledge graphs is to start by modelling data as a graph, necessitating a robust graph data model able to represent and employ entities, relations, their types, in addition to ontological descriptions and Organisation (Sakr et al. 2021). According to Angles et al. (2017); Hogan et al. (2021), the most common knowledge graph models are the directed edge-labelled (del) graph, the property graph, and heterogeneous graphs. A description of each graph model type is given in Table 2.3.

*Table 2.3 Graph model types*

<b>Graph model type</b>	<b>Description</b>
Directed edge-labelled	According to Angles et al. (2017); Hogan et al. (2021), the directed edge-labelled (del) graph is described as nodes that stand in for entities and directed labelled edges that stand in for connections among those nodes. The resource description framework is the standard data model of this graphs (Cyganiak et al. 2014).
Heterogeneous Graphs	According to Hogan et al. (2021), a heterogeneous graph is distinguished by its array of distinct nodes and edges. Within this graph, each node and edge is designated a unique type. While these graphs share similarities with (del) graphs—in which edge types indicate their direction—it's the node's type in heterogeneous graphs that's integral to its model, rather than being portrayed by a unique relationship.
Property Graph	According to Angles (2018); Hofer et al. (2023); Hogan et al. (2021), a property graph is a type of graph that enables nodes and edges to be associated with a set of properties, which are essentially value pairs and a label, providing greater versatility when modeling data. The property graphs are widely used in popular graph databases, including Neo4j. (Angles et al. 2017).

### 2.1.7 Graph database

There are multiple ways to record knowledge graphs, using graph applications, data models, and algorithms (Yan et al. 2018). Relational databases, triple stores, and graph databases are some example of data models used with knowledge graph (Hogan et al. 2021). Graph database is a type of storage system that utilises graph structures to store and represent data (Pokorny 2017). As this research relates to property graph data models, this model is supported by several graph databases such as Neptune (Beebe et al. 2018), Neo4j (Van Bruggen 2014) and TigerGraph (Deutsch et al. 2019). Of these, Incredibly scalable, reliable, and Open-source

Neo4j is a graph database (Pokorný 2015). Neo4J graph database was adopted in this research to represent the developed IJPRA ontology.

Neo4j is an open-source graph database that stores data as a graph, where edges represent semantic relationships and nodes represent concepts (Das et al. 2020; Guia, Soares & Bernardino 2017; Konno et al. 2017; Nahar, Gill & Roach 2021). Neo4j is a fully transactional database with Java engine that allows users to store data as graphs instead of tables (Webber 2012). It was first released in 2007 and comes in three versions: community, government, and enterprise. The community edition is a trial version that anyone can use, while the enterprise edition offers a more complete version for testing for 30 days (Guia, Soares & Bernardino 2017). The two versions of Neo4j, including community and enterprise, differ primarily in terms of online support, fast performance, and comprehensive system monitoring (Das et al. 2020; Guia, Soares & Bernardino 2017). Nodes and relationships in Neo4j can both contain properties (Das et al. 2020).

The main advantages of Neo4j as discussed by Das et al. (2020); Guia, Soares & Bernardino (2017); Van Bruggen (2014) are: 1) it has scalable, reliable, and flexible schema; 2) it supports cypher query languages for quiring data of the graph database;3) it utilises property graph data model and Apache Lucence index support ; 4) the interface is highly intuitive and accessible.

## 2.2 Systematic literature review

To understand the passenger interaction journey in the smart airport context and the information privacy concerns relevant to passenger information, two systematic literature reviews (SLRs) were conducted. In addition, these SLRs are used to address the research questions in Chapter 1(See Section 1.3) and they follow the method proposed by Kitchenham & Charters (2007) to analyse articles published in well-known academic databases relevant to the smart airport and privacy risks. The findings of these SLRs are used to identify the research gap in the topic at hand and are then used as the initial data in the initiation step of the DSR method adopted from Vaishnavi & Kuechler (2015) to develop the proposed framework. Section 2.2.1 presents the scope, results, and findings of the first SLR, and Section 2.2.2 presents the scope, results, and findings of the second SLR.

### 2.2.1 Passenger digital information privacy concerns in smart airports (Reported in (Alabsi & Gill 2021))

To understand the passenger journey in a smart airport and the relevant information privacy concerns, a SLR was conducted by Alabsi & Gill (2021) to systematically review and

synthesise the elements involved in the passenger journey in the smart airport context and information privacy concerns in smart airports. This SLR followed the method proposed by Kitchenham & Charters (2007) to analyse articles published in well-known academic databases relevant to smart airports. For this SLR, 31 studies were carefully selected and reviewed. For ease of reference, it is important to note that each study is denoted by the letter 'S' followed by a number. For example, “S1” refers to the first selected study. This notation is used consistently throughout the text and tables to identify the studies under discussion. Each study was evaluated and a score of 1-5 was assigned based on five assessment criteria to ensure its relevance and quality, namely research context relevance, research aim, research method relevance, and a detailed discussion of the results and future directions. In this SLR, the results were analysed using Customer Journey Map (CJM) (Rosenbaum, Otalora & Ramírez 2017) and Concerns for Information Privacy (CFIP) frameworks (Smith, Milberg & Burke 1996) as a theoretical lens. This approach is suitable for categorising the results of this SLR as it provides adequate coverage of the elements involved and the information privacy concerns in smart airport. The results of this review were analysed using the aforementioned frameworks as theoretical lenses and reported based on the following categories: (1) passenger travel journey involving smart airport applications; (2) elements (people, process, information, technology) in the journey; (3) passenger's digital information privacy challenges; (4) current solutions; (5) standards and regulations. More details about the research method of this SLR is found in (Alabsi & Gill 2021).

### ***Passenger travel journey through smart airport application***

The results show that only 48% of the selected studies discuss the stages of the passenger travel journey (supported by smart airport applications), as shown in Table 2.4. Overall, passengers pass through three stages during their travel journey, as outlined in Figure 2.2 (Willemsen & Cadee 2018).

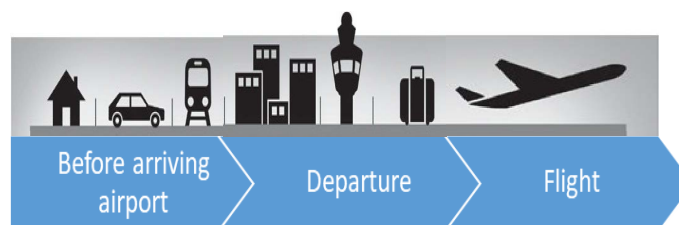


Figure 2.2 The stages of passenger journey

After booking a flight, the real interaction between the passenger and the smart airport applications begins at the check-in stage. At this point, the passenger utilises smart check-in applications through the self-service kiosk, the website, or mobile devices to obtain the

boarding pass and bag tags. Most recently, it has been observed that biometric services are used for check-in, such as at Brisbane and Hamad international airports (Negri, Borille & Falcão 2019). This stage also includes the smart baggage handling applications available to finalise the baggage check-in and drop-in via an automated system.

The security control stage involves the verification of travel documents and screening of the passengers and their carry-on luggage. In 2014, the International Air Transport Association and Airport Council International (ACI) introduced their smart security control initiative, aiming to implement end-to-end self-service by 2020, to make security control checkpoints more secure and convenient for passengers (International Air Transport Association 2014). However, many airports currently use conventional methods. Biometric services have also been adopted by Custom and Border Protection (CBP) at Hartsfield-Jackson Atlanta International (ATL) airport in the USA (Zhang 2020). It can be observed from Table 2.4 that 29% of the selected studies cover Automated Border Control (ABC) at the border control stage. It transpires that smart border control applications (including self-service and biometric service) are mainly used at departure and arrival to accelerate identity verification at the border control stage. Finally, at the boarding stage, 6% of the studies dealt with how smart boarding applications empower the passenger to board the aircraft using self-service. In addition to the aforementioned applications, smart airport apps for mobile devices are widely used by passengers to guide them throughout the course of their travel journey (Harteveldt 2016). For instance, they provide information about locations and the status of counter numbers, flight updates, boarding time, shops, and other utilities. In addition, they can be used to track luggage, check the waiting queue, and find available parking places.

*Table 2.4 Passenger journeys in the smart airport*

<b>Passenger travel journey</b>	<b>Smart airport application</b>	<b>Papers</b>	<b>Percentage</b>
Check-in stage	Smart check-in	S14, S26, S27, S28	13%
Bag drop stage	Smart baggage handling	S14, 26, S28, S29	13%
Airport security control stage (smart security)	Smart security	S11, S14	6%
Border control stage	Smart border control	S4, S10, S20, S26, S29, S16, S30, S31, S6	29%
Boarding stage	Smart boarding	S26, S29	6%
Guide passenger during their journey	Smart airport apps for mobile devices	S26, S2, S3, S1, S14	16%

## *Elements involved in the passenger journey*

### **People**

As shown in Table 2.5, 13% is the total of the reviewed studies cover the transfer mechanism of the passengers' digital information during their travel journey. This information is collected and handled by various stakeholders such as airlines, airports, and governments agencies (such as border controller authorities) during departure or arrival. Further, the information at the check-in stage is handled by airlines to check tickets, passengers, and travel documents. Later, government agencies need the passenger's information as it plays an essential role in airport security control and border control. Furthermore, the airport uses the passenger's information for statistical purposes to improve services and the passenger experience.

*Table 2.5 People involved in passenger's travel journey*

<b>Elements</b>	<b>Who and what involved</b>	<b>Papers</b>	<b>Percentage</b>
People	Airlines	S14, S21, S26	10%
	Airport	S14, S26	6%
	Government	S11, S26	6%
	Border control authorities	S21	3%

### **Process**

As shown in Table 2.6, 10% of the selected studies describe how passengers can finalise their check-in process using self-service kiosks (either standard ones or intelligent ones), or online (using smart devices) to print their boarding pass. One study (S27) discussed the use of biometric technology for smart check-in. Confirmation of passenger information including biometric data is key to the check-in process. During the smart baggage handling process, passengers scan their passports and boarding passes to print out and affix the baggage tag, then they put their luggage in the automated bag drop area.

The smart security control process involves the following: (1) the passenger scans their passport and boarding pass; (2) the system verifies the passenger's name on both documents; (3) the passenger's photo is captured to confirm the match between the photo taken and the one in the passport; (4) if the passenger's biometric identity matches that stored in the government database, the passenger's details are sent to the tablet of the security officer to proceed with the security screening.

As shown in Table 2.6, 13% of the selected studies outline the process of using smart border control applications. The process starts and ends through an automated gate (e-gate), and includes scanning the passenger's e-passport, verifying their photo (biometric data) by camera, and finalising this part of the process after confirming the match between the e-passport and

the biometric data. Before entering the aircraft, the passenger goes through a smart boarding application to scan their boarding pass, and then the automated gate will open to let them enter the aircraft.

*Table 2.6 Processes which are implemented by passengers*

Process	Description	Papers	Percentage
Passenger's Check- in	The check-in process in the smart check-in application relies on applied services (either self-service or biometric).	S14, S26, S27	10%
Baggage check-in	The process is implemented through the smart baggage handling application using self-service.	S14, S26	6%
Security control	The security checkpoint process where the passengers undergo the security check uses the smart security control application.	S11	3%
Border control	The process within the smart border control application where the passenger's identity is verified without human assistance.	S10, S11, S31, S30	13%
Boarding	The passenger boards the aircraft after following the steps through the smart boarding application.	S26	3%

### **Passenger information**

Based on this review, passenger information was addressed in only 26% of the selected studies, as shown in Table 2.7. Passenger information is classified into biographical data and biometric data. Biographical data is usually located on the second page of the passport document. It includes the passenger's name, nationality, place and date of birth, signature, photograph, passport number, date of issue, and expiry date. Biometric data refers to information detailing the biological characteristics of an individual that can be captured using scanners or cameras (Patel 2018). Based on our review, the passenger's biometric data such as fingerprints, and facial and iris data, are of great relevance to smart airports and are collected at check-in, security control, and border control stages. As indicated in Table 2.7, 16% of the selected studies describe the e-passport as an example of an e-travel document that is commonly used in smart airports. According to International Civil Aviation Organisation (ICAO), an e-passport is a booklet that stores passengers' biographical information and biometric data (such as fingerprint, face image) on an electronic chip. A unique digital signature protects this type of e-document for each country (International Civil Aviation Organisation n.d.).

On the other hand, two types of passenger information records are discussed in 6% of the selected studies, as shown in Table 2.7. The first type is the Advanced Passenger Information (API), which includes the passenger's ID number, nationality, name, date of birth, and boarding pass (such as flight number and time, boarding time, seat number, airline name, and departure

time). The other type is the Passenger’s Name Record (PNR), which has the passenger's contact number, address, and credit card details. This information is generated at the booking and check-in stages by airlines and the passengers themselves. In most cases, airlines are required to share this information with the border control authority of the particular destination before the flight's arrival time (International Air Transport Association n.d).

*Table 2.7 Passenger's digital information handled through the journey*

Digital Information types		Papers	Percentage
Biometric data	Facial recognition	S11, S24, S20	10%
	Fingerprint	S10, S24	6%
	Iris	S10, S24	6%
E-travel documents (E-passport)		S10, S20, S30, S31, S6	16%
PNR and API		S21, S24	6%

### Technology

In the smart airport context, smart applications rely on the use of the underlying technologies that enable them. Based on our review, we have classified the smart airport technology items into several groups, as shown in Table 2.8, Internet of Things (IoT), RFID, mobile devices, autonomous systems such as intelligent check-in kiosks (KATE), Artificial Intelligence (AI), machine learning, biometric technology, automated systems, and cloud computing. Sensor technology is an example of the IoT, which is widely used in smart airport applications at each stage. It is observed that smart airport applications are implemented using a combination of two or more enabling technologies. For example, sensors and RFID, in addition to biometric technology and automated systems, are utilised in smart boarding control and smart security control applications to increase the efficiency and security of the passenger identification process. RFID and automated drop off machines are vital in smart baggage handling applications. They are used by passengers to print baggage tags and to self-drop-off their baggage. Mobile devices are commonly employed by passengers to use smart airport apps. Approximately 6% of the selected studies discuss the importance of adopting AI and machine learning technologies, in addition to biometric technology and automated systems, in the security control application to improve the security level and the passenger experience. On the other hand, 6% of the reviewed studies discuss the importance of the integration between IoT and cloud technology when processing and analysing the information collected from passengers during their journey.



Table 2.8 Enabling technology used for smart airport applications

Enabling Technology Type	Papers	Percentage
IoT	S1, S26, S15, S25, S22, S12, S13	23%
Biometric	S16, S20, S11, S10, S24, S14, S26, S4, S27, S30, S31, S6	39%
Mobile devices	S3, S26, S1, S14	13%
Cloud computing	S22, S25	6%
AI	S11, S1	6%
Machine learning	S11	3%
Virtual reality	S25	3%
RFID	S1, S3, S26, S25, S5	16%
Automated systems	S26, S14, S20, S10, S16	16%
Autonomous system (KATE intelligent kiosks)	S27	3%

### *Passengers' digital information privacy challenges and current solutions*

#### **Privacy challenges**

We used the CFIP framework (Van Slyke et al. 2006) to identify and categorise the passenger's privacy challenges that may affect their digital information in smart airports. In Table 2.9, we identified 7 challenges, grouped into following categories: collection, error, unauthorised use, improper access. As shown in Table 2.9, 10% of the reviewed studies highlight the information privacy challenges within the collection category (C1). These include: (1) collection and transfer of PNR between airlines and countries, and between countries; (2) collecting and storing big data without proper supervision, which may increase the privacy preservation challenge.

Under the error category (C2), 10% of the reviewed studies identify the privacy challenges that arise due to accidental or intentional errors. These are mainly caused by: (1) manipulating the stored information in cloud servers; (2) modifying the stored big data, which may affect the analysis results; and (3) modifying and altering the information by authorised persons in edge and fog computing.

The unauthorised use category (C3) appeared in 16% of the selected studies. Our review discovered secondary usage of information and data leakage under this category. Secondary usage could occur when the database owner or cloud service provider reuses the stored information without the passenger's consent or permission, whereas data leakage occurs due to the use of RFID chips for storing the passenger's information in the e-passport. Furthermore, the use of edge and fog computing may, in the smart airport infrastructure, lead to the leakage of data to third parties. Improper access (C4) is the last category and includes unauthorised



access challenges. Based on our review, 3% of the selected studies pointed to unauthorised access to the stored information in cloud servers on the part of the cloud service provider.

*Table 2.9 Privacy challenges for passenger information*

Ref	Categories	Concerns	Papers	Percentage
C1	Collection	Collection and transfer of PNR and API	S21, S22	10%
		Privacy-preserving concerns in big data	S7	
C2	Error	Data manipulation, deletion, and loss	S22	10%
		Data protection concerns in big data.	S7	
		Data integrity concerns in FMEC	S22	
C3	Unauthorised use	Secondary usage of stored data	S10, S24, S11, S22	16%
		Data leakage	S22, S5	
C4	Improper access	Unauthorised access	S22	3%

### **Current solution**

In addition to information privacy challenges, we carefully reviewed the selected studies with the aim of identifying possible privacy solutions. Based on our review, we identified 6 solutions, extracted from 23% of the selected studies Table 2.10.

As shown in Table 2.10, three types of the identified solutions were related to cryptography. For instance, the Public Key Infrastructure (PKI) cryptographic method is proposed to prevent unauthorised access (C4) and to ensure the secure sharing (C1) of the information stored in an e-passport, while the AES algorithm is proposed to encrypt the information and biometric data in a QR code to address the current data leakage challenge (C3) when using RFID chips in e-passports. The multi-dimensional encryption algorithm is proposed for challenge (C1) to guarantee the security of the shared information in the System Wide Information Management (SWIM) architecture. To address the challenges (C1, C2) related to big data technology, a security as a service framework is proposed to monitor the data and protect it from errors with a view to guaranteeing the correctness of the data and analysis results. The main idea of this framework is focused on OpenSSL authentication and attribute authorisation. The Fog and Multi-access Edge (FMEC) paradigm is proposed as a solution for the information privacy challenges in cloud servers, these being: secondary use of stored information (C3), unauthorised access to stored information (C4), and modifying stored information (C2).

As shown in Table 2.10, 6% of the reviewed studies discussed the European Union (EU) agreements that delineates the role of PNR transfer between EU and other countries. The EU agreements are considered to be a solution for sharing passenger information (C1). In September 2011, agreements were signed between the EU and Australia and in December 2011 between the EU and the USA (Vedaschi 2018). In addition, agreement between EU and Canada was launched in 2018 (Vedaschi 2018).

*Table 2.10 Current solutions*

Category	Solutions	Papers	Percentage
C1	Multi-dimensional encryption algorithm to ensure the confidentiality, integrity, availability, and non-repudiation of shared information in SWIM.	S17	16%
	Security as a service framework to solve the privacy-protection challenges associated with big data.	S7	
	EU agreement for sharing PNR.	S8, S21	
	PKI to secure the sharing of e-passport information.	S10	
C2	Security as a service framework to solve the data protection challenge in big data.	S7	6%
	Fog and multi-access edge computing (FMEC) paradigm.	S22	
C3	Encrypt (AES algorithm) the e-passport information in Quick Response Code (QR) to avoid data leakage challenge in RFID chip.	S5	6%
	Fog and multi-access edge computing (FMEC) paradigm to prevent the secondary use of information in cloud server.	S22	
C4	Public key infrastructure (PKI) cryptographic method to secure access to e-passport information.	S10	6%
	Fog and multi-access edge computing (FMEC) paradigm to prevent the unauthorised access to the information in cloud server.	S22	

### ***Passenger’s information standards and Privacy Regulation***

Privacy administrative and constitutional laws, as well as policies, play a vital role in addressing privacy concerns (Hiller & Blanke 2016). For example, the GDPR is a significant regulation for information privacy. The EU adopted the GDPR in 2018 and incorporated principles for personal information processing (Wolford 2020). The GDPR explains principles that help in protecting individual privacy (GDPR.EU 2023). Consent, breach announcement, and privacy by design are some examples of GDPR principles (GDPR.EU 2023).

In the USA, the Fair Information Practice Principles (FIPPs) were developed in 1973 to discuss the importance of protecting individual privacy and was adopted by the U.S. Privacy Act

(Gellman 2017; Li & Palanisamy 2018). Since then, different sectors in the USA, such as the health and business sectors, have developed privacy regulations called the Health Insurance Portability and Accountability Act (HIPAA) (Silva, Monteiro & Simões 2021).

In Australia, the Australian Privacy Principles (APPs) are the cornerstone of the Privacy Act 1988 (Act) which seeks to protect and guide the use of personal information (Office of the Australian Information Commissioner n.d.). The APPs govern the collection, handling and access to personal information, and ensure the accuracy and integrity of personal information (Office of the Australian Information Commissioner n.d.).

Based on the above review, it is clear that countries share the common objective to protect the privacy of personal information and to govern how it is used despite the differing regulations. We identified and extracted the standards and policies relevant to passenger information in the aviation industry from 26% of the selected studies. As shown in Table 2.11, biometric data needs to adhere to standards (ISO/IEC 29794 & ISO/IEC 19794) to ensure its quality. According to our review, 19% of the selected studies commented on the role ICAO in developing standards for biometric/biographic information and e-passports, while 3% discussed that the European Border and Coast Guard Agency (Frontex), and National Institute of Standards and Technology (NIST) also devise standards for biometric information in the e-gate context. A list of standards relevant to the aviation industry is detailed in 10% of the reviewed studies.

*Table 2.11 Standards for passenger's information in the aviation industry*

<b>Governing body</b>	<b>Description</b>	<b>Papers</b>	<b>Percentage</b>
ICAO	Introduced standards for biometric data, biographic/passport data.	S10, S16, S5, S20, S12, S30	9%
ISO/IEC	Standards ISO/IEC 29794 & ISO/IEC 19794 to address the quality of biometric data.	S10	3%
Frontex, NIST	Contributed to formulating standards and for biometric information.	S30	3%
EN, ISA/IEC, ENISA	List of standards for the aviation industry	S12, S15, S18	10%

We also undertook a manual search to identify and include the recent relevant known information privacy regulations to complement this academic SLR. We focussed on the most recent GDPR, which was adopted by the EU in 2018 and includes its principle for processing personal information (Wolford 2020) and also, the APPs, which are set out in the Privacy Act

1988 to govern the use of PII (Office of the Australian Information Commissioner n.d.). Table 2.12 details these two key regulations in the context of smart airports. It is worth noting at this point that the manual research results were used to cover information privacy regulations in smart airports and were not critically analysed. Thus, these results are not included in the total number of selected studies.

*Table 2.12 GDPR and APPs privacy regulations in Australian and European airports*

	<b>Description</b>
GDPR	GDPR enables airports of all sizes to ensure that passenger data are kept safe and protected during the collection, storage and dissemination process (Robson 2019).
	GDPR Article 5 includes the principle of personal data processing, while Article 44 and Article 50 cover principles regarding the transfer of personal data to third countries or between international organisations (INTERSOFT CONSULTING 2018).
APPs	The Australian Airport Association (AAA) applies the Australian Privacy Principles (APPs) to guarantee the privacy of the passenger information it holds (Australian Airport Association 2023).
	The Australian Privacy Principles consist of 13 principles to govern standards and rights for the following (Office of the Australian Information Commissioner n.d.): <ul style="list-style-type: none"> <li>- Collect, utilise, and reveal personal data.</li> <li>- The responsibility and governance of organisations.</li> <li>- Correct the personal data</li> <li>- Access personal data by individuals.</li> </ul>

### ***Review results (SLR1)***

The results of this SLR show that there is an increasing interest in topics related to smart airports and the privacy challenges surrounding passengers’ digital information. A total of 324 studies were selected from well-known databases in the initial stage of this study, then 31 relevant studies were reviewed and evaluated to address the research questions.

The privacy and security issues around the use of several technologies such as RFID, IoT, and cloud and fog computing have been investigated in the literature. According to Ayoade (2006); Ohkubo, Suzuki & Kinoshita (2004), using FRID could affect personal privacy as the collected information can be leaked without the users’ knowledge and it can also be used for other purposes. Furthermore, the use of IoT devices in handling personal information may introduce a number of security and privacy issues (Makhdoom et al. 2019; Weber 2010). Imine, Lounis & Bouabdallah (2020) state that privacy is becoming one of the major concerns when personal information is shared through cloud and fog computing. This is because there is a possibility of personal information leakage and activity tracking such as travel journeys. As shown in Table 2.8, our findings reveal that the majority of the reviewed studies (62%) focus on enabling

technologies, which are used to support smart airport applications without consideration the privacy issues that may arise when using these technologies. However, only one study proposes a framework to encrypt passengers' information, which is stored in an e-passport using a QR code as a countermeasure of the current security issues when using RFID chips. Since the protection of passengers' digital information is essential, future research is needed to address the implications of enabling technologies in relation to the privacy of passenger information in smart airports.

Passengers' digital information is collected and shared among several stakeholders (airlines, airports, and government agencies). Agrawal (2014) defines digital information as an invisible piece of information that needs to be made visible using hardware and software technologies. The characteristics of digital information are set out as follows: dependency, multipliable, dynamic, economic, modular, and delicate. As shown in Table 2.5, to the best of our knowledge, the reviewed selected studies have not outlined how the stakeholders handle passenger information that is collected during their travel journey. As a result, there are concerns around the use of the collected information for other purposes without the passengers' consent. On the other hand, there is no standardised system to verify the mechanism of sharing passengers' digital information between airlines and governments (border control authorities). In light of this, there is a need to develop a trusted framework for sharing passenger information among multiple stakeholders. This should consider passengers' consent and control over access to their information. This draws our attention to another important future research direction.

The academic community is becoming increasingly interested in information privacy concerns. According to Choi, Lee & Sohn (2017), the majority of the literature discusses information privacy concerns based on the CFIP provided by Van Slyke et al. (2006) or the Internet Users' Information Privacy Concerns (IUIPC) provided by Malhotra, Kim & Agarwal (2004). In this study, we used the CFIP framework to identify and categorise the passengers' digital information privacy in the selected studies in the specific context of smart airports. As shown in Table 2.9, a number of information privacy challenges were identified. However, the reviewed studies did not offer any concrete or explicit guidance on how to link the privacy challenges to the stages of the passenger travel journey. This appears to remain an area for further research.

As shown in Table 2.10, although we identified the current solutions for the privacy concerns detailed in Table 2.9, it can be observed that there is a lack of knowledge about the

implementation of solutions for protecting passenger's information. Furthermore, it has been observed that, to the best of our knowledge, three of the privacy challenges discussed in this study have remained unsolved. These challenges are the secondary use of information stored in government databases, and the data leakage and data modification challenges in fog computing. As shown in Table 2.10, most proposed solutions relate to encryption methods. Encryption, biometrics, anonymity, and access control solutions have been proposed (or have been implemented) to preserve individual privacy in a smart city (Elmaghraby & Losavio 2014; Weber 2010; Zhang et al. 2017). However, Cui et al. (2018) stated that such encryption methods are not sufficient for the current context of smart environments. Similarly, Labati et al. (2016) discuss that conventional cryptographic methods are not suitable for biometric data. The authors propose that ad-hoc methods be used to protect biometric data. It is thus necessary to investigate and develop more relevant solutions involving Privacy-Enhancing Technologies (PETs) and methods (e.g., blockchain) to ensure the privacy of passengers' digital information in smart airports.

There is also a dearth of published academic studies or results related to the implementation and impact of information privacy regulations and standards in the context of smart airports. For instance, as shown in Table 2.11, only 9% of the selected studies briefly mention ICAO standards, policies, and recommendations for biometric and biographic/passport information. Thus, there is clearly an increasing need for academic research in this important area of privacy regulation and standards to ensure the privacy of passengers' information in smart airports.

### 2.2.2 Personal information handling in smart cities: risks, impacts, and controls (SLR 2)

The second SLR reviewed several privacy risk models in different smart environments to extract concepts relevant to the privacy risks associated with personal information including privacy threats, vulnerabilities, current privacy control, and privacy requirements. This serves to ensure that the important concepts relevant to the domain are not overlooked when dealing with information privacy in smart airports. The comprehensive view of privacy risks in the second SLR is used to design a holistic solution to assess the privacy risks that may impact passengers' personal information in their interaction journey in smart airports within the broader context of smart cities. This will ensure that important privacy concerns are not overlooked when dealing with information privacy in smart airports. This SLR followed the method proposed by Kitchenham & Charters (2007) to analyse articles published in well-known academic database relevant to smart airports. For this SLR, 83 studies (See Appendix A) were selected from both academic and industry fields and reviewed. In this SLR, each study

selected from an academic field is denoted by the letter 'S' followed by a number, such as “S1” whereas the studies selected from an industry field are denoted by the letter “N” followed by a number for ease of reference to each selected study. This notation is used consistently throughout the text and tables to identify the studies under discussion. Similar to SLR1, each selected paper was evaluated and a score of 1-5 was assigned based on 5 assessment criteria to ensure its relevance and quality. In this SLR, the results were systematically analysed and synthesised using the Adaptive Enterprise Architecture (AEA) (Gill 2022) and CFIP (Smith, Milberg & Burke 1996) as a theoretical lens, alongside NIST 800-30 (National Institute of Standard and Technology 2013; Stoneburner, Goguen & Feringa 2002) framework as a practical lens. This was done to ensure that important points from practice are not overlooked. This method is appropriate for categorising the outcomes of this SLR since it offers sufficient coverage of the elements involved and the information privacy concerns in smart airports. The results of this review fell into three main groups: privacy risks, impacts, and controls.

### ***Privacy risks***

Risk is defined as the presence of uncertainty caused by the possibility of a negative outcome occurring. (Havlena & DeSarbo 1991). Privacy risk is defined as the expected losses related to personal information disclosure (Xu et al. 2011). Much of the literature discusses the privacy risks of personal information. For example, Nissenbaum (2004) proposes a privacy taxonomy based on contextual integrity (CI) theory, which considers human factors, including their norms and attitudes, as part of the privacy risk arising in public surveillance. Henriksen-Bulmer, Faily & Jeary (2019) propose a taxonomy using the same theoretical lens, CI, to address privacy risks in open data publishing. The privacy taxonomy developed by Solove (2006) aims to improve the understanding of information privacy in the legal system. This taxonomy classifies privacy risk into four elements: collection, processing, dissemination, and invasion (Solove 2006). Avancha, Baxi & Kotz (2012) developed a privacy taxonomy that classifies privacy threats into identity, disclosure, and access threats in e-health. The framework designed by Deng et al. (2011) provides a comprehensive analysis of privacy threats to help analysts cover the key issues in designing software. Hence, in this research, the privacy risk concept is adopted from (Xu et al. 2011), in which privacy risk is defined as the expected losses related to personal information disclosure.

We use the CFIP and AEA as theoretical lenses to identify the privacy risks associated with individual personal information in several smart environments. Firstly, we identify and categorise the privacy risk components, including privacy threats and vulnerabilities, related to

the privacy risks associated with sharing personal information in smart cities by adopting the CFIP framework dimensions: Collection, Error, Unauthorised use, and Improper access (Smith, Milberg & Burke 1996). Then, we mapped the identified risks with the layers of AEA to present the elements which are involved and interact in sharing personal information associated with the identified risks, and the relevant regulation as a governmental element that influences this sharing activity. AEA consists of the following layers: Human, Technology, Facility, and Environmental (Gill 2015a).

### Privacy threats

NIST defines threats as undesired and potential harm to Organisational assets such as operation and service, or individual information (National Institute of Standard and Technology 2013). We reviewed the selected studies to identify the privacy threats that affect the sharing of personal information in smart cities in general and several smart city sectors such as smart healthcare, smart grids, smart governments, smart business/Organisation, and smart transportation. Based on the CFIP framework, we identified seven types of privacy threats categorised as: collection, unauthorised use, improper access, and error from the total of 41% of selected studies. Table 2.13 presents the identified threats, categories, and the selected studies.

*Table 2.13 Identified privacy threats*

Category	Identified threat	Study	Percentage
Improper access	Unauthorised access (T1)	S4, S5, S6, S7, S8, N3, S38, S9, S10 S11, N2, N5, S23	16%
Unauthorised use	Secondary use (T2)	S12, S5, N3 S11, S13, S1	31%
	Modification (T3)	S14, S4, S15, S16, S11, S23	
	Information leakage (T4)	S12, S4, S7, S17, S3, S27, S38, N3, S58, S18, S19, S20, S21, S22, S56, S49, N2, S23	
	ID theft (T5)	S12, S5 S20, N11, S23	
Error	Misuse (T6)	S4, S11	2%
Collection	Policy and consent non-compliance (T7)	N3, S24, S26, S25	6%

As shown in Table 2.13, the majority of the selected studies (31%) discuss privacy threats under the unauthorised use category. This category includes the following threats: secondary use (T2),



information modification (T3), information leakage (T4), and identity theft (T5). 17% of the reviewed studies highlight unauthorised access (T1) as a privacy threat under the improper access category. The remaining studies discuss policy and regulation non-compliance privacy threats (T7) under the collection category (6%), with a few studies (2%) focussing on information misuse (T6) privacy threats under the error category (3).

As shown in Table 2.13, the privacy threats related to patients' information sharing in the smart health context have been widely discussed in the reviewed studies (N3, S4, S5, S6, S7, S8, S12, S17, S3, S27). For example, unauthorised access (T1), information misuse (T6), and modification threats (T3) have been identified as the most common threats that affect the privacy of patient information (Iwaya et al. 2019). Patient biometric data are handled by many parties in the smart health sector, which leads to secondary use (T2) and ID theft (T5) threats (Romanou 2018). Regulators and ethics committees relevant to the health sector classify information leakage (T4) as a privacy threat that affects personal information that collect, use, share in smart health (Thapa & Camtepe 2020).

As for smart grids, the reviewed studies (S9, S16, S18, S19) highlight issues such as: information modification (T3), information leakage (T4), and unauthorised access (T1) as the most common threats that impact consumers' information privacy due to sharing with different parties. On the other hand, unauthorised access (T1), secondary use (T2) and information leakage (T4) are discussed in the reviewed studies (S11, S20, S21, S13, S10, S22, N2, N5) as privacy threats that affect personal information sharing in smart cities.

As shown in Table 2.13, 6% of reviewed studies identify non-compliance with privacy policies and regulations (T7) as a privacy threat. Several countries and organisations have taken considerable steps to implement data privacy policies and regulations in order to protect personal information. According to Wall, Lowry & Barlow (2015), privacy compliance refers to an Organisation's adherence to regulatory privacy requirements to protect personal information. The reviewed studies discuss increasing information privacy issues in organisations due to non-compliance with privacy policies and regulations in different sectors, including smart cities. For example, healthcare industries handle patients' information in the USA without explicit patient consent, which is at odds with granular consent under the Health Insurance Portability and Accountability Act (HIPAA) (Runyon 2020).

## Vulnerability

A vulnerability is a weakness of an asset (e.g., information and system) plausibly exploited by threats (National Institute of Standard and Technology 2013). Based on this definition, this section reviews the selected studies to extract the perceived vulnerabilities that might be exploited by the identified threats.

As shown in Table 2.14, we identified three types of vulnerabilities relevant to the identified threats. Based on our review, 5% of the selected studies discuss that insufficient and untransparent policies lead to several privacy threats (Chua et al. 2017; Hou, Gao & Nicholson 2018; Taplin 2021). Examples of these policies include consent, ethics, and privacy policies. Furthermore, the lack of privacy regulations related to handling and sharing personal information, including biometric data, could make this information vulnerable to several privacy threats (S30) (Khi 2020). Insecure/unprotected storage systems and insecure/unprotected sharing mechanisms are identified as vulnerabilities in 3% of the selected studies. Insecure storage refers to storing sensitive data without appropriately controlling access. Sharing information in unsecured or unprotected environments leads to privacy risks in smart cities (Agrawal et al. 2021; Romanou 2018).

*Table 2.14 Identified vulnerabilities*

	<b>Identified vulnerability</b>	<b>Study</b>	<b>Percentage</b>
V1	Lacking or untransparent policies and regulations	S23, S24, S25, S30	5%
V2	Unprotected/insecure storage systems	S12, S32	2%
V3	Insecure/unprotected sharing mechanisms	S12, S32, S3	4%

### ***Mapping CFIP dimensions with AEA layers***

Our review focused on the threats that affect personal information handled in smart cities in general and different smart cities sectors such as smart health, smart grids, smart government, and smart business/organisations. Furthermore, we considered who and what are involved and interact in the handling activity, in addition to the relevant regulations as a governmental element that influences this activity (based on AEA). Tables 2.15-2.19 present the elements relevant to AEA layers, human, technology, facility, and environment, in smart cities. Figures 2.3-2.6 map of CFIP dimensions with AEA layers.

## Smart health

As illustrated in Figure 2.3, in the smart health context, elements under the human layer are identified in 11% of the selected studies and discuss the unauthorised use privacy risk associated with sharing patients' information in smart health, whereas only 7% and 1% of the studies discuss improper access and error risks. On the other hand, the elements under the technology layers are discussed in 6% of the selected studies that investigate improper access and unauthorised use privacy risks, with 0% of studies covering error and collection risks under the technology layer. However, the environmental layer is considered in 4% of the selected studies which address the privacy risks categorised under unauthorised use which is more than the studies in the improper access (1%) and collection dimensions (2%).

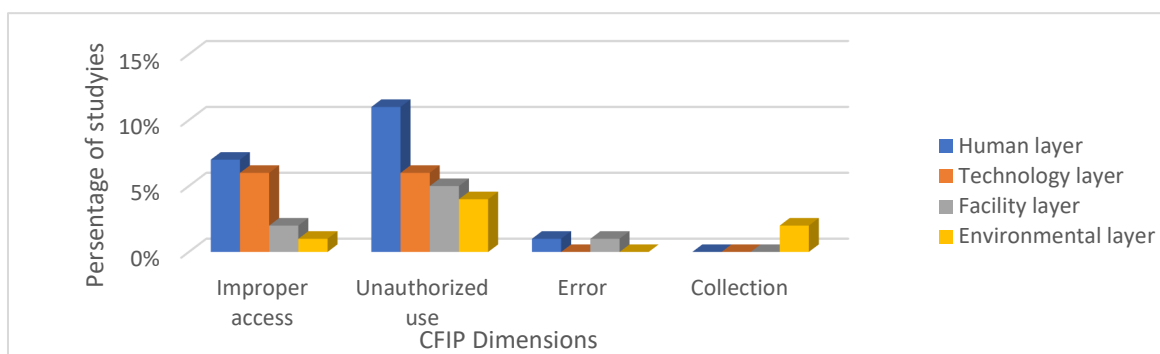


Figure 2.3 Mapping CFIP dimensions with AEA layers in smart health

We identified patients, service providers, and doctors as the main actors under the human layers from 13% of the selected studies. Infrastructure such as IoT, and data storage, such as centralised databases, are identified under the technology layer in 11% of the selected studies. The facility layer is discussed in 6% of the selected studies. The facility layer covers different smart health buildings such as hospitals, medical centres, laboratories, and clinics. Privacy regulations are mainly discussed under the environmental layer in 6% of the selected studies, which can be used to define or inform a separate layer of privacy. This seems to suggest the extension of the AEA framework through the introduction of the privacy layer.

Table 2.15 presents elements under each layer of Adaptive AE in the smart health context.

Table 2.15 Elements under AEA layers in smart health

AEA layers	Elements	Studies	Percentage
Human	Actors	S4, S5, S6, S7, S8, S38, S14, S17, S27, S58, S23	13%
Technology	Infrastructure and data storage	S5, S6, S7, S8, S38, S14, S17, S27, S23	11%
Facility	Building	S4, S8, S14, S27, S23	6%
Environmental	Privacy regulation	N3, S12, S15, S24, S1	6%

## Smart grid

In relation to smart grid, Figure 2.4 shows that more of the selected studies mention human, technology, and facility layers when addressing improper access and unauthorised use privacy risks associated with handling users' information, whereas no studies discussed these layers in relation to error and collection privacy risks.

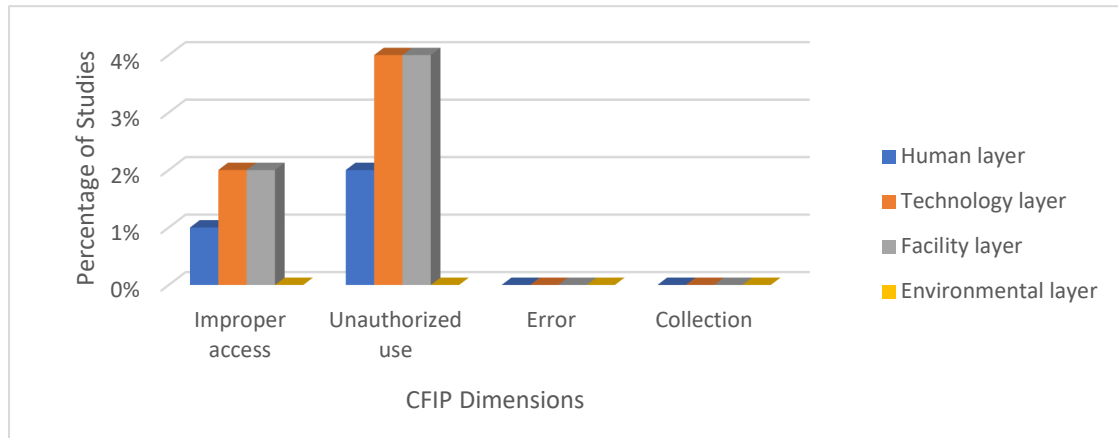


Figure 2.4 Mapping CFIP dimensions with AEA layers in the smart grid

As shown in Table 2.16, 4% of the selected studies identify different actors under the human layer in the smart grid context, including users and customer service providers. Based on our review, 6 % of selected studies discuss the usage of the cloud as the main data storage facility in the smart grid, while IoT applications and smart meters are the main infrastructures discussed in the smart grid system. Elements under the facility layer are found in 6% of selected studies that discuss privacy risks associated with sharing personal information in smart grids. Examples of facility layer elements are control centres, power sources, and home gateways.

Table 2.16 Elements under AEA layers in the smart grid

AEA layers	Elements	Studies	percentage
Human	Actors	S9, S16, S19	4%
Technology	Infrastructure, data storage, application	S9, S16, S18, S19, S23	6%
Facility	Building, utility	S9, S16, S18, S19, S23	6%

## Smart city

In smart cities, as presented in Figure 2.5, only a few studies mention the human and technology layers with improper access risk, compared with studies that address unauthorised use privacy risks associated with sharing users' information in a smart city context.

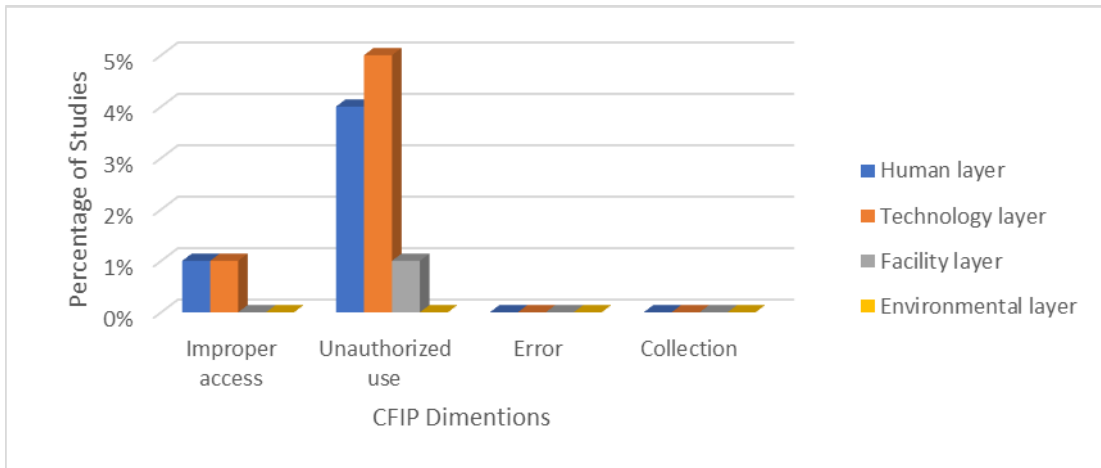


Figure 2.5 Mapping CFIP dimensions with AEA layers in smart city

Based on Table 2.17 from 5% of selected studies, we identified two main actors under human layers who are involved in sharing personal information in smart cities. The main actors include individuals, such as citizens and users, and organisations, including service providers and data holders. Moreover, IoT devices, Cloud systems, and smart cities applications are identified in 6% of selected studies as elements under the technology layers used in sharing personal information in smart cities.

Table 2.17 Elements under AEA layers in the smart city

AEA layers	Elements	Studies	Percentage
Human	Actors	S11, S13, S20, S56	5%
Technology	Infrastructure, data storage, smart application	S11, S13, S20, S21, S56	6%
Facility	Building	S13	1%

### Smart business

As illustrated in Figure 2.6, most selected studies in the smart business/Organisation context explain elements in the human, technology, and facilities layers when addressing unauthorised privacy risks associated with sharing personal information, but this percentage decreases for

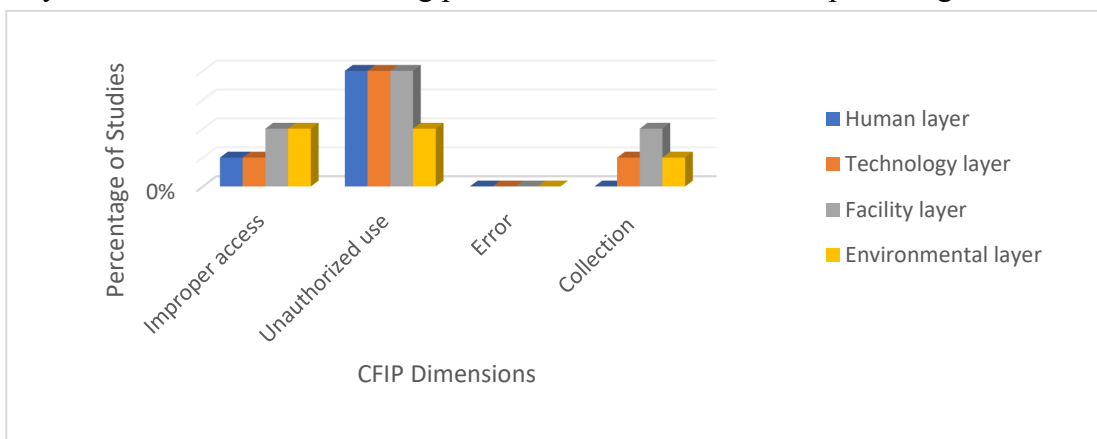


Figure 2.6 Mapping CFIP dimensions with AEA layers in smart business/Organisation

improper access privacy risk. On the other hand, the environmental layer is mentioned in 2% of studies that address privacy risks under improper access and unauthorised risks, with 1% for collection privacy risk.

Based on Table 2.18, we identified several actors, such as employees, customers, and experts, under the human layer in 4% of the selected studies. The facility layer including buildings, such as organisation, public workplaces, and industry, is discussed in 7% of the selected studies. On the other hand, technical layer elements, such as infrastructure and data storage, and environmental elements, such as privacy regulations, are discussed in 5% of the selected studies.

*Table 2.18 Elements under AEA layers in smart business/Organisation*

AEA layers	Elements	Studies	Percentage
Human	Actors	N11, N2, S22	4%
Technology	Infrastructure and data storage	N11, N2, S22, S26	5%
Facility	Building	N2, N5, S22, N11, S26, S25	7%
Environmental	Privacy regulation	N4, N5, N11, S25	5%

### Smart government and smart transportation

Table 2.19, human, technology, and facility layers are mentioned in 2% of selected studies that discuss improper access and unauthorised use privacy risks in smart government, with 1% of studies addressing unauthorised use in the smart transportation context.

*Table 2.19 Elements under AEA layers in smart government and smart transportation*

Context	AEA layers	Elements	\Studies	Percentage
Smart government	Human	Actors	S10, S23	2%
	Technology	Applications, data storage	S10, S23	
	Facility	Buildings	S10, S23	
Smart transportation	Human	Actors	S49	1%
	Technology	Infrastructure	S49	
	Facility	Vehicle	S49	

### Privacy risks impacts

We reviewed the selected studies to identify and extract the privacy requirements that are impacted by the identified privacy risks. Privacy requirements should be considered when personal information is handled in smart cities. Thus, we reviewed the selected studies to extract the privacy requirements that might be impacted by the identified threats Table 2.20. As shown in Table 2.20, we identified 8 requirements that were classified. The classifications

include the CIA triad (confidentiality, integrity, availability) and IAAA (identification, authentication, authorisation, accounting). In addition, we extracted the privacy requirements based on the classification proposed by Pfitzmann & Hansen (2010), which is very common in the privacy domain. The classification includes five privacy requirements: unobservability, anonymity, unlinkability, undetectability, and pseudonymity. Table 2.20 includes a list of privacy requirements that need to be met when sharing personal information in smart cities.

Concerning the CIA classification, 20 % of the selected studies discuss confidentiality and integrity as essential requirements to achieve privacy Table 2.20. In contrast, availability is discussed in 10 % of the selected studies to achieve security. In smart health, Health Information Exchange (HIE) has been adopted to enable the electronic sharing of patient information between several parties (Mutanu, Gupta & Gohil 2022). Thus, confidentiality, integrity, and availability are essential requirements to preserve the privacy and security of patients' information (Yi et al. 2013). In addition, the CIA triad should be satisfied in the smart grid and smart transportation to protect privacy as the information is shared between relevant parties to provide various services to the users (Yang, Xue & Li 2014).

As for the IAAA classification, 13% of the selected studies discuss authentication as a requirement for privacy Table 2.20. However, authorisation was discussed in 5% of the selected studies, whereas identification was discussed in only 2% of selected studies. In the smart grid, identification and authentication requirements need to be satisfied to secure access to the information or system component (Ferrag et al. 2018; Sadhukhan et al. 2021). In smart health, authentication, authorisation, and identification requirements should be satisfied when sharing patient information to ensure that privacy is not compromised (Shamshad et al. 2020; Wang et al. 2019).

We reviewed the selected studies to extract the requirements classified based on the terminology proposed by (Pfitzmann & Hansen 2010). As shown in Table 2.20, 12% of the selected studies discuss anonymity as an essential requirement to ensure the privacy of information, where only 1% mention unlinkability requirements. These requirements are addressed in both smart health and smart transportation to achieve the privacy of personal information (Chenthara, Khandakar & Whittaker 2019; Yang et al. 2018).

Table 2.20 Identified privacy requirements

Associated threats	Affected Requirements	Definition	Study	Percentage
T1, T3, T4, T6	Confidentiality (R1)	Restricting access to the information to authorised individuals (National Institute of Standard and Technology 2013).	S14, S4, S37, S39, S6, S40, S7, S41, S16, S9, S42, S21, S43, S45, S38, S46, S3	20%
T1, T3, T4, T6	Integrity (R2)	Preventing unauthorised changes and ensuring authenticity of information (National Institute of Standard and Technology 2013).	S14, S4, S37, S39, S6, S40, S7, S41, S16, S9, S42, S21, S43, S45, S38, S46, S3, S71	20%
T1, T3, T4, T6	Availability (R3)	Providing timely and dependable access to and utilisation of information (National Institute of Standard and Technology 2013).	S4, S14, S39, S16, S36, S42, S43, S48.	10%
T1, T3, T4	Authentication (R4)	Verification of user's identification before accessing information system resources (National Institute of Standard and Technology 2013).	S14, S6, S37, S7, S18, S36, S9, S21, S22, S45, S49	13%
T1, T3	Authorisation (R5)	Permitting access to a system resource, e.g., information (National Institute of Standard and Technology 2013).	S14, S37, S8, S48	5%
T4	Identification (R6)	Allowing only authorised people to access the stored information (Kalloniatis, Kavakli & Gritzalis 2008).	S18, S37	2%
T4, T1	Anonymity (R7)	Subject's identity is not identified by others (Pfitzmann & Hansen 2010).	S37, S7, S36, S21, S43, S44, S38, S50, S49, S3	12%
T4	Unlinkability (R8)	Impossible to determine whether the set of information is related (Pfitzmann & Hansen 2010).	S44	1%

### ***Existing privacy control***

Interest in privacy protection has been increasing since the 1990s. Thus, there has been a continuous flux of efforts to develop and use of PETs (Hiller & Blanke 2016). PETs are well-designed (ICT) systems for securing and protecting the privacy of information through the reduction, deletion, or avoidance of the improper and unnecessary processing of personal data, without decreasing the value of the individual information (Chun 2015). The goal of using PET



in smart cities is to enable the personal and sensitive information embedded in the collected data to be hidden so that it cannot be discovered by any third party or service provider (Curzon, Almeahmadi & El-Khatib 2019). Recently, many PETs have been proposed to protect the privacy of information. For example, Van Blarckom, Borking & Olk (2003) described various PET techniques such as encryption, anonymisation, pseud-identity, biometrics, identification, authorisation, and authentication. Heurix et al. (2015) provided a PET taxonomy that covered privacy aspects such as user privacy and data privacy across different domains that were not covered in the security classifications. Curzon, Almeahmadi & El-Khatib (2019) provided a comprehensive review of PETs, commonly classified as anonymisation, such as data sensitive data disruption and masking, and security techniques (such as hashing and cryptographic techniques), as the broad types of techniques used mostly for personal information privacy protection. The PETs classification proposed by Kang et al. (2007) includes three types based on the privacy information life-cycle, including operation technology, common-based technology, and administrative technologies. It is clear from previous and related research that the study of privacy-enhancing technology has been actively addressed, reflecting its importance in protecting the privacy of personal information.

We reviewed the privacy-preserving schemes for handling personal information in smart cities and extracted the existing privacy controls proposed to mitigate the risks identified from the selected studies Table 2.21 maps the privacy controls with the identified threats. Further, we classified the identified control under technical and non-technical, as shown in Table 2.21. Technical control methods include security-based solutions, such as encryption, access control, etc., whereas non-technical methods refer to management and law (National Institute of Standard and Technology 2013). Figure 2.7 represents the percentage of the identified privacy controls from the selected studies.

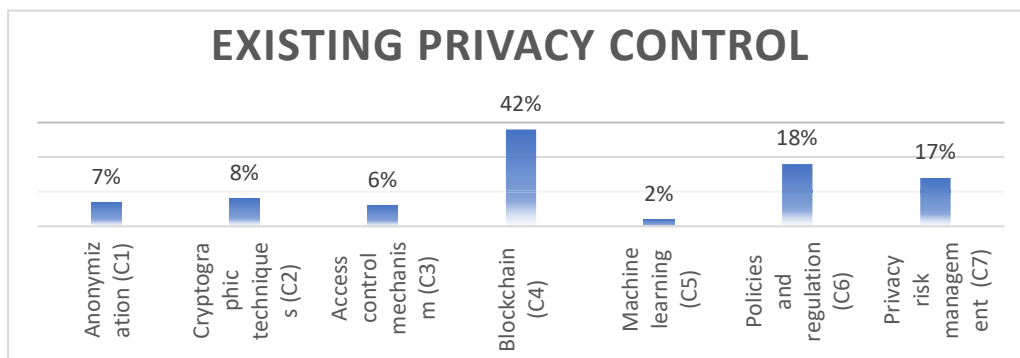


Figure 2.7 Existing privacy controls

Considering the technical solution, we identified 10 technical controls that are categorised into four groups: anonymisation, cryptographic techniques, access control techniques, and

blockchain and machine learning Table 2.21. In this study, the classification of technical solutions is based on the classification of PETs proposed by Van Blarckom, Borking & Olk (2003) and Curzon, Almeahmadi & El-Khatib (2019). In addition, we reviewed the technical controls developed based on blockchain and machine learning.

### **Data anonymisation**

As shown in Table 2.21, 7% of the reviewed studies discussed anonymisation techniques as technical privacy controls. This includes K-anonymity, differential privacy, and pseudonyms. Data anonymisation is the method used to protect personal information by preventing linking of identities (Curzon, Almeahmadi & El-Khatib 2019; Iyengar 2002; Silva, Monteiro & Simões 2021). K-anonymity and differential privacy are the most common methods of anonymisation (Iyengar 2002). As for smart health, one reviewed study (S12) discussed the popularity of using anonymity to preserve personal information privacy transmitted between parties. On the other hand, the pseudonym is discussed in (S49) as an anonymous technique that is proposed to preserve the privacy of shared information in smart transportation.

### **Cryptographic Technique**

Table 2.21 details the cryptographic techniques used in privacy-preserving schemes for sharing personal information in smart cities. The techniques were extracted from 8% of the selected studies. Cryptographic technology entails ways of entirely concealing data equivalent to the intensity of the cryptographic key and algorithm employed. Encrypting transmitted or stored personal information in smart cities is a widely used technology that protects against data leakage and achieves the privacy requirements (Curzon, Almeahmadi & El-Khatib 2019; Gaire et al. 2019). For example, Attribute-Based Encryption (ABE) is proposed to preserve patient information sharing in smart health (S7, S57). A cryptographic technique for processing biometric data is presented in (S12); in this method, the digital key is securely linked by a biometric sample that is used to encrypt and decrypt the key. Elliptic curve cryptography to secure and authenticate the communication between the consumer and the service provider in smart grid is discussed elsewhere (S36, S28).

### **Access control mechanism**

Access control is defined as security methods to control the access and use of information by applying access policies (Sandhu & Samarati 1994). As shown in Table 20.21, 6% of the reviewed studies discuss privacy-preserving schemes based on the access control mechanism. For example, the schemes presented in the selected studies propose several access control

mechanisms, such as fine-grained access control and multi-layer access control (MLAC) to preserve the privacy of patient information handled by different parties in a cloud-based environment.

### **Machine learning**

As shown in Table 20.21, we found that privacy-preserving schemes for sharing information in smart cities using machine learning techniques are discussed in 2% of the selected studies. A self-organising map (SOM) is a machine learning technique used to share information about electricity usage between parties in a smart grid (S65). The machine learning technique named federated learning is used for sharing and analysing medical cases in smart health without compromising patient privacy (S58).

### **Blockchain**

As shown in Table 20.21, 42% of the selected studies proposed privacy-preserving schemes for sharing information using blockchain technology. Blockchain is a decentralised cryptographic scheme employed to privatise and safeguard transactions in the confines of a network (Curzon, Almeahadi & El-Khatib 2019). It is noted that the privacy-preserving schemes in the selected studies integrate blockchain with other PETs to handle personal information without compromising their privacy. For example, access control mechanisms and blockchain are proposed in several studies (S4, S6, S20, S41, S48, S50, S6, S8, S26, S27, S33, S34), mainly for two purposes. The first is to allow individuals to monitor and regulate information sharing between parties in smart cities. The second purpose is to authenticate the identity while sharing and accessing the information in smart cities. The selected studies (S9, S39, S14, S63, S21, S45, S31) propose privacy-preserving schemes that use several cryptographic techniques, including signature, identity-based proxy, proxy re-encryption, zero-knowledge, and attribute-based encryption, with blockchain to protect the privacy of individual information in smart grids and smart health.

### **Non-technical control**

Of the selected studies, a total of 35 % discuss non-technical privacy control to mitigate the identified threats Table 20.21, For example, the importance of Privacy by Design (PbD) as a principle of GDPR is discussed in an attempt to protect the privacy of personal information in smart health and biometric applications (S12). Several policy-based schemes are discussed to capture the imposed requirements and restrictions that enhance the privacy of personal information in smart cities (S5, S66). On the other hand, privacy management is discussed in

the selected studies as a type of non-technical privacy control (S42, S13, S68, S67). As shown in Table 20.21, non-technical privacy controls are discussed widely in the industry reports (N1, N6, N7, N8, N9, N10, N11, N12, N4). Organisations need to reduce information disclosure as it leads to privacy and financial risks (Brian Lowans 2019).

Effective privacy management programs should address privacy risk prevention and incorporate privacy-by-design principles into all business activities (Bart Willemsen 2017). In this context, many risk management approaches, such as integrated risk management (IRM), data security governance (DSG) framework, privacy impact assessment (PIA), and continuous adaptive risk and trust assessment (CARTA), are discussed to help businesses deal with risks and their consequences, and to ensure the sustainability of the protection of any project (N6, N7, N1, N11). Furthermore, the importance of designing a privacy-aware risk program to define and assess the risk of using blockchain technology for sharing personal information is a topic of discussion in industry publications (N8, N9).

Table 2.21 Existing privacy controls

Associated threats	Privacy control classification	Type	Subtype	Study	Percentage	
T2, T4, T5	Technical- based	Anonymisation (C1)	K-anonymity	S54, S55, S56	7%	
			Differential privacy	S12, S55		
			Pseudonym	S49		
T1, T2, T4, T5,		Cryptographic techniques (C2)		Attribute-based encryption (ABE)	S7, S57	8%
				Identity-based encryption	S57	
				Biometric encryption	S12	
				Elliptic curve cryptography.	S36,28	
				Homomorphic encryption	S58	
T1, T4,		Access control mechanism (C3)		Fine-grained access control	S7, S59, S60, S2	6%
				Multi- layer access control mechanism (MLAC).	S38.	
T1, T2, T3, T4, T6		Blockchain (C4)			S9, S11, S10, S20, S41, S4, S6,	42%

Associated threats	Privacy control classification	Type	Subtype	Study	Percentage
				S61, S47, S39, S37, S8, S14, S45, S21, S22, S62, S46, S48, S50, S63, S64, S58, S27, S29, S31, S33, S34, S35, S51, S52, S53, S69, S70, S71	
T5		Machine learning (C5)		S65, S58	2%
T1, T2, T3, T4, T5, T7	Non-technical solution	Policies and regulation (C6)		S12, S5, S66, S4, S6, S20, S41, S48, S50, S23, S24, 25, S61, N12, S1	18%
T1, T2, T5, T7		Privacy risk management (C7)		S67, S42, S68, S13, N1, N6, N7, N8, N9, N10, N11, N12, N4, S23	17%

### ***Review results (SLR 2)***

This research has provided a consolidated view of the selected studies from academic and industry sources and reported on the privacy risks, impacts, and controls related to personal information sharing in smart cities. This was done to thoroughly identify the privacy risks that affect the sharing of personal information in smart cities. Since sharing personal information in smart cities results from the interaction among different elements, this study also aims to identify these elements, including actors, technologies, facilities, and privacy laws, that are involved in the sharing activity. Identifying privacy risks, including threats and vulnerabilities, the risk impacts, and existing controls, considering the elements involved in the sharing activity will assist the organisations in determining the appropriate controls to mitigate the risks when sharing personal information in smart cities. This section describes the implications based on our review and provides an analysis of the selected studies. It also includes the limitations of this work.

## **Privacy risk**

Many studies have proposed threat taxonomies that organise threats into different categories (Deng et al. 2011; Xiong & Lagerström 2019). However, to the best of our knowledge, there is a lack of a systematic and theoretical understanding, which is filled by this study using the CFIP as a theoretical lens. This study proposes a taxonomy of privacy risks of handling personal information in smart cities, including threats and vulnerabilities, based on the CFIP theoretical lens. As shown in Table 2.13 The rationale for including policies and consent non-compliance as essential aspects of our investigation lies in their crucial role in governing the handling of personal data that is gathered and utilised in smart cities. Adherence to established policies and obtaining informed consent from individuals are paramount. Failure to comply with these policies or to secure proper consent can lead to severe breaches of privacy, potentially exposing individuals to data exploitation. Furthermore, the oversight of misuse and identity theft as significant threats underscores the multifaceted nature of privacy risks within smart cities, posing substantial harm to both individuals and the broader community. The absence of thorough investigation into these threats within the reviewed studies is concerning, as it suggests a potential gap in current research and practice surrounding privacy in smart cities. Ignoring these threats leaves individuals vulnerable to exploitation and undermines the trust necessary for the successful implementation of smart city initiatives. Therefore, our finding highlights the urgent need for future research and policy development to address this critical gap.

Furthermore, we found that the selected studies do not clearly distinguish between threat events and their sources, making it hard to identify the privacy threats of relevance to the scope of this study. Thus, there is still a great deal of work to be done in this area in both academic and industry research.

On the other hand, as shown in Table 2.13, most of the selected studies discuss privacy threats associated with sharing personal information in smart cities in general and in the smart health system, specifically. In contrast, studies that discuss the same topic under the smart grid, smart government, and smart transportation systems are limited. In addition, studies selected from industry sources discuss the identified privacy threats relevant to personal information without mentioning their relationship with smart cities or any other smart system. The limited representation of studies addressing privacy concerns within specific contexts of smart cities underscores a critical gap in the existing studies. Addressing this gap is crucial for tailored privacy protection. Each smart city sector, such as the smart grid and transportation systems,

presents unique risks due to its specific functionalities. Failure to examine these risks comprehensively may leave personal information vulnerable. Understanding threats across diverse smart city sectors is vital for developing holistic privacy frameworks and policies, and enhancing innovation while mitigating risks effectively. This draws our attention to the need for more studies to cover this gap.

On the other hand, it is well accepted that any risk analysis should be done based on the identified threats and relevant vulnerabilities (Norta, Matulevičius & Leiding 2019; Stoneburner, Goguen & Feringa 2002). The identification of vulnerabilities is an essential factor that plays a role in identifying privacy risks. As shown in Table 2.14, we found that the selected studies do not investigate vulnerabilities as a significant factor in addressing privacy risks relevant to sharing personal information in smart cities. As a result, knowledge about the identified privacy risks is limited. Thus, there is a need to understand the threats and vulnerabilities to identify and mitigate privacy risks.

Based on our review, it is clear that very few studies explain who and what elements are involved in addressing the privacy risks associated with sharing personal information in smart cities. Furthermore, to the best of our knowledge, no previous studies have demonstrated the interaction among the elements involved when addressing the topic in question. To overcome these shortcomings of the previous studies, we adopted AEA as a theoretical lens to map the identified privacy risks relevant to sharing personal information in smart cities, with the elements involved and interacting in the sharing activity. This study maps the identified privacy risks based on CFIP dimensions, including improper access, unauthorised use, error, and collection, with AEA layers including human, technology, facility, and environmental. Based on Figures 2.3-2.6, it is clear that of all the studies that address the privacy risks associated with sharing personal information, most studies discuss human and technical layers, followed by the facility layer in all smart city sectors. However, a few of the studies discuss the environmental layer, including privacy regulations and policies, only when addressing improper access and unauthorised use privacy risks relevant to sharing personal information in smart health and smart business/Organisation contexts. Furthermore, based on Tables 2.15-2.19, we found that most studies that define elements under human and technology layers pertain to smart health, with few studies on other smart city sectors. Additionally, although applying policies and regulations is vital to mitigate the privacy risks associated with personal information in smart cities, we noticed that these elements, mainly categorised under the

environmental layer, have not been investigated to a sufficient extent in the selected studies. Based on the above, there is a need to cover these gaps in future work.

### **Impacts**

Undoubtedly, defining privacy requirements helps to study the consequences of privacy risks relevant to personal information. Moreover, it makes it easier to choose the proper treatment for the identified risks. In this regard, we reviewed the selected studies to identify the privacy requirements based on well-known classifications such as CIA, IAAA, and the privacy requirement terminology (Pfitzmann & Hansen 2010). Based on Table 2.20, our findings reveal that the current studies investigate the CIA triad and the identification, authorisation, authentication, and anonymity requirements for privacy risks in smart cities. However, the impact of privacy risks on accounting, undetectability, unobservability, and pseudonymity are still largely unclear. This draws our attention to the need for more studies that define these requirements when discussing the privacy risks of sharing personal information in smart cities. Another finding shows that most of the selected studies link the requirements with the proposed technical controls. They test the proposed solutions against those requirements to explain how the solutions should satisfy the requirements. However, there is a lack of studies that discuss the link between these requirements and privacy risks. For example, to the best of our knowledge, secondary use, ID theft, and policy and consent non-compliance threats are not linked with any of the identified requirements; thus, more studies are needed to cover this gap to address the consequences and impact of these risks.

### **Existing control**

We reviewed the selected studies to extract the existing privacy controls that have been proposed to preserve the privacy of shared personal information in smart cities. We categorised privacy controls based on the well-known practical framework NIST 800-30 into technical and non-technical controls. Based on Table 2.21, our findings show that technical privacy controls, such as cryptography, anonymity, access control, blockchain, and machine learning, are frequently discussed in the selected studies. However, these controls are not sufficient to preserve the privacy of personal information in smart cities because they are poorly developed due to technical and cost restrictions. Regarding technical limitations, these privacy controls can pose significant challenges as they require careful design and implementation to prevent vulnerabilities and ensure secure communication and data protection, while also preventing attacks and ensuring privacy. On the other hand, cost restrictions significantly impact the effectiveness of privacy controls in smart cities, as high costs can limit control scope and



potential vulnerabilities, and budget constraints often limit resource allocation. Thus, future efforts should be directed towards enhancing the development of these controls, ensuring their robustness, and exploring cost-effective solutions to enable comprehensive privacy protection in the complex of smart cities

Another finding shows that 23 of the selected studies propose technical solutions without implicitly explaining what kind of privacy threats could be mitigated by each proposed solution. This means that they propose their solution to preserve privacy issues in general in smart cities. Thus, linking the technical solution with specific privacy threats needs more literature investigation. Table 2.21 also shows that blockchain is widely used in privacy-preserving schemes proposed in the academic literature. These schemes integrate blockchain with various PETs, such as encryption and anonymisation techniques, so cities can ensure the security and confidentiality of sensitive data while facilitating efficient operations and services. The extensive adoption of blockchain in privacy-preserving schemes reflects its potential to address privacy concerns effectively, making it a valuable tool for smart city development.

On the other hand, our findings show that risk management has received less research activity in academic fields. This observation suggests a gap in the current understanding and exploration of risk mitigation strategies in the context of smart cities. Addressing this research gap is essential for enhancing the resilience and sustainability of smart city ecosystems, ensuring their ability to effectively mitigate and respond to emerging risks and challenges. Therefore, this area requires further research investigation.

Finally, the current research investigates the risks, impacts, and existing controls in different areas of focus (e.g., information security, information privacy) and domains (e.g., smart health, smart grid, smart airport, and smart organisations). However, based on the analysis results, it seems that these studies lack a systematic and common understanding of information privacy risks in smart cities. To address this challenge, there is a need to develop an ontology-based privacy risk assessment framework for a systematic and common understanding of privacy risks associated with sharing personal information in smart cities. Thus, this study is a first step in systematically synthesising and conceptualising the knowledge dispersed across different papers. It provides a knowledge base and foundation for developing a personal information privacy risk ontology. The ontology will help enhance the understanding of the complex concepts and their relationships. Furthermore, it will help establish a common understanding for assessing and mitigating privacy risks in an informed manner. The development and

evaluation of such an ontology are beyond the scope of this paper and are subject to further research. However, this research provides a strong foundation for this much-needed ontology work.

### 2.3 Additional literature review

This section incorporates recent relevant studies via manual search to ensure that important literature is not overlooked. The manual search focused on studies that provide both information privacy concerns and the possible solutions in the context of smart airports.

Based on the review, a study conducted by Malik et al. (2023) highlights that, as airports increasingly use digital technology and store data in specialised cloud databases, they become vulnerable to several data breach and cyber-attacks, resulting in a lack of consumer's trust. They propose a searchable encryption (SE) scheme based on partial homomorphic encryption (PHE) to improve the privacy and security of airport collected and stored data. The focus of this study is on providing a technical solution to improve the privacy and security of airport-collected data; however, it does not take into account the broader understanding of privacy risks in smart airports.

In summary, while information privacy is a key concern in smart cities and studies seek to understand it (Panahi Rizi & Hosseini Seno 2022; Rao & Deebak 2022), there is a lack of understanding this concern in smart airports. Thus, this research aims to address this gap by understanding, identifying, and analysing the privacy risks associated with passenger information in smart airports.

### 2.4 Research gaps

The SLRs analysis and review (see Sections 2.2.1 and 2.2.2) identified gaps related to the information privacy concerns in smart airports. An investigation into the context of the smart airport and information privacy indicates that passenger information privacy is a significant concern in the smart airport context. The results and findings of SLR 1 and SLR 2 indicate that studies lack an understanding of the elements involved in the passenger interaction journey in a smart airport and the relevant privacy risks. Furthermore, there is a need for a common and systematic understanding of the privacy risks associated with passenger information in smart airports. The research gaps addressed in this thesis are derived from the research problem identified in Chapter 1 (see Section 1.2) and the result of analysing the existing studies in both academic and industry fields in SLR 1 and 2. The identified research gaps are filled by answering the research questions outlined in Chapter 1 (see Section 1.3). The proposed

IJAPRA framework addresses the research gaps listed in Table 2.22 by providing a holistic framework that conceptualises, understands, assesses, and communicates the privacy risks in the smart airport context. The research gaps are presented in Table 2.22 and linked this research topic, and research questions in hand.

*Table 2.22 Research Gaps*

<b>Broad Topic</b>	<b>Narrowed Topic</b>	<b>Research Gap</b>	<b>Research Question</b>
Smart airport	Passenger interaction journey (departure side) in a smart airport (passenger-centric journey).	There is a lack of a research-based systematic conceptualisation and understanding of the elements involved to represent a passenger-centric interaction journey in smart airports.	-RQ1 must help in understanding and communicating the elements involved in a passenger interaction journey in smart airports. -RQ1 must help in conceptualising and representing a passenger-centric interaction journey in smart airports. -RQ2 aims to structure (or design) a passenger interaction journey in smart airports.
Information privacy concerns	Privacy risks associated with passengers' personal information in smart airport., existing privacy controls, and privacy requirements in smart airport context	-Studies lack of systematic and common understanding of the privacy risks associated with passenger information in the smart airport context. -There is a lack of a research-based assessment tool to assess the privacy risks associated with passenger information in smart airports.	-RQ1 must help in understanding and communicating the privacy risks associated with passenger information in smart airports. -RQ1 must help in conceptualising and representing the privacy risks associated with passenger information in smart airports. -RQ3 must assist in identifying the privacy risks associated with passenger personal information in smart airports. -RQ3 must assist in analysing the identified privacy risks in the smart airport context.

## 2.5 Summary

This chapter provided a review of relevant existing studies to obtain a better understanding of the research topic. The literature review in Section 2.1 review studies related to the following topics: smart airport, personal information, privacy, ontology, knowledge graph, graph-data model, and graph database. The chapter also discussed the results and findings of two SLRs conducted following the method proposed by Kitchenham & Charters (2007) to identify the gap in this research and develop the proposed solution. The first SLR covered in section 2.2.1

focused on the passenger interaction journey and relevant information privacy concerns, while the second SLR presented in Section 2.2.2. discussed the privacy risks associated with the handling of personal information in smart cities. This refers to the complexity of the topic addressed in this research. This chapter also provided additional review in Section 2.3 covered recent studies via manual search under the scope of this research. The research methodology adopted in this research is DSR, which is discussed in the next chapter.

## 3 Chapter 3: Design science research

This chapter presents the methodology of DSR for the development and evaluation of the proposed artefact. Before discussing the DSR, this chapter first provides an overview of the research methodologies and methods in section 3.1, followed by a review of the potential research methodologies available in the literature that are applicable to this research in section 3.2. It then discusses DSR as the most appropriate methodology to adopt in this research in section 3.3. In addition, the adopted DSR guidelines and the implementation of the DSR method in this research are discussed in sections 3.4 and 3.5. It describes the research ethics and data management in section 3.6, followed by a discussion of the methodology validity and limitations in section 3.7. Finally, the conclusion is presented in section 3.8.

### 3.1 Background

The research methodology was defined by Kothari (2004) as a systematic approach to solving the research problem and to show how the research is. It outlines the manner of applying the appropriate method to build and evaluate an artefact (Guba & Lincoln 1994). Another definition proposed by Crotty (1998); Steenkamp & McCord (2007) states that a research methodology is a strategy that guides the selection of a particular method and connects it to the intended study outcome. Research methods are defined as a set of techniques employed for collecting and analysing data relevant to a given research question or hypothesis (Crotty 1998). The nature of the research problem, questions and objectives, the type of data and resource availability, and the local research tradition in organisations are considered the main factors influencing the choice of research methodology (Benbasat, Goldstein & Mead 1987). Research methodologies can be categorised in several ways. However, the research questions nature in this research along with its underlying objectives require an iterative problem-solving methodology to achieve the aims of the research identified in Chapter 1.

### 3.2 Review of research methodologies

Several methodologies can be used in IT research. According to Steenkamp & McCord (2007); Vaishnavi & Kuechler (2015), IT research includes computer science and IS as sub-domains. This research follows the same approach. Accordingly, there are several methodologies to choose from, such as experimental research, grounded theory, case studies, analytical surveys, and DSR (Crotty 1998; Gray 2014; Vaishnavi & Kuechler 2015). In this section, a review of some of these methodological choices for this research is included.

### 3.2.1 Action research

Action research is a collaborative approach in which people work together to address problems in their communities or Organisations, with the aim of producing practical knowledge or new abilities to create knowledge that will benefit society, regardless of the scale of the outcome's impact (Reason & Bradbury 2001). It provides a method that combines practical solutions with reflection and theory, in collaboration with others, to address the needs of people (Reason & Bradbury 2001). The process of action design involves six stages, starting with identifying a real-world problem, collecting and examining data to determine the proper action to take, creating a plan for implementation, executing the plan, and finally, evaluating the effectiveness of the action taken to achieve the desired outcome (Coughlan & Coughlan 2002). Action research centres on intervention by looking at both implementation in organisations and researcher-industry collaboration (Coughlan & Shani 2005; Coughlan & Coughlan 2002). The benefits of action research lie in their practical outputs; it can employ structured quantitative or unstructured qualitative methods (frequently involving a case study)(Gray 2014). However, the research problem at hand does not focus on the collaboration and engagement of stakeholders in industry, meaning that this method was found to be unsuitable for this research.

### 3.2.2 Grounded theory

Grounded theory takes the view that the usual manifestation of social reality in practical situations should be analysed by forming grounded conceptualisations (Corbin 1990). This theory allows for the development of theories via the systematic collection and processing of data during the research (Charmaz 2006, p. 2; Fernandez, Lehmann & Underwood 2002). This methodology is well tailored to research questions where the existing literature is lacking and where a new theory needs to be constructed (Urquhart, Lehmann & Myers 2010) . The strength of grounded theory lies in its ability to provide context-specific, process-oriented explanations and details regarding a particular research issue (Orlikowski 1993). Grounded theory is exceedingly popular for IS research and is used in the following ways: the complete utilisation of the method, utilising the method to produce ideas and combining grounded theory with other research methods (Urquhart & Fernandez 2006; Urquhart, Lehmann & Myers 2010).

### 3.2.3 Experimental research

Experimental research permits the researcher to generate quantitative hypotheses as to the causal relationship between two variables, while controlling for environmental factors and altering the independent variable to eliminate alternative interpretations (Gray 2014). The benefit of experimentation is its ability to replicate laboratory results methodically, accurately

measuring the outcomes (Gray 2014). However, based on the research problem and question type (how) in this research, the qualitative research approach is a suitable choice; thus, experimental research does not suit the present project.

#### 3.2.4 Design science research (DSR)

DSR is an iterative process to develop and assess a new artefact to solve a real-world problem (Hevner et al. 2004). This type of research, which places such great emphasis on problem-solving, has the potential to close the existing gap between theory and practice (Romme 2003; Van Aken 2005). The artefact produced with the DSR process is novel and pertains to a particular research problem (Hevner 2007). It is developed based on the researcher experience, creativity and problem-solving to apply, evaluate, and refine existing theories (Hevner et al. 2004). Such artefacts can have different types such as, framework, model, method, architecture, construct, and instantiation (Vaishnavi & Kuechler 2015). Interest is rising in the research community on using DSR in IT-related fields to produce outcome and impact-driven research (Gill 2018; Gregor & Hevner 2013; Peffers et al. 2007; Vaishnavi & Kuechler 2015).

#### 3.2.5 Rationale for choosing DSR

In light of the above, DSR is selected as the most suitable approach for developing and evaluating the proposed IJAPRA framework in this research. The rationale for choosing DSR for this thesis is as follows:

1. DSR involves a problem-solving process that assists in designing and evaluating an IJAPRA artefact meant to solve the problem identified in Chapter 1.
2. DSR offers an iterative process that assists in incrementally developing the IJAPRA artefact based on kernel theories and existing knowledge (Hevner et al. 2004).
3. DSR offers clear evaluation methods and criteria to measure and test the developed IJAPRA artefact.
4. DSR has been adopted in a range of research and studies relating to privacy, risk, digital environment, and modelling (Barev, Janson & Leimeister 2020; Custodio 2021; Gerber 2015; Gross et al. 2021; Szekeres 2020).

A description of the DSR methodology implemented in this research is provided in the next section.

### 3.3 DSR: Methodology

Multiple researchers have discussed and presented ways to implement the DSR process. The DSR process adopted in this thesis is that presented by Vaishnavi & Kuechler (2015). This process model comprises five steps: awareness of the problem, suggestion, development, evaluation, and conclusion. These steps are typically ordered sequentially in the research process. Then, a description of the adopted guideline proposed by Hevner et al. (2004) to assist in conducting and evaluating the DSR process is given, followed by details on how to apply the DSR steps in this research. Figure 3.1 illustrates the DSR methodology used in this research.

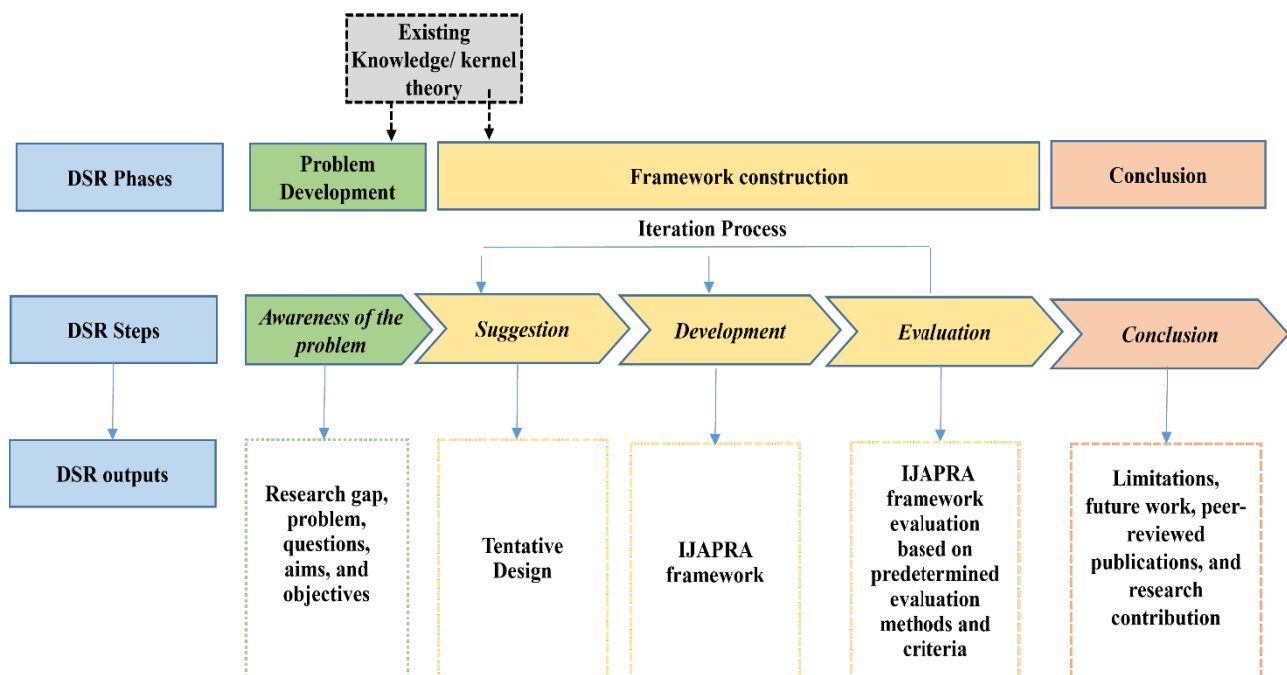


Figure 3.1 DSR Methodology

As shown in Figure 3.1, the methodology consists of three phases, namely problem development, framework construction, and conclusion. Phases one and two (problem development, framework construction) are drawn from existing studies, relevant kernel theories, and well-known standards relevant to privacy. Each phase consists of one or more steps and their outputs proceed in an iterative manner to develop and evaluate the proposed artefact. A brief description of the DSR methodology phases, steps and outcomes used in this research is given below.

The DSR process in this thesis involves five steps:

- The *awareness of the problem* step aims to generate awareness of the research domain and the problem from several sources. Chapters 1 and 2 include an overview of the initial



research and a comprehensive SLR to help understand the research domain and the analysis of the relevant studies to identify the research gaps and formalise the research problem.

- The *suggestion* step aims to propose a tentative or initial design as a problem solution while also including the choice of an appropriate tool to develop the solution. This step also relies on the review and analysis of the existing knowledge (Chapter 2) as a first step in the process of solution design.
- The *development* step presents the full development of the proposed solution. The development of the IJAPRA framework proceeds through an iterative process that is incrementally developed to fill the research gap and answer the research questions identified in Chapter 1.
- The *evaluation* step aims to evaluate the proposed artefact to identify the specific evaluation criteria. The IJAPRA framework is evaluated through three iterative processes using illustrative scenarios and expert evaluation methods to demonstrate the evaluation criteria presented in Table 3.2. and evolve the IJAPRA framework versions: alpha, beta, gamma.
- The *conclusion* step presents the output of the research effort and research journey, the key contributions, publications, implications, limitations, and future work (Chapter 6).

The eventual DSR output in this thesis consists of the following:

- Research domain, problem, questions, aims, and objectives (Chapter 1)
- Comprehensive review and research gaps (Chapter 2)
- Framework development (Chapter 4)
- Framework evaluation (Chapter 5)
- Thesis conclusion (Chapter 6)

### 3.4 Design guideline

In addition to the DSR process adopted in this research which was proposed by Vaishnavi & Kuechler (2015), this research follows the guidelines proposed by Hevner et al. (2004) to assist in conducting and evaluating an effectual DSR process and understanding the requirements for effective research. A description of these guidelines with a detailed explanation of their application in this research, is presented in Table 3.1.

*Table 3.1 DSR guidelines and their specific use in this research*

Guidelines	Description
Guideline 1- Design an artefact	According to Hevner et al. (2004), the research must produce an innovative, purposeful IT artefact to solve a specific research problem. The artefact comes in different forms such as an algorithm, framework, model, method, construct, or instantiation (Peffer et al. 2012).

Guidelines	Description
	<p>In this research, the developed artefact is the IJAPRA framework. The proposed artefact aims to address the research problem discussed in Chapter 1. The proposed framework consists of two main components: the IJPRA ontology and the IJPRA architecture. More details about the IJAPRA framework are given in Chapter 4.</p>
<p>Guideline 2- Problem relevance</p>	<p>This guideline states that DSR aims to create IT solutions for significant research problems (Hevner et al. 2004).</p> <p>The research problem presented in this thesis is that there is a lack of understanding of the privacy risks associated with passenger information in smart airports in the existing research. The research problem is presented in chapter 1. The proposed IJAPRA framework aims to address the research problem and fill the research gaps. The identified research problem and gaps are highlighted based on the analysis and results of two systematic literature reviews (SLRs), presented in chapter 2.</p>
<p>Guideline 3- Design evaluation</p>	<p>According to this guideline, the proposed artefact must be evaluated using clear evaluation methods to measure specific evaluation criteria (Hevner et al. 2004).</p> <p>In this research, the proposed IJAPRA framework is evaluated to demonstrate its applicability to represent the domain and its usefulness to fill the research gaps (see Section 1.2.1 in Chapter 1) and answer the research questions (see Section 1.3 in Chapter 1). Further evaluation criteria including applicability, understandability, usefulness for privacy experts, and generalisability are also measured (see Table 3.2). The evaluation methods that are used in this research are illustrative scenarios and expert evaluation methods (Peffer et al. 2012). Chapter 5 includes details of the evaluation of the IJAPRA framework using the aforementioned evaluation methods and criteria.</p>
<p>Guideline 4- Research Contribution</p>	<p>The effectiveness of DSR is measured by providing a significant contribution to the artefact design, methodology, or foundation (Hevner et al. 2004). The guideline requires the researcher to generate an artefact that solves a significant problem and contributes a novel idea and new knowledge to the problem domain.</p> <p>This research makes a significant contribution to the design of an artefact by developing a IJAPRA framework that addresses a significant research problem (see Section 1.2, Chapter 1) and brings new knowledge and an understanding of the privacy risks in the smart airport context. The development of the IJAPRA framework is discussed in Chapter 4.</p> <p>Furthermore, the development and documentation of illustrative scenarios (see Chapter 3) used to evaluate the proposed artefact is another contribution of this research.</p>
<p>Guideline 5- Research rigour</p>	<p>This guideline states that rigorous methods must be applied to conduct and evaluate the design artefact (Hevner et al. 2004).</p> <p>In this thesis, relevant existing knowledge, such as frameworks and standards are used as theoretical and practical lenses to guide and develop the IJAPRA framework (see Chapter 4). This approach provides valuable insights for developing an appropriate solution to the research problem. The frameworks adopted in these research were used as kernel theories as a theoretical lens in</p>

Guidelines	Description
	<p>developing IJAPRA, including CJM (Rosenbaum, Otalora &amp; Ramírez 2017), AEA (Gill 2022), CFIP (Smith, Milberg &amp; Burke 1996), LINNDUN(Robles-González, Parra-Arnau &amp; Forné 2020), and Unified foundational Ontology (UFO) (Guizzardi 2005). In addition, the well-known standards and frameworks of the NIST, including the NIST privacy framework (National Institute of Standard and Technology 2020), and NIST 800-30 (National Institute of Standard and Technology 2013) are used as practical lenses to guide the development of the IJAPRA framework. The utilisation of these theoretical and practical lenses is discussed in Chapter 4.</p> <p>Moreover, rigorous methods were used for the IJAPRA framework evaluation (see Chapter 5) The framework was evaluated using two well-known DSR evaluation methods: illustrative scenarios and expert evaluation methods. The developed research instruments were assessed internally by supervisors and externally by experts in the domain and updated based on their feedback to ensure the quality and relevance of the developed instrument, including scenarios and a survey. A survey with experts in the field of information privacy/security and data protection was conducted to get their feedback and opinions on the proposed framework; then, the framework was updated based on the responses of the experts which helped in building and refining the framework and its components.</p>
Guideline 6- Design as a research process	<p>This guideline advises using all resources and means to reach desired goals while following the problem environment's laws (Hevner et al. 2004). The systematic well-known DSR process steps proposed by Vaishnavi &amp; Kuechler (2015) are utilised to create new artefacts. The adopted process involves five main steps: (1) awareness of the problem,(2) propose a tentative solution, (3) develop the solution, (4) evaluate the developed solution, (5) conclusion. The research DSR process adopted in this thesis relies to a very great extent on the iterative review of relevant exciting knowledge and developing and evaluating the IJAPRA framework. The iterative process identifies the problem, presents the solution, and repeats the process until the solution meets the research objectives.</p>
Guideline 7- Communication of research	<p>This guideline recommends that the output of DSR should be presented to both management-oriented and technology-oriented communities (Hevner et al. 2004). In this thesis, the outcome produced by DSR is communicated in peer-reviewed publications.</p>

### 3.5 Applying DSR in this research

The steps of the research process model applied in this thesis are discussed below. The process consists of five steps, namely awareness of the problem, suggestion, development, evaluation, and conclusion.

### 3.5.1 Awareness of the problem

This step aims to generate awareness of the research domain, formulate the research problem, and identify the research questions, aims and objectives. To understand the research domain, a literature review was undertaken to cover topics on privacy, personal information, and smart airports (Chapter 1 and Chapter 2). Following this review, two SLRs were conducted to identify the research gaps (Chapter 2). The results of the SLRs were reported under the main categories in Chapter 2. Based on the SLR findings, the research gaps relevant to the domain were identified. In addition to conducting the SLRs, a brainstorming session and discussion with the supervisors took place. Consequently, the research gap was specified, the research scope was determined, and the research problem was formulated (see Section 1.3, Chapter 1). Further, the research questions, aims, and objectives were identified as well. The tasks and output of this step are presented in Figure 3.2. The main research question of this research is:

**How to design the passenger interaction journey and assess the associated information privacy risks in the context of the smart airport?**

This research question was divided into three sub-questions:

RQ1: How to model the knowledge of the domain of privacy risk associated with passenger information during their interaction journey in a smart airport?

RQ2: How to design the passenger interaction journey architecture in a smart airport?

RQ3: How to assist in the assessment of privacy risks associated with passengers' information during their interaction journey in a smart airport?

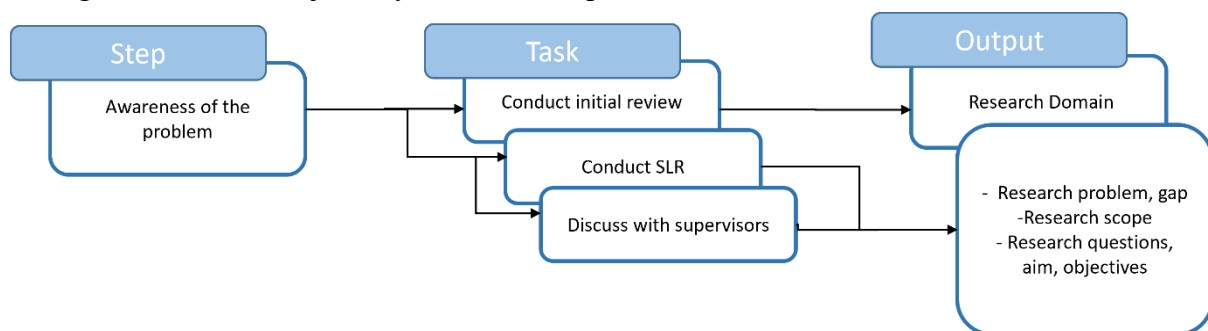


Figure 3.2 Awareness of the problem step

### 3.5.2 Suggestion

This step aims to provide a roadmap for developing the proposed solution to solve the research problem and research gap (see Section 1.2, Chapter 1). Thus, a useful technique is identified and the necessary elements to develop the proposed solution are determined as a part of this step. The IJAPRA framework has been proposed as a solution to the research questions outlined in Chapter 1 (Section 1.3), providing a practical solution to the identified problem.

The proposed solution is the IJAPRA framework which provides a practical solution to the research questions identified in Chapter 1. The IJAPRA framework consists of two components: IJPRA ontology and IJPRA architecture (Figure 4.1 in Chapter 4). The vital part of the proposed framework is the IJPRA ontology. The IJPRA ontology is the result of the integration of IJ and PR ontology which captures the knowledge, concepts, and relationships around privacy risks in a smart airport (see Chapter 4, Figure 4.2). The graph-based modelling approach is identified as an appropriate technique to represent the IJPRA ontology. The second component is the IJPRA architecture which comprises two layers: the IJ and PR layers (see Chapter 4, Figure 4.11), which are designed based on the IJPRA ontology. According to Ameller & Franch (2011); Gill (2022), architectural models can be designed utilising ontology, which involves capturing concepts and their corresponding relationships. To design the proposed solution, kernel theories, including the relevant frameworks, as well as the standards are identified and adopted as theoretical and practical lenses (Chapter 4, Table 4.2). The IJAPRA framework aims to help privacy experts in understanding and analysing privacy risk to design the best privacy solutions relevant to passenger information in the smart airport context. Figure 3.3 illustrates the tasks and output of the suggestion steps implemented in this research.

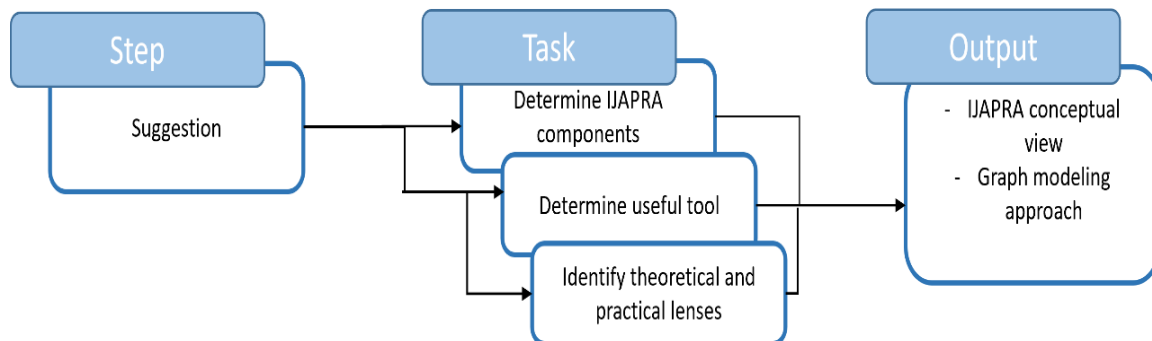


Figure 3.3 Suggestion step

### 3.5.3 Development

In this stage, the IJAPRA framework is fully developed through increments conducted to answer the research questions (RQ1, RQ2, RQ3) (see Section 1.3, Chapter 1). The IJAPRA framework consists of two components: IJPRA ontology and IJPRA architecture. The IJPRA ontology addressed **RQ1: How to model the knowledge of the domain of privacy risk associated with passenger information during their interaction journey in a smart airport?**, whereas the IJPRA architecture addressed **RQ2: How to design the passenger interaction journey architecture in a smart airport?**

And **RQ3: How to assist in the assessment of privacy risks associated with passenger's information during their interaction journey in a smart airport?**

The development of the IJAPRA framework was organised in five increments: three increments for the development of the IJPRA ontology, and the remaining two increments for IJPRA architecture development (as discussed in Chapter 4, Table 4.1). In the IJPRA ontology development, the first two increments involved the development of the IJ and PR ontologies, followed by representing the ontologies using a graph-based modelling approach (Pokorný 2016). The third increment included the integration of the IJ and PR ontology to develop the IJPRA ontology, which was also represented using graph-based modelling approaches (Pokorný 2016). To develop the IJPRA ontology, the guidelines of ontology development proposed by Uschold & Grüninger (1996) were adopted. These guidelines comprise three steps: purpose, capture, and implementation (Uschold & Grüninger 1996). The IJAPR ontology purpose and intended uses were identified in the purpose step and the relevant key concepts and relationships were captured by conducting two SLRs (see Chapter 2) in the capture step. The first SLR extracted and identified the concepts relevant to the smart airport domain, while the second SLR reviewed several privacy risk models in different smart environments to extract concepts relevant to the privacy risks associated with personal information. This serves to ensure that the important concepts relevant to the domain are not overlooked when dealing with information privacy in smart airports. After the development of the IJPRA ontology, the development of the IJPRA architecture, the second component of the IJAPRA framework, was carried out in the remaining two increments, increments 4 and 5 (Chapter 4, Table 4.1). The fourth increment involved the development of the IJ layer, followed by the development of the PR layer in increment 5. The proposed solution aims to answer the research questions (RQ1, RQ2, RQ3) in Chapter 1. The development of the last version (gamma) of the IJAPRA framework is discussed in Chapter 4. During the development process, the identified frameworks and standard were adopted as theoretical and practical lenses to guide the development of each IJAPRA framework components (see Chapter 4, Table 4.2). Figure 3.4 shows the tasks and output of development steps implemented in this research.

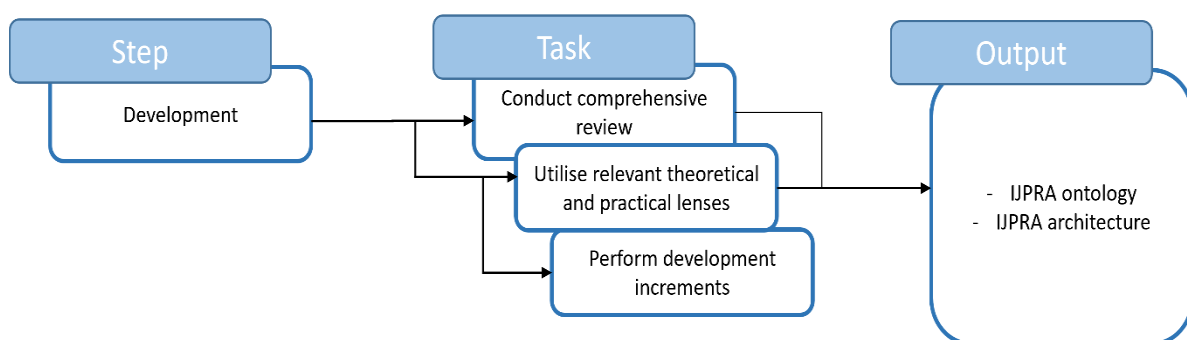


Figure 3.4 Development step.

### 3.5.4 Evaluation

The evaluation step used the well-known DSR evaluation methods to evaluate the proposed framework against predetermined evaluation criteria (Peffers et al. 2012; Venable, Pries-Heje & Baskerville 2012). The evaluation aims to evaluate the developed IJAPRA framework against the evaluation criteria, shown in Table 3.2, and update the framework based on the evaluation result. The proposed IJAPRA framework is evaluated through iterative processes. Three iterations are implemented and the IJAPRA framework is updated based on the result of each iteration evaluation as illustrated in Chapter 5. The proposed IJAPRA framework is evaluated using two well-known DSR evaluation methods:

- Illustrative scenarios
- expert evaluation via field survey.

As previously discussed, the evaluation went through three iteration process to evaluate and update the framework versions (alpha, beta, gamma). In the first and second iterations, the alpha version of the developed framework was evaluated using illustrative scenarios to measure the applicability of the IJPRA ontology, the first component of the framework, in representing and capturing the domain. This evaluation process aligns with the cognitive process that includes perception, learning, synthesising, and analysis to create new knowledge (Wang & Chiew 2010). By employing this approach, the scenarios were deeply explored with analysis and comparisons conducted to capture new knowledge. The results of these evaluation iterations were used to evolve the developed ontology by emerging new concepts and relationships relevant to the domain; followed by refining and improving the IJPRA architecture, the second component of the IJAPRA framework, whereupon the beta version of the framework was developed. Then, the beta version was evaluated using the expert evaluation method via a field survey. In the expert evaluation method, the IJPRA architecture, the second component of the IJAPRA framework, was evaluated to measure its applicability, usefulness, generalisability, and understandability (Table 3.2). The survey was sent to 230 experts via LinkedIn and email, requesting their opinions and feedback on the beta version of the framework. The participants were selected based on their minimum three years of experience in the field of information privacy/security and data protection. Of the 230 surveys distributed, 35 experts completed the survey, and their responses were considered for data analysis in the evaluation. The results of the field survey were used to obtain the gamma version of the IJAPRA framework based on the experts' feedback and to identify the scope for future work. The gamma version of the IJAPRA framework is discussed in Chapter 4. The tasks and output of the evaluation step are shown in Figure 3.5.



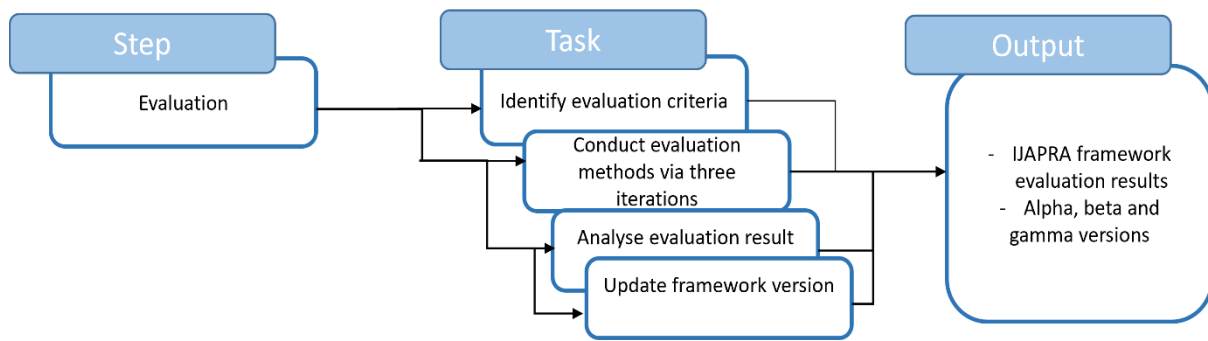


Figure 3.5 Evaluation Step

Table 3.2 Evaluation criteria

Criteria	Description	Evaluation method
Applicability	The framework is applicable for representing and capturing knowledge relevant to the domain. The framework is applicable for assisting in privacy risk assessment.	Illustrative scenario Expert evaluation via field survey
Understandability	The framework is clear and understandable.	Expert evaluation via field survey
Usefulness	The framework is useful for privacy experts (practitioners and researchers). The framework is useful to fill the research gaps.	Expert evaluation via field survey
Generalisability	The framework is general and can be fitted to different smart environments or contexts.	Expert evaluation via field survey
Novelty	The framework provides new knowledge on privacy risks in the context of smart airports.	Study review

### ***Illustrative scenario***

The developed ontology, the first component of the IJAPRA framework, is evaluated by undertaking an analysis with multiple illustrative scenarios to verify whether the artefact meets its goal (Prat, Comyn-Wattiau & Akoka 2014). Five hypothetical scenarios are developed to instantiate the developed IJPRA ontology. The developed scenarios vary depending on different personas and privacy risks that impact their information, to describe the problem and provide a solution. This evaluation method is used to provide evidence of the applicability of the IJPRA ontology to represent and capture the domain of privacy risks in the smart airport context.

Scenarios are defined as a description method that is of great interest in both academic and industry fields (do Prado Leite et al. 2000). The literature presents scenario development approaches, each with its own focus and objectives. For example, Williams et al. (2016) proposed a methodology for future scenarios for privacy and security that involves four steps: reviewing the existing relevant scenarios, coding the scenarios in themes, grouping similar scenarios, and finally expanding the scenarios for different situations. Mahmoud et al. (2009)



reviewed the existing scenario development approaches and proposed a scenario construction process for environmental decision making. This approach consists of a scenario definition, where extensive consultations among researchers and stakeholders take place to identify a particular feature of the scenario that is of interest; scenario construction involves scrutinising scenarios with sufficient information and the capability of bringing outcomes; scenario analysis, which relies heavily on the experts' findings and analytical results among the driving forces; scenario assessment identifies the risks involved, trade-offs, and mitigating opportunities; risk management involves monitoring and post-audits as things continue to change and be reviewed. Another development approach proposed by do Prado Leite et al. (2000) focuses on scenario management and Organisation . This approach comprises five activities to generate and evaluate scenarios, namely deriving, describing, organising, verifying, and validating. Although existing approaches provide a good starting point for scenario development, there is a need for more effective scenario development and documentation approaches (do Prado Leite et al. 2000; Mahmoud et al. 2009). Thus, this research proposes a methodology to develop and document scenarios. The TOGAF framework (Terence Blevins and Mike Lambert 2022) and scenario construction process illustrated by do Prado Leite et al. (2000) have been adopted to guide the development of the scenario documentation methodology proposed in this research. The proposed methodology consists of four phases that are used in an iterative manner to develop and document the scenarios, as shown in Figure 3.6.

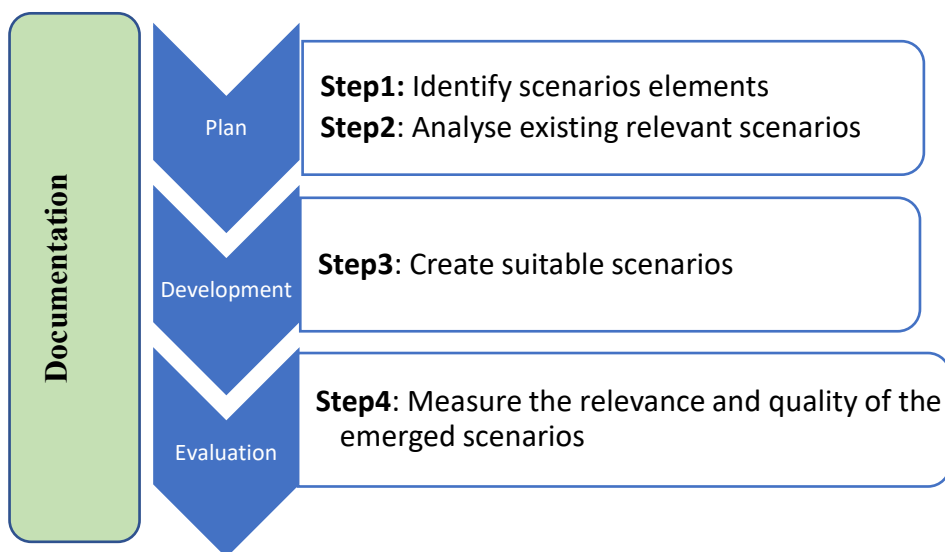


Figure 3.6 Scenario development and documentation

As shown in Figure 3.6, the first phase, plan, consists of two steps. The first step is determining the problem and providing appropriate solutions as well as identifying scenario elements such

as actors and environment and the interaction between them. The second step involves reviewing and analysing the relevant existing scenarios in both academia and industry. The second phase is development, which includes emerging scenarios that are relevant to the research based on the output of the first phase. The third phase, evaluation, includes evaluating the scenarios produced to ensure their quality and relevance; the evaluation includes walkthrough review sessions which were conducted with the research team, and a review of the scenarios by the external experts in the domain. The developed scenarios were refined based on the feedback received. The documentation phase is a crosscutting phase to document important details about the scenario in textual form. The documentation includes a scenario overview, a description of the actors, process, technology, as well as their relationships, a description of the problem and appropriate solutions, the scenario implementation tool, and the scenario result.

***Expert evaluation via field survey***

The developed architecture, the second component of the IJAPRA framework, is evaluated using the expert evaluation method via a field survey. According to Runeson & Höst (2009), a survey constitutes the gathering of particular information from specialists and specific population groups. As shown in Table 3.3, the survey in this research employs the rating numbers. The participants' qualitative responses to the survey questions are transformed into numerical values (quantitative ratings), as shown in Table 3.3. This helps facilitate the quantitative analysis of the survey results. The values in Table 3.3 reflect how strongly the participants agreed or disagreed with the statement.

*Table 3.3 Survey rating*

Qualitative rating	Quantitative rating	Rating description
Strongly disagree	1	Indicates that the participants disagreed strongly with the statement.
Disagree	2	Indicates that the participants disagreed with the statement.
Average	3	Indicates that the participants somewhat agreed with the statement.
Agree	4	Indicates the participants agreed with the statement.
Strongly agree	5	Indicates the participants agreed strongly with the statement.

This research followed a well-known survey process proposed by Hyndman (2008) presented in Table 3.4.

Table 3.4 Survey process

Process	Activity
Planning a survey	State the survey objective, including its needs, purpose, and required information.
Design the sampling procedure	Identify target participants (with due consideration of ethics).
Select a survey method	Plan the method of data collection. For the purpose of this research, an online method was utilised.
Develop the questionnaire	Develop a field survey questionnaires with experts using the evaluation criteria in (Prat, Comyn-Wattiau & Akoka 2014).
Pre-test the questionnaire	Conduct the survey with a small sample of participants to evaluate the construction and relevance of the research instrument
Conduct the survey	Carry out the survey effectively over a specified timeframe. period
Collect and analyse the data	Collect qualitative and quantitative data from the survey. Analyse the collected data from the survey using two steps: <ul style="list-style-type: none"> <li>• quantitative evaluation</li> <li>• qualitative evaluation.</li> </ul>

### Survey questionnaire development

The evaluation criteria were employed for quantitative and qualitative survey evaluation. The evaluation criteria utilised in the field survey were created using a common artefact evaluation criteria (Prat, Comyn-Wattiau & Akoka 2014) to evaluate the IJAPRA artefact. These criteria were used to develop the survey questionnaire (see Appendix E), which was then used to assess the IJAPRA against the evaluation criteria identified in Table 3.2, as discussed in Chapter 5.

### Survey quantitative evaluation

The data collected from the field survey were categorical in nature, and the participants provided qualitative responses to the survey questionnaires (as presented in Table 3.3). In this study, statistical formulas were utilised to analyse the survey data, adapted from (Bou Ghantous & Gill 2021). Statistical formulas are commonly used when the objective is to interpret numerical data from a survey. Statistics is concerned with extracting meaning from data (Hyndman 2008). The statistical formulas employed in the analysis of the data are presented in Equations 3.1–3.3.

Chi <sup>2</sup> Statistical Formula
Chi <sup>2</sup> or X <sup>2</sup> = $\sum(O-E)^2/E$ (O = frequency and E = expected value) (p-value < 0.01)
E = $\sum O/N$ (O = frequency and N = total number of observations)
The p-value determines if the null hypothesis H <sub>0</sub> is accepted or rejected based on a critical value, $\alpha = 0.01$
If p-value < $\alpha$ , then H <sub>0</sub> is rejected and H <sub>1</sub> is accepted, and there is a positive association between the test variables (IJAPRA components) and the evaluation criteria (see Table 3.2).
[If p-value < 0.000 $\alpha$ ( $\alpha$ is a small number), then p is mathematically corrected to p < 0.001]
H <sub>0</sub> (null hypothesis): there is no association between the test variables and the evaluation criteria.
H <sub>1</sub> (alternative hypothesis): the test variables and the evaluation criteria are positively associated.

Equation 3.3 Frequency of Average and Above (FAA) Formula

PAA Formula
PAA = $\sum$ Percentage (ratings $\geq 3$ )
PAA is the sum of all response percentages [Average (3) + Agree (4) + Strongly Agree (5)].

Equation 3.3 Percentage of Average and Above (PAA) Formula

FAA Formula
FAA = $\sum$ Frequency (Ratings $\geq 3$ )
FAA is the sum of all participants' responses [Average (3) + Agree (4) + Strongly Agree (5)]

### Survey qualitative evaluation

The qualitative data gathered from the field survey was analysed using the hypothesis confirmation general analysis technique (Runeson & Höst 2009). The hypotheses were determined by the evaluation criteria (Table 3.2). The evaluation criteria adopted from (Prat, Comyn-Wattiau & Akoka 2014). The feedback from participants, who were experts, was compared to the evaluation criteria by identifying the occurrence of criteria in the participants' responses, adopted from (Bou Ghantous & Gill 2021). The expert feedback was then organised into Tables, which provided explanations of the participants' feedback and categorisations to identify the criteria in the feedback.

#### 3.5.5 Conclusion

As shown in Figure 3.7, the consolidated IJAPRA framework for privacy risks associated with passenger information in the smart airport context produced output consists of the following:

- IJAPRA framework
- Research publications and output
- Research implications
- Discussion of research limitations and future direction for IJAPRA.

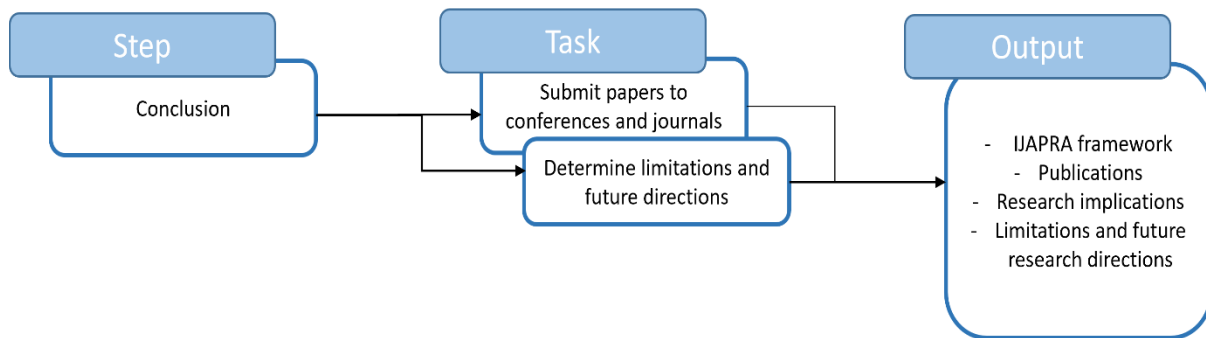


Figure 3.7 Conclusion step

### 3.6 Research ethics

According to the University of Technology Sydney research ethical guidelines, a formal approval (approval number UTS HREC REF NO. ETH20-5093) was acquired from the UTS Research Ethics Committee. The formal approval is presented in Appendix B. There were no ethical problems raised by this research. Each participant to the survey received the invitation letter (Appendix C) along with the online survey information sheet (Appendix D). The online survey information sheet provides information about the online survey, the IJAPRA framework, and a survey link. The purpose of these forms was to ensure transparency regarding the project details, survey questionnaires, data anonymity, and data storage. Participants were informed that they were not required to participate in this research, they could withdraw from the study at any time, and their responses would be kept confidential if they chose to participate. In addition, according to UTS research data management policy, the data will be stored in the UTS systems, and only the supervisor and researcher of this thesis have access to the stored data via their UTS secure login. The information collected anonymously from the participants' responses to the online survey will not reveal their identities in any way and will only be utilised for the purpose of this research project and any resulting publications, whether in the form of conference presentations or journal articles.

### 3.7 Research validity and limitations

The validity and reliability of the overall DSR and qualitative research can be upheld according to Golafshani (2003), who indicated that validity and reliability should be considered by qualitative researchers when developing and analysing the results of a study and evaluating its quality.

According to Creswell & Miller (2000), validity in qualitative research can be influenced by the researcher's perception of validity and their paradigm choices. Consequently, researchers have devised multiple terms to define validity, such as quality, rigour, and trustworthiness (Golafshani 2003). Lincoln & Guba (1985, p. 316) state that validity and reliability are closely

interrelated, and validity cannot exist without reliability; thus, establishing validity is deemed sufficient to ensure reliability (Golafshani 2003).

To ensure the validity and reliability of this research, the rigour of DSR, the methodology adopted in this research, is evaluated according to guideline 5 (see Table 3.1) in pertinent work (Hevner et al. 2004). The proposed IJAPRA framework was developed through the DSR iterative process, and relevant knowledge bases including frameworks and standard were used as theoretical and practical lenses to develop the IJAPRA framework. Furthermore, the proposed framework was examined by conducting evaluation using two methods: illustrative scenarios and expert evaluation. The illustrative scenario was conducted by developing five hypothetical privacy risk analysis scenarios to demonstrate the framework applicability to describe and represent the domain in the scope of this research. A field survey was conducted with 35 experts in information privacy/security and data protection from both academia and industry to obtain their valuable opinion and feedback on the proposed framework. The proposed framework was updated based on the results of the evaluation analysis of both evaluation methods; this helped in building and refining the framework and its components. In addition, the development research instruments, including illustrative scenarios and the field survey, were reviewed internally with supervisors and externally by experts in both the academic and industry fields to ensure their quality and relevance and the instruments were updated based on the feedback received.

There are potential methodological limitations relevant to the field survey recruitment method and the sample used in this research. The first concern is that the survey included closed-ended questions with a list of predetermined choices from which the participants were required to select. This approach may limit their responses to the current options and components of the proposed framework, potentially overlooking other aspects. However, the survey design also incorporated open-ended questions, allowing participants to provide subjective feedback and suggestions on the proposed framework beyond the predefined options. This combination of closed-ended and open-ended questions aimed to allow participants to provide valuable feedback to assess and improve the framework. Further, a combination of qualitative and quantitative data analysis was used to gain a more comprehensive understanding of the survey results.

Another consideration is the sample size of the participants, as data collection and analysis were limited to 35 respondents due to the research project scope constraints. Similar to other

studies, a sample size of 35 is considered sufficient for evaluating the proposed framework (Albladi & Weir 2018; Almaliki et al. 2014). It is worth mentioning here that after 25 surveys, there was a repetitive pattern of responses with less new information. Furthermore, to compliment the survey, illustrative scenarios were used to provide additional evaluation and insights. This involved applying the proposed framework to hypothetical scenarios to analyse and update the framework based on the evaluation result. These two different methods helped to identify gaps and resultant improvements in the proposed framework (see Chapter 5).

### 3.8 Summary

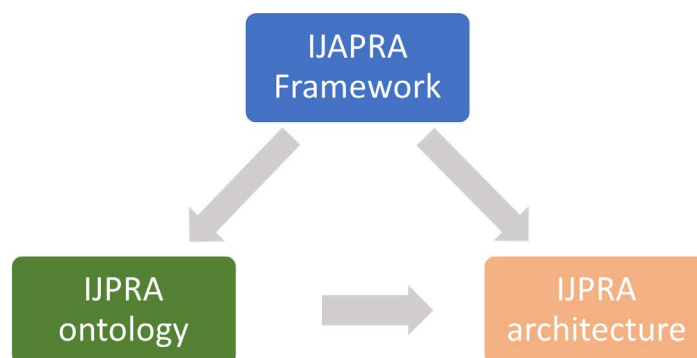
This research aims to develop a novel IJAPRA framework for privacy risks associated with passenger information in the smart airport context. The DSR employed to develop the proposed framework, following the well-known guidelines (Hevner et al. 2004; Vaishnavi & Kuechler 2015). This chapter presented the methodology used to develop and evaluate the IJAPRA. The evaluation methods used were illustrative scenarios and expert evaluation methods. The expert evaluation was conducted by field survey to involve experts in the field to obtain their feedback relating to the Generalisability, applicability, understandability, and usefulness of the IJAPRA framework. The IJAPRA (final version) development is presented in detail in Chapter 4.

## 4 Chapter 4: The IJAPRA framework

The novel IJAPRA framework, which is the main contribution of this research, is discussed in this chapter based on the scope of this research. The proposed framework provides a practical solution to the research questions identified in Chapter 1. The IJAPRA consists of two components: the IJPRA ontology and the IJPRA architecture. The IJAPRA framework was developed using the well-known DSR methodology discussed in Chapter 3. This chapter presents details of the incremental development of the gamma version of the IJAPRA framework, which is the final version. Section 4.1 provides an overview of the IJAPRA framework. Section 4.2 discusses the incremental development of the IJPRA ontology, which is a vital component of the framework. Section 4.3 explains the development of IJPRA architecture driven by the IJPRA ontology. Finally, Section 4.4 presents the conclusion. The iteration process of the evaluation of the alpha and beta versions of the IJAPRA framework is discussed in Chapter 5 to prevent potential confusion between the contribution, which is the development of the IJAPRA gamma version, and the evaluation in this research.

### 4.1 The IJAPRA framework overview

The IJAPRA framework provides new knowledge and an understanding of the privacy risks associated with passenger information in the smart airport. The novel IJAPRA framework consists of two components: IJPRA ontology and IJPRA architecture. A high-level conceptual view of the IJAPRA framework and its two components is presented in Figure 4.1.



*Figure 4.1 High-level conceptual view of the IJAPRA framework*

The development of the IJAPRA framework was organised into five increments to achieve the research objectives (Section 1.3, Chapter 1). The first three increments include the activities of developing the IJPRA ontology, whereas the remaining two increments encompass the development of the IJPRA architecture (Table 4.1). A description of the activities associated



with these increments, along with the corresponding IJAPRA framework components, is shown in Table 4.1.

*Table 4.1 Increments activities for developing the IJAPRA framework*

IJAPRA framework components	Increment	Activity
IJPRA ontology	Increment 1- IJ ontology development	Identified kernel theories, including frameworks (see Table 4.2), review existing studies relevant to smart airport systems to capture the knowledge (concepts and relationships), and extract and define concepts and their relationships for IJ ontology development. The developed IJ ontology was represented using a graph modelling approach.
	Increment 2- PR ontology development	Identified kernel theories, including frameworks and practical standards (see Table 4.2) and reviewed existing studies relevant to privacy risk models to capture and define concepts and their relationships for PR ontology development. The developed PR ontology was represented using the graph-modelling approach.
	Increment 3-IJPRA ontology development	Integrated IJ and PR ontologies to develop IJPRA ontology. The concepts of the integrated ontology were arranged into metamodel layers (M2, M1, M0). The integrated ontology was represented using a graph-modelling approach.
IJPRA architecture	Increment 4- IJ layer development	Developed the main components of the IJ layer, including asset and journey. The components were organised into five views: IJ-Actor, IJ-Technology, IJ-Process, IJ-Information, and IJ-Factor.
	Increment 5- PR layer development	Developed privacy risk identification (PRIdentification) tool and privacy risk assessment (PRAssessment) tool to assist and guide the identification and assessment of privacy risks associated with passenger information in smart airports.

Furthermore, the IJAPRA framework is developed based on existing studies, relevant kernel theories, including frameworks and standards as theoretical and practical lenses, and expert evaluation feedback. The set of theoretical and practical lenses adopted in developing the IJAPRA framework is presented in Table 4.2. The utilisation of these lenses is discussed in the development of each component of the IJAPRA framework (see Section 4.2 and Section 4.3). The IJAPRA framework aims to assist privacy experts, in both the academic and

industry fields, in understanding and analysing privacy risk to design the best privacy solutions relevant to passenger information in a smart airport. Details of the development of the IJPRA ontology and IJPRA architecture are discussed in the following sections.

*Table 4.2 Adopted theoretical and practical lenses.*

<b>Theoretical and practical lenses</b>	<b>Description</b>
Customer Journey Map (CJM)	CJM is a visual representation of the sequence of activities and actions that Organisations widely apply to understand customer interactions and experience (Rosenbaum, Otolara & Ramírez 2017). The CIM was utilised as a theoretical lens in the development of the IJAPRA framework, specifically in the development of the IJ under the IJPRA ontology and the IJ layer in the IJPRA architecture.
Adaptive Enterprise Architecture (AEA)	AEA is a framework that comprises layers, such as human, technology, facility, environment, and security, interacting in a system, including organisations and enterprises (Gill 2015b; Gill 2022). AEA layers help in systematically extracting and mapping domain-related elements (Anwar, Gill & Beydoun 2019; Gill 2022). The AEA was used as a theoretical lens in developing both components of the IJAPRA framework, particularly in developing IJ under the IJPRA ontology and IJ layer in the IJPRA architecture.
Concerns for Information Privacy (CFIP)	CFIP is a framework that provides a multidimensional structure to identify and analyse individuals' concerns regarding the privacy of their information in practice (Smith, Milberg & Burke 1996). CFIP categorises privacy concerns under various categories including collection, unauthorised use, improper access, error, combining data, and reduced judgment (Smith, Milberg & Burke 1996). CFIP has been adopted as a theoretical lens to identify and categorise privacy threats affecting passenger information in smart airports. This framework served as a theoretical lens in developing both components of the IJAPRA framework. It was particularly adopted to develop the PR ontology and (PRIdentification) tool.
Threat modelling framework (LINNDUN)	LINNDUN is a well-known privacy threat modelling framework offering a systematic approach for eliciting privacy threats (Robles-González, Parra-Arnau & Forné 2020). Deng et al. (2011) proposed the LINDDUN framework, which is notable for its systematic approach to privacy threats. Each letter in LINNDUN stands for each threat type identified in the framework (Deng et al. 2011). The LINNDUN also provides a comprehensive list of privacy threat tree patterns and maps PETs to recognised privacy threats (Robles-González, Parra-Arnau & Forné 2020; Wuyts, Scandariato & Joosen 2014). LINNDUN is classified as one of the mature approaches to elicit and categorise threats relevant to privacy (Wuyts, Sion & Joosen 2020). The categorisation is structured based on the threat categories: linkability, identifiability, non-repudiation, detectability, disclosure of information, unawareness, and non-compliance (Deng et al. 2011; Wuyts, Scandariato & Joosen 2014; Wuyts, Sion & Joosen 2020). LINNDUN was adopted as a theoretical

Theoretical and practical lenses	Description
	lens in developing both components of the IJAPRA framework, including the IJPRA ontology and IJPRA architecture, specifically in developing PR ontology and (PRIdentification) tool.
Risk-based framework	The risk-based framework was proposed by Iguchi, Uematsu & Fujii (2018) as a guideline to assess and quantify privacy risk by evaluating both the severity level and likelihood level. The combination of severity and likelihood level scores helps determine the overall risk level. The framework is utilised as a theoretical lens in developing the (PRAssessment) tool under the PR layer in the IJPRA architecture.
National Institute of Standards and Technology (NIST)	<p>NIST plays a pivotal role in providing comprehensive guidance and standards for various aspects of cybersecurity and privacy (Brooks, Lefkovitz &amp; Nadeau 2017). NIST's expertise extends to privacy, offering invaluable guidance to organisations seeking to effectively protect individual privacy (National Institute of Standard and Technology 2020). Two notable contributions from NIST in this regard are the NIST 800-30 (National Institute of Standard and Technology 2013) and the NIST Privacy Framework (National Institute of Standard and Technology 2020).</p> <p>NIST 800-30 (National Institute of Standard and Technology 2013) is a well-known standard that offers comprehensive, improved and flexible guidelines that are used widely in the industry to carry out risk assessments in compliance with NIST guidelines (National Institute of Standard and Technology 2013; Peacock 2021). The NIST Privacy Framework serves as a tool, aiding organisations in identifying and managing privacy risks. This enables them to create innovative services and products to protect the privacy of individuals (National Institute of Standard and Technology 2020).</p> <p>NIST SP 800-30 standard and NIST privacy framework were adopted as practical lenses to understand and extract essential elements to identify and assess privacy risks to develop the IJPRA ontology.</p>
Unified Foundational Ontology (UFO)	UFO is an essential framework that serves as a common grounding for knowledge representation and constructing domain ontologies, providing a standardised set of foundational concepts and relationships (Guizzardi 2005). By utilising UFO as a starting point, ontology developers can ensure consistency and interoperability among different domain ontologies (Guizzardi 2006). The UFO is used as a theoretical lens to develop the IJPRA ontology to ensure its consistency and interoperability.

## 4.2 The IJPRA ontology

The IJPRA ontology is an essential component of the IJAPRA framework. The IJPRA ontology is used to define the domain concepts as well as the relationships among them and with the passenger interaction journey and associated privacy risks in the smart airport. The IJPRA

ontology addresses **RQ1: How to model the knowledge of the domain of privacy risk associated with passenger information during their interaction journey in a smart airport?** (see Section 1.3, Chapter 1). The IJPRA ontology is the outcome of the integration of the IJ ontology, which represents knowledge pertaining to the passenger interaction journey in the smart airport, and the PR ontology, which captures key concepts and relationships relevant to the privacy risk associated with passenger information in smart airports. A conceptual view of the IJPRA ontology is shown in Figure 4.2.

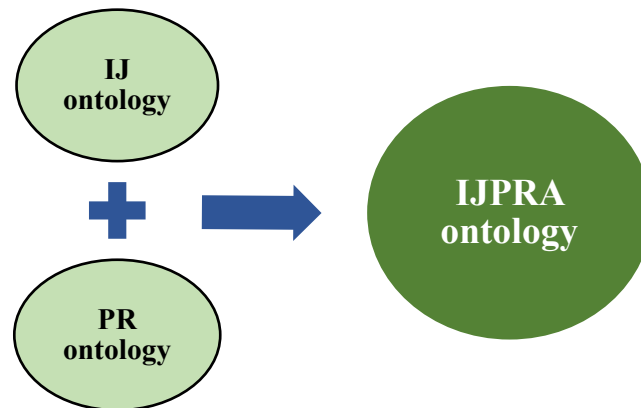


Figure 4.2 IJPRA ontology conceptual view

The IJPRA ontology was incrementally developed through the stages of the DSR methodology along with the ontology development guidelines proposed by Uschold & Grüninger (1996), as discussed in Chapter 3, Section 3.5.3. The IJPRA ontology was developed according to the three steps based on ontology development guidelines (Uschold & Grüninger 1996).

- *Step 1: Defining the purpose*

This step aims to identify the IJPRA ontology purpose and intended uses (Uschold & Grüninger 1996). The purpose of developing the IJPRA ontology is to fill the gap in relation to the lack of research-based systematic and common understanding of privacy risks associated with passenger information in the smart airport context. The IJPRA ontology can be utilised as a tool to conceptualise, analyse, and communicate privacy risks in smart airports.

- *Step 2: Capturing the knowledge*

This step involves capturing knowledge about the passenger interaction journey in smart airports and the associated privacy risks by identifying and defining relevant concepts and relationships within the domain. The knowledge capture was executed through comprehensive reviews and the adoption of relevant practical and theoretical lenses to identify and categorise

the concepts. A list of adopted practical and theoretical lenses used in developing the IJPRA ontology are presented in Table 4.2. The UFO (Guizzardi 2005) was used as a theoretical lens to develop the IJPRA ontology due to its significant role in developing the domain ontology conceptual model (Guizzardi 2006). The concepts identified in the IJPRA ontology were mapped with relevant concepts in the UFO based on the meaning and properties for consistency and interoperability of the developed ontology (Guizzardi 2006). Definitions of the UFO concepts are found in the literature (Guizzardi 2005; Guizzardi, Falbo & Guizzardi 2008; OntoUML 2018).

- *Step 3: Implementing the ontology*

The implementation step includes representation of the ontology using a graph-based modelling approach (Pokorný 2016). To represent the IJPRA ontology using a graph-based modeling approach, the concepts in the ontology are represented as labelled nodes, where labelled edges represent the relationships in the IJPRA ontology (Pokorný 2016). The graph modelling approach is appropriate as it provides a connection-oriented (relating to concepts and their relationships) and a flexible structure to represent the ontology (Gill 2022). The graph model was implemented using the Neo4j graph database (Van Bruggen 2014).

As explained in Section 4.1, the development of the IJPRA ontology is organised into three increments (see Table 4.1). The increment activities include: (1) development of the IJ ontology, (2) development of the PR ontology, and (3) integrating the IJ and PR ontology to develop the IJPRA ontology.

#### 4.2.1 Increment 1 - IJ ontology

Increment 1 explains the development of the IJ ontology. Following the capture step in the ontology guidelines (Uschold & Grüninger 1996), the CJM (Rosenbaum, Otalora & Ramírez 2017) and AEA (Gill 2022) were adopted as theoretical lenses (see Table 4.3) to assist in extracting and identifying entities relevant to the passenger interaction journey in the smart airport context. The CJM was selected because it aids in the recognition and understanding of passenger travel stages, and activities during their travel, such as check-in, border control, and boarding stages. AEA was selected because it provides systematic layers for extracting and mapping the elements involved and interacting during passenger journeys, such as actors, processed, information, and technology. This indicates the complex nature of the problem being addressed in this research.

Additionally, an SLR (Alabsi & Gill 2021) (see Chapter 2) was conducted to identify and extract concepts and relationships relevant to the passenger travel journey in the smart airport context. The SLR results were analysed and reported in the following categories: (1) passenger travel journey stages involving smart airport applications; (2) elements (people, process, information, and technology) in the journey; and (3) standards and regulations relevant to privacy in the aviation industry that regulate the handling of passenger information during the journey. The definitions of some concepts were inferred from the theoretical lenses used, including CJM and AEA, as well as relevant existing studies from academic and industry fields. However, there are newly emerged concepts that can be mapped to closely related definitions in relevant studies but may not be exactly defined; these emerged concepts are labelled as “new” under the ref column. Table 4.3 includes the identified concepts, sub-concepts, and their definitions in IJ ontology.

*Table 4.3 IJ ontology concepts, sub-concepts, and their definitions (C is concept label; the SC label refers to sub-concept).*

<b>Label</b>	<b>Concept</b>	<b>Definition</b>	<b>Ref</b>
C1	Actor	Individual and organisation interact with each other as per their role in the smart airport.	(Gill 2022)
SC1.1	Individual/Passenger	An individual who benefits from services provided by several organisations in a smart airport.	New
C1.2	Organisation/ SP	A service provider that offers several services for passengers and airlines in a smart airport.	(European Union Agency for Network and Information Security 2016)
SC1.3	Organisation/Airline	An airline company that offers air transport services to passengers.	(European Union Agency for Network and Information Security 2016)
SC1.4	Organisation/Gov	A government that operates security services for passengers at several stages of their journey.	(European Union Agency for Network and Information Security 2016)

Label	Concept	Definition	Ref
C2	Passenger_Information	Represents passenger data, in digital format, that is handled during the interaction journey in a smart airport.	(Gill 2021b)
SC2.1	E_Tdoc	Represents numerous kinds of travel documents in their electronic versions such as e-passport, e-visa, e-boarding pass, and e-ID, that include passenger personal information.	New
SC2.2	Ppersonal_Information	Represents any information in digital format about an identified or identifiable passenger in the smart airport.	(Milne et al. 2017; Psychoula 2020)
C3	Information_Type	The category of the passenger personal information in a smart airport, such as PII, medical, or financial information, as well as passenger records and biometric data.	(Chua, Ooi & Herbland 2021)
SC3.1	PII	Personally identifiable information is a type of personal information that is linked to the passenger either directly or indirectly.	(Chuleeporn 2008; ISACA n.d.)
SC3.2	Passenger_Record	A type of passenger personal information that includes information about the passenger booking and identity in an electronic record.	new
SC3.3	Financial_Info	A type of passenger personal information that identifies a passenger's financial details, such as credit cards, assets, income, bank accounts, and expenses.	(Chua, Ooi & Herbland 2021)
SC3.4	Biometric_Info	A type of passenger personal information that refers to biological information about a passenger.	(Morosan 2018; Patel 2018)
SC3.5	Medical_Info	A type of passenger personal information that identifies their health or medical conditions.	(Chua, Ooi & Herbland 2021)
C4	Information_Classification	The way to classify passenger personal information based on its sensitivity level, for example, confidential, public, private, and restricted.	(Peter H.Gregory 2021, p. 315)
C5	Technology	Represents technological interface and digital infrastructure involved in the passenger interaction journey.	New
SC5.1	Tech_Interface	Represents interfaces, for example, self-service technology, automated technology, and biometric technology, used by actors to implement the processes during passenger interaction journey.	(Rajapaksha & Jayasuriya 2020) (Gill 2022)

Label	Concept	Definition	Ref
SC5.2	Storage_System	Represents a type of digital infrastructure that enables a technological interface in a smart airport. Examples of storage systems are databases and cloud-based storage.	New
C6	Smart airport	The facility that hosts elements involved and interact in the passenger interaction journey.	(Gill 2022)
C7	PasInterJourney	Represents elements involved and interacting during the passenger travel journey in a smart airport.	new
C8	Journey_Stage	Represents several zones of passenger travel journey in the smart airport.	(Willemsen & Cadee 2018)
C9	Process	A set of activities during the passenger journey.	(Gill 2022)
SC9.1	Stage_Process	The activities to complete each stage of the passenger journey.	(Gill 2022; Rosenbaum, Otorora & Ramírez 2017)
SC9.2	Information_Flow	The activities of handling passenger personal information during each stage of the passenger journey.	(Gill 2022)
C10	Factor	Represents internal and external legal influences and guides the passenger journey and the use and handling of their information, such as privacy regulations, privacy standards.	(Gill 2022)
SC10.1	Privacy_Regulation	The law that influences and guides the purpose behind collecting passenger personal information and its intended use.	(ISACA n.d.)
SC10.2	Privacy_Standard	The guideline of establishing requirements for handling passenger personal information, implementing data security, and compliance with privacy regulations in the smart airport.	(ISACA n.d.)

Following the identification and definition of the IJ concepts, the IJ concepts and sub-concepts were grounded in eight concepts in the UFO. Table 4.4 presents the mapping between the IJ concepts and UFO concepts.



Table 4.4 Mapping IJ concepts and sub-concepts with UFO concepts

UFO concepts	IJ concepts
Kind/role	Actor, Individual/ Passenger, Organisation/ SP, Organisation/Airline, Organisation/Gov
Object	Passenger_Information, Ppersonal_Information, E_Tdoc, PII, Passenger_Record, Financial_Info, Biometric_Info, Medical_Info
Kind	Technology, smart airport
Action	PasInterJourney, Process, Stage_Process, Information_Flow.
Phase	Journey_Stage
Plan	Factor, Privacy_Regulation, Privacy_Standard
Category	Information_Type, Information_Classification, Tech_Interface, Storage_System

As discussed previously, the capture step in the ontology development guidelines (Uschold & Grüninger 1996) includes identifying concepts and relationships relevant to the domain. According to this step, a list of relationships among the identified concepts was captured based on a review of the existing studies. The identified relationships included INTERACT, HOST, INVOLVEDIN, USE, HANDLE, CLASSIFY, PASSTHROUGH, COMPLETE, INFLUENCE, ENABLE, TYPE\_OF, IMPLEMENT, INCLUDE, and SUB\_CLASS\_OF. The relationship "SUB\_CLASS\_OF" is used to define the connection between concepts and their sub-concepts. Figure 4.3 shows the IJ concept- relationship matrix. To access the Excel sheet for larger matrix, Figure 4.3, please click on [IJ concepts relationships matrix](#), or zoom in to view Figure 4.3 in a larger size. This matrix focuses on the core relevant relationships in IJ ontology. The matrix is shown in next page in Figure 4.3.

	Actor	Individual/Passenger	Organisation/SP	Organisation/Airline	Organisation/Gov	Passenger_Information	E_Tdoc	Ppersonal_Information	Information_Type	PII	Passenger_Record	Financial_Info	Biometric_Info	Medical_Info	Information_Classification	Technology	Tech_Interface	Storage_System	Smart airport	PasInterJourney	Journey_Stage	Process	Stage_Process	Information_Flow	Factor	Privacy_Regulation	Privacy_Standard
Actor	INTERACT	BASE_CLASS_OF	BASE_CLASS_OF	BASE_CLASS_OF	BASE_CLASS_OF											USE			HOSTE_BY	INVOLVEDIN							
Individual/ Passenger	SUB_CLASS_OF																				PASSTHROUGH						
Organisation/ SP	SUB_CLASS_OF																										
Organisation/Airline	SUB_CLASS_OF																										
Organisation/ Gov	SUB_CLASS_OF																										
Passenger_ Information							BASE_CLASS_OF	BASE_CLASS_OF											HOSTE_BY	INVOLVEDIN							
E_Tdoc						SUB_CLASS_OF		INCLUDE																			
Ppersonal_ Information						SUB_CLASS_OF	INCLUDED_IN								CLASSIFIED_INT0									HANDLED_BY			
Information_Type								TYPE_OF		BASE_CLASS_OF	BASE_CLASS_OF	BASE_CLASS_OF	BASE_CLASS_OF	BASE_CLASS_OF													
PII									SUB_CLASS_OF																		
Passenger_Record									SUB_CLASS_OF																		
Financial_Info									SUB_CLASS_OF																		
Biometric_Info									SUB_CLASS_OF																		
Medical_Info									SUB_CLASS_OF																		
Information_Classification								CLASSIFY																			
Technology																	BASE_CLASS_OF	BASE_CLASS_OF	HOSTE_BY	INVOLVEDIN		IMPLEMENT					
Tech_Interface									SUB_CLASS_OF									ENABLED_BY									
Storage_System									SUB_CLASS_OF								ENABLE										
Smart airport	HOST					HOST										HOST											
PasInterJourney																						DEVIDED_INT0				INFLUENCED_BY	
Journey_Stage																							COMPLETED_BY				
Process																			HOSTE_BY	INVOLVEDIN				BASE_CLASS_OF	BASE_CLASS_OF		
Stage_Process																					COMPLETE	SUB_CLASS_OF					
Information_Flow								HANDLE															SUB_CLASS_OF				
Factor																					INFLUENCE					BASE_CLASS_OF	BASE_CLASS_OF
Privacy_Regulation																								SUB_CLASS_OF			
Privacy_Standard																								SUB_CLASS_OF			

Figure 4.3 IJ ontology concepts-relationships matrix

The identification of the adopted theoretical lenses (Table 4.2), the extraction and definition of the relevant concepts and sub-concepts (Table 4.3), and the identification of the relationships among concepts (Figure 4.3) were conducted in the capture step to develop the IJ ontology. Then, the IJ ontology is represented using a graph-modelling approach (Pokorný 2016) according to the implementation step in the ontology development guidelines (Uschold & Grüninger 1996). In the graph modelling approach, concepts in the IJ ontology are depicted as labelled nodes, with labelled edges representing the relationships of the IJ ontology (Pokorný 2016). Employing graph modelling to represent ontology gives a connection-oriented (as in concepts and their associations relationships) and flexible structure to depict the ontology (Gill 2022). As shown in Figure 4.4, the IJ graph-based model is implemented using the Neo4j graph database (Pokorný 2015). In Figure 4.4, green nodes represent main concepts (Table 4.3), while blue nodes show sub-concepts (as presented in Table 4.3).

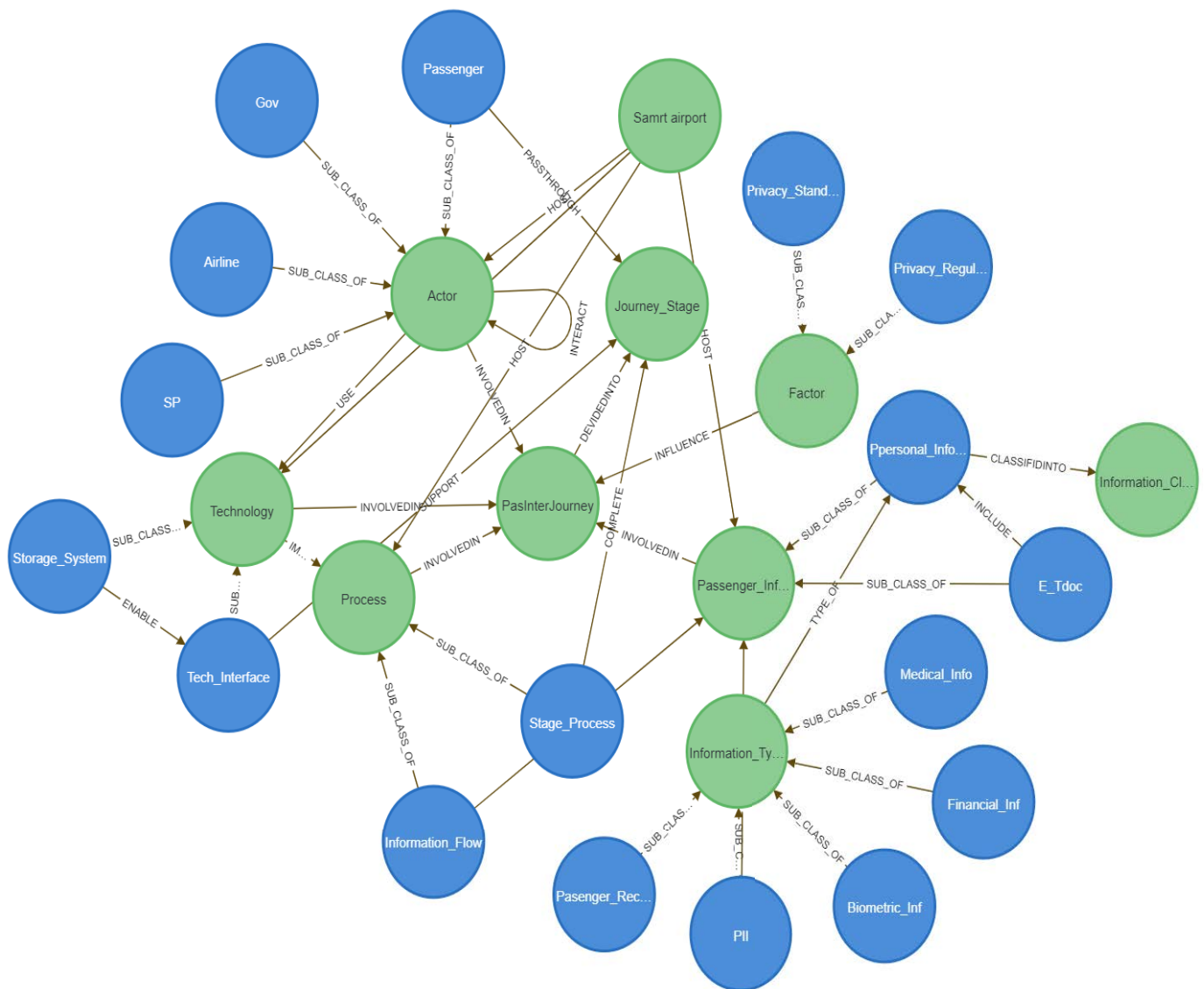


Figure 4.4 IJ graph-based model

#### 4.2.2 Increment 2 - PR ontology

In Increment 2, the PR ontology was developed by adhering to the capture and implementation steps in the adopted ontology development guidelines (Uschold & Grüninger 1996). In the capture step, an exhaustive review of the existing studies in both the academic and industry fields on privacy models in several smart environments, such as smart health, smart homes, smart airports, and smart cities, etc. was conducted (see Chapter 2). This review aims to identify and extract key concepts and relationships relevant to privacy risks, requirements, and controls associated with personal information in several smart environments, including smart airports (Chapter 2). This provided broader coverage and a comprehensive view of the privacy risks that impact passenger information in their interaction journey in smart airports within the overall context of smart cities. In addition, relevant kernel theories, including frameworks such as CFIP (Smith, Milberg & Burke 1996) and privacy threat analysis framework (Deng et al. 2011), along with standards such as the NIST 800-30 standard (National Institute of Standard and Technology 2013) and NIST privacy framework (National Institute of Standard and Technology 2020), were adopted for concept extraction and categorisation. This indicates the complex nature of the problem being addressed in this research. A description of the theoretical and practical lenses used to develop the PR ontology is provided in Table 4.2. The NIST SP 800-30 and NIST privacy framework were used as practical lenses to identify and extract essential elements in privacy risks associated with passenger information in smart airports. These elements include privacy threats, vulnerabilities, privacy requirements, and privacy control. The CFIP and privacy threat analysis frameworks were utilised as theoretical lens to extract and categorise numerous privacy threats that cause privacy risks associated with passenger information in smart airports. The extracted privacy threats are categorised into four categories: unauthorised access, improper use, non-compliance, and unawareness, based on the adopted theoretical lenses. The definitions of concepts were inferred from the theoretical and practical lenses used, as well as the existing studies. The identified concepts and sub-concepts of the PR ontology and their definitions are presented in Table 4.5.

*Table 4.5 PR concepts, sub-concepts, and their definitions (C label refers to concept, SC is the sub-concept label).*

Label	Concept	Description	Ref
C1	Privacy_Risk	Probability of the passenger information being disclosed by a potential event and resulting in impact to passenger and their information in the smart airport context.	(National Institute of Standard and Technology 2013, 2020; Xu et al. 2011)

Label	Concept	Description	Ref
C2	Privacy_Threat	Undesired potential events, either internal or external, that cause privacy risk.	(National Institute of Standard and Technology 2013)
SC2.1	Unauthorised_Access	Represents a threat type of access to passenger information by unauthorised people.	(Smith, Milberg & Burke 1996)
SC2.2	Improper_Use	Represents a threat type of modifying stored information and/or using collected passenger information for other than an authorised purpose (secondary use), and/or sharing information with unauthorised parties.	(Smith, Milberg & Burke 1996)
SC2.3	Non-Compliance	Represents a threat type of handling passenger personal information in the smart airport context without compliance with privacy regulation.	(Deng et al. 2011; Smith, Milberg & Burke 1996)
SC2.4	Unawareness	Represents a threat type where a passenger is unaware of the purpose of collecting their personal information, of what and how their personal information is handled.	(Deng et al. 2011)
C3	Privacy_Requirement	Represents obligations arising from law and other sources to meet passenger privacy needs to protect passenger information handled during their journey.	(National Institute of Standard and Technology 2013, 2020)
SC3.1	Confidentiality	Represents a privacy requirement to maintain authorised constraints on accessing and disclosing passenger personal information to protect their privacy.	(National Institute of Standard and Technology 2013, 2020)
SC3.2	Integrity	Represents a privacy requirement to prevent unauthorised changes and ensure the authenticity and non-repudiation of passenger personal information.	(National Institute of Standard and Technology 2013, 2020)
SC3.3	Availability	Represents a privacy requirement to guarantee timely and dependable access to and utilisation of passenger information.	(National Institute of Standard and Technology 2013, 2020)
SC3.5	Anonymity	Represents a privacy requirement to ensure passenger's identity is not identified by others	(Deng et al. 2011; Pfitzmann & Hansen 2010)
SC3.6	Unlinkability	Represents a privacy requirement to conceal the connection between two or more types of passenger personal information.	(Deng et al. 2011; Pfitzmann & Hansen 2010)

Label	Concept	Description	Ref
C4	Privacy_Control	Safeguards to mitigate the privacy risk and satisfy privacy requirements relevant to passenger personal information in the smart airport.	(National Institute of Standard and Technology 2020)
SC4.1	Tech_Control	Represents a type of privacy control that includes security-based solutions	(National Institute of Standard and Technology 2020)
SC4.2	NonTech_Control	Represents a type of privacy control that includes administrative safeguards.	(National Institute of Standard and Technology 2020)
C5	Privacy_Vulnerability	Represents a weakness in handling passenger personal information that may be exploited by a privacy threat.	(National Institute of Standard and Technology 2013)

Following the identification and definition of the PR concepts, these concepts are mapped with three concepts in UFO based on the correspondence in their meanings. The mapping of the PR concepts with UFO concepts is shown in Figure 4.6.

*Table 4.6 Mapping PR concepts and sub-concepts with UFO*

UFO concepts	PR concepts
Event	Privacy risk, Privacy threat, Unauthorised_Access, Improper_Use, Non-Compliance, Unawareness, Privacy Vulnerability
Plan	Privacy requirement, Confidentiality, Integrity, Availability, Anonymity, Unlinkability.
Action	Privacy_Control, Tech_Control, NonTech_Control

In ontology development guidelines, the capture step involves identifying relevant concepts and relationships within the domain (Uschold & Grüninger 1996). As part of this step, a list of relationships between the identified PR ontology concepts was formed by analysing the existing studies. The relationship matrix between PR concepts and sub-concepts is shown in Figure 4.5. This matrix focuses on core relevant relationships in the PR ontology. The identified relationships for the PR ontology included: CAUSE, MITIGATE, EXPLOIT, AFFECT, and SUB\_CLASS\_OF. The relationship "SUB\_CLASS\_OF" is used to define the connection between concepts and their sub-concepts in the PR ontology.

	Privacy_Risk	Privacy_Threat	Privacy_Vulnerability	Unauthorized_Access	Improper_Use	Non-Compliance	Unawareness	Privacy_Requirement	Confidentiality	Integrity	Availability	Unlinkability	Anonymity	Privacy_Control	Tech_Control	NonTech_Control
Privacy_Risk		CAUSED_BY						AFFECT						MITIGATED_BY		
Privacy_Threat	CAUSE		EXPLOIT	BASE_CLASSES_OF	BASE_CLASSES_OF	BASE_CLASSES_OF	BASE_CLASSES_OF									
Privacy_Vulnerability		EXPLOITED_BY														
Unauthorized_Access		SUB_CLASS_OF														
Improper_Use		SUB_CLASS_OF														
Non-Compliance		SUB_CLASS_OF														
Unawareness		SUB_CLASS_OF														
Privacy_Requirement	AFFECTED_BY								BASE_CLASS_OF	BASE_CLASS_OF	BASE_CLASS_OF	BASE_CLASS_OF	BASE_CLASS_OF	SATISFIED_BY		
Confidentiality								SUB_CLASS_OF								
Integrity								SUB_CLASS_OF								
Availability								SUB_CLASS_OF								
Unlinkability								SUB_CLASS_OF								
Anonymity								SUB_CLASS_OF								
Privacy_Control	MITIGATE							SATISFY							BASE_CLASS_OF	BASE_CLASS_OF
Tech_Control														SUB_CLASS_OF		
NonTech_Control														SUB_CLASS_OF		

Figure 4.5 PR ontology concepts-relationships matrix

After capturing the knowledge (concepts, sub-concepts, and relationships) to develop the PR ontology, the ontology is represented using a graph-modelling approach (Pokorný 2016) based on the implementation step in the adopted ontology development guidelines (Uschold & Grüninger 1996). In the graph-modelling approach, concepts in the PR ontology are represented as labelled nodes, whereas labelled edges represent the relationships of the PR ontology (Pokorný 2016). In Figure 4.6, the main concepts are showcased as yellow nodes, while sub-concepts are illustrated as light brown nodes. The Neo4j graph database (Pokorný 2015) was used as a tool to implement the PR graph model, as shown in 4.6.

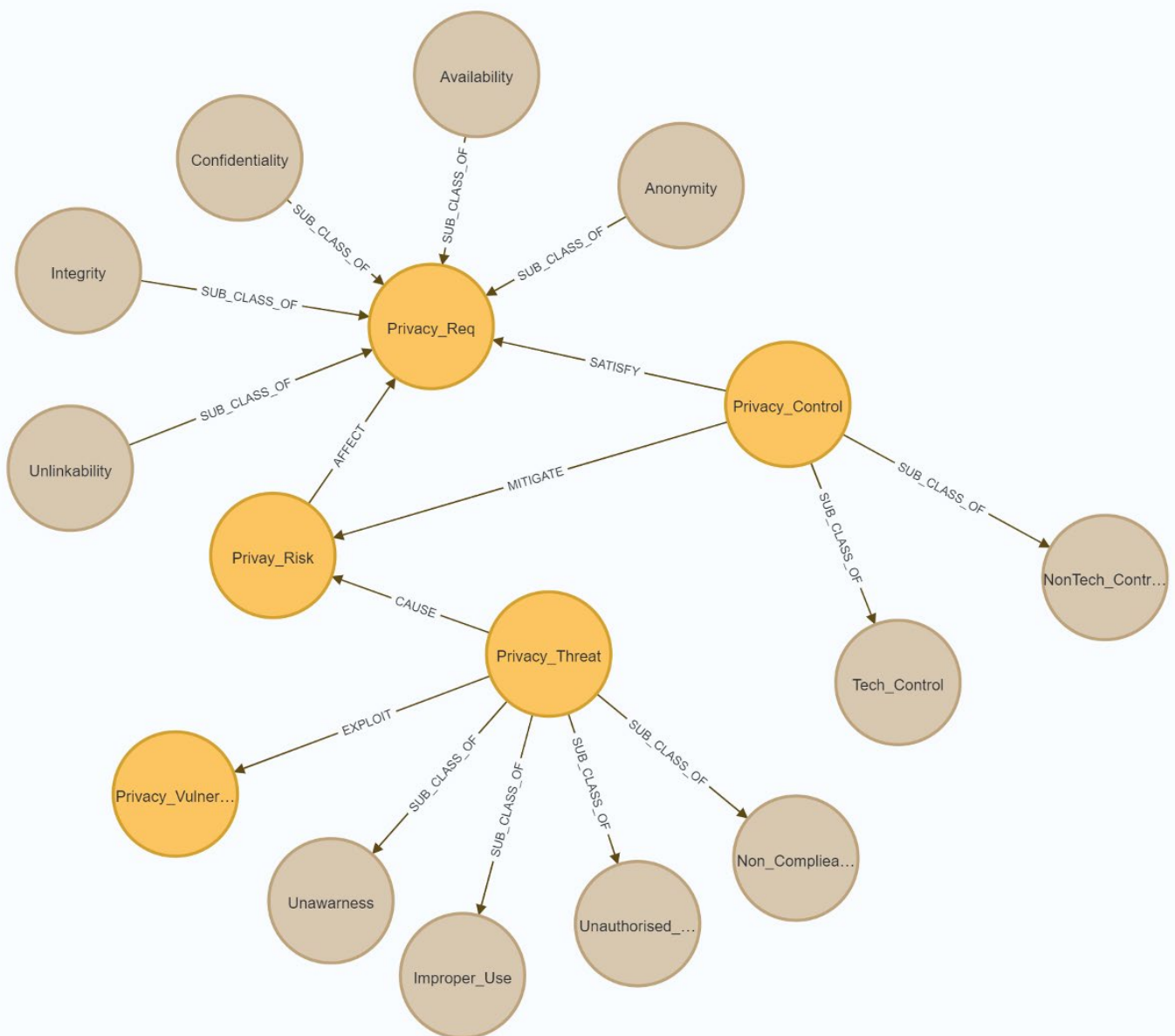


Figure 4.6 PR graph-based model



### 4.2.3 Increment 3 - integrated IJPRA ontology

The third increment includes the integration of the IJ and PR ontologies to develop the IJPRA ontology. The structure of the IJPRA ontology consists of three elements, namely concepts, relationship, and layers, as shown in Figure 4.7.

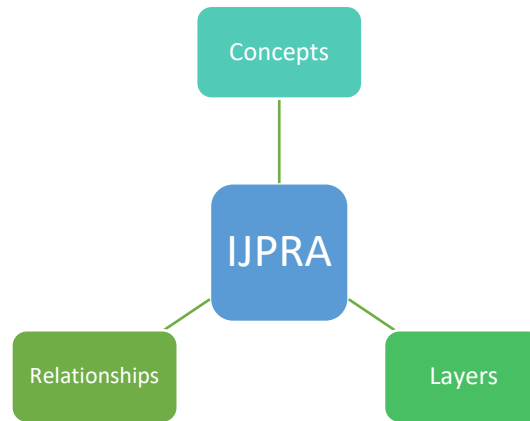


Figure 4.7 IJPRA ontology structure

A description of each element in the IJPRA ontology structure is provided below.

#### ***IJPRA emerged concepts***

The concepts that emerged for the integration of IJ and PR ontologies were captured based on the capture step in the adopted ontology development guidelines (Uchold & Grüninger 1996). The NIST 800-30 standard was used as a practical lens for integration because it offers a structured process to assess privacy risks (National Institute of Standard and Technology 2013). Consequently, a list of concepts and relationships was identified in this increment for integration purposes. The identified concepts are listed in Table 4.7. The definitions of these concepts (see Table 4.7) were inferred from the practical lens used mentioned above.

Table 4.7 Emerged concepts for integrating IJ and PR ontologies and their definitions.

Label	Concept	Definition	Ref
C1	PrivacyRiskAssess	Represents the process of identifying and assessing privacy risks associated with passenger information in the smart airport.	(National Institute of Standard and Technology 2013)
C2	SeverityLvl	Represents the level of potential impact on passengers and their information due to the occurrence of privacy risks.	(National Institute of Standard and Technology 2013)
C3	Impact	Represents the potential damage to passengers and their information due to the occurrence of privacy risks.	(National Institute of Standard and Technology 2013)
C4	LikelihoodLvl	Represents the probability of the passenger personal information being disclosed	(National Institute of Standard and Technology 2013)

Following the identification of the concepts for integration purposes, these concepts were mapped to the concepts in the UFO, as presented in Table 4.8.

Table 4.8 Mapping IJPRA emerged concepts with UFO concepts

UFO concepts	IJPRA emerged concepts
Action	PrivacyRiskAssess
Event	Impact
Phase	SeverityLvl, LikelihoodLvl

### ***IJPRA emerged relationships***

To integrate the IJ ontology with the PR ontology, seven relationships emerged as a part of capture step in the guidelines of ontology development (Uschold & Grüninger 1996) and by adapting The NIST 800-30 standard was used as a practical lens for integration because it offers a structured process to assess privacy risks (National Institute of Standard and Technology 2013). These relationships connected the IJ and PR ontologies concepts with the IJPRA emerged concepts (presented in Table 4.7). Table 4.9 presents the emerged concepts for integration purpose.

Table 4.9 IJPRA – emerged relationships for integration purposes

Concept 1	Emerg ed relationship for integration purposes	Concept 2
“PrivacyRiskAssess”	IDENTIFY	“Passenger_Information”, “Privacy_Risk”, “Privacy_Control”, “Privacy_Requirement”
“PrivacyRiskAssess”	ASSESS	“likelihoodLvl”, “severityLvl”
“Ppassenger_Information”	HASVUL	“Privacy_Vulnerability”
“Privacy_Threat”	THREATEN	“Ppersonal_Information”
“Impact”	IMPACT	“Individual/ Passenger”, “Passenger_Information”
“Privacy_Threat”	RESULT_IN	“Impact”
“Factor”	INFLUNCE	“PrivacyRiskAssess”

As shown in Table 4.9, the relationship "IDENTIFY" was established to represent the connection between the privacy risk assessment concept and “Ppersonal\_Information” (main asset), “Privacy\_Risk,” “Privacy\_Requirement,” and “Privacy\_Control” concepts. Another relationship called "ASSESS" was established to represent the connection between the “PrivacyRiskAssess” concept and "SeverityLvl" and "LikelihoodLvl”, indicating that the severity and likelihood levels were assessed to determine the level of the identified risk. The relationship “THREATEN” was established to connect the concept “Privacy\_Threat” in the PR ontology with the concept “Ppersonal\_Information”, indicating that a privacy threat threatens

passenger personal information handled during the journey, while the relationship “IMPACT” was established to show the “Impact” of the privacy risk on the passenger and their information. Another relationship, called “HASVAL,” was established between the concept “Passenger\_Information” in the IJ ontology and the “Privacy\_Vulnerability” concept in the PR ontology, indicating that passenger information is vulnerable to privacy threats. The relationship “INFLUENCE” represents the connection between “PrivacyRiskAssess”, “PasInterJourney”, and “Factor” concepts, referring to the risk assessment processes and passenger interaction journey, which are influenced by the legal factors relevant to privacy. The last established relationship is “RESULT\_IN,” representing the relationship between the “Privacy\_Threat” concept in the PR ontology and the emerged concept of “Impact” indicating that the identified risk results in an impact to passengers and their information. Figure 4.8 presents the IJPRA relationships sub-matrix that includes the emerged relationships for integration purpose, highlighted in yellow colour, along with their relevant concepts. The full matrix of IJPRA ontology concepts\_relationships is accessible via this link [IJPRA concept-relationships matrix \(full\)](#).

	Individual/ Passenger	Passenger_ Information	Ppersonal_ Information	Privacy_Risk	Privacy Vulnerability	Privacy_Requirement	Privacy_Control	PrivacyRiskAssess	SeverityLvl	Impact	LikelihoodLvl
Passenger_Information			BASE_CLASS_OF		HASVUL			IDENTIFIED_BY			
Information_Flow			HANDLE								
Factor								INFLUENCE			
Privacy_Regulation											
Privacy_Standard											
Privacy_Risk						AFFECT	MITIGATED_BY	IDENTIFIES_BY			
Privacy_Threat			THREATEN	CAUSE	EXPLOIT					RESULT_IN	
Privacy_Vulnerability											
Unauthorized_Access											
Improper_Use											
Non_Compliance											
Unawareness											
Privacy_Requirement				AFFECTED_BY			SATISFIED_BY	IDENTIFIED_BY			
Confidentiality						SUB_CLASS_OF					
Integrity						SUB_CLASS_OF					
Availability						SUB_CLASS_OF					
Unlinkability						SUB_CLASS_OF					
Anonymity						SUB_CLASS_OF					
Privacy_Control				MITIGATE		SATISFY		IDENTIFIED_BY			
Tech_Control							SUB_CLASS_OF				
NonTech_Control							SUB_CLASS_OF				
PrivacyRiskAssess		IDENTIFY		IDENTIFY		IDENTIFY	IDENTIFY		ASSESS		ASSESS
SeverityLvl								ASSESSED_BY			
Impact	IMPACT	IMPACT									
LikelihoodLvl								ASSESSED_BY			

Figure 4.8 IJPRA concepts- relationships matrix

### ***IJPRA layers***

After integrating the concepts from the IJ and PR ontologies and identifying the concepts needed for integration to develop the IJPRA ontology, these concepts are organised into metamodel layers (M2, M1, and M0), as shown in Figure 4.9. As illustrated in Figure 4.9, the M2 layer includes top-level concepts that are independent, more general, and have a broad domain scope (Henderson-Sellers 2012). The concepts in layer M2 include the actor, technology, process, passenger information, facility, journey, factor, and privacy risk. Then, the concepts in M2 are broken down into concepts in the M1 layer that are more specific and dependent on the M2 layer. The concepts in the M1 layer provide more detailed information and are essential for a deeper understanding of the domain (Henderson-Sellers 2012). The M0 layer includes concepts that provide detailed instances of concepts from the M1 layer (Henderson-Sellers 2012).

According to the implementation step in the guidelines for ontology development that were adopted from (Uschold & Grüninger 1996), the integrated IJPRA ontology is represented using a graph-modelling approach (Pokorný 2016). As presented in Figure 4.10, in the graph-modelling approach, concepts in the IJPRA ontology are represented as labelled nodes, whereas labelled edges represent the relationships of the IJPRA ontology (Pokorný 2016). The blue nodes refer to IJ ontology, the yellow nodes present PR ontology, and the red nodes show the concepts for integrated IJPRA ontology development. As shown in Figure 4.10, The Neo4j graph database (Pokorný 2015) is utilised as a tool to implement the IJPRA graph model. Figure 4.10 presents the IJPRA graph-based model using Neo4j. Zoom in to view Figure 4.10 at a larger size.

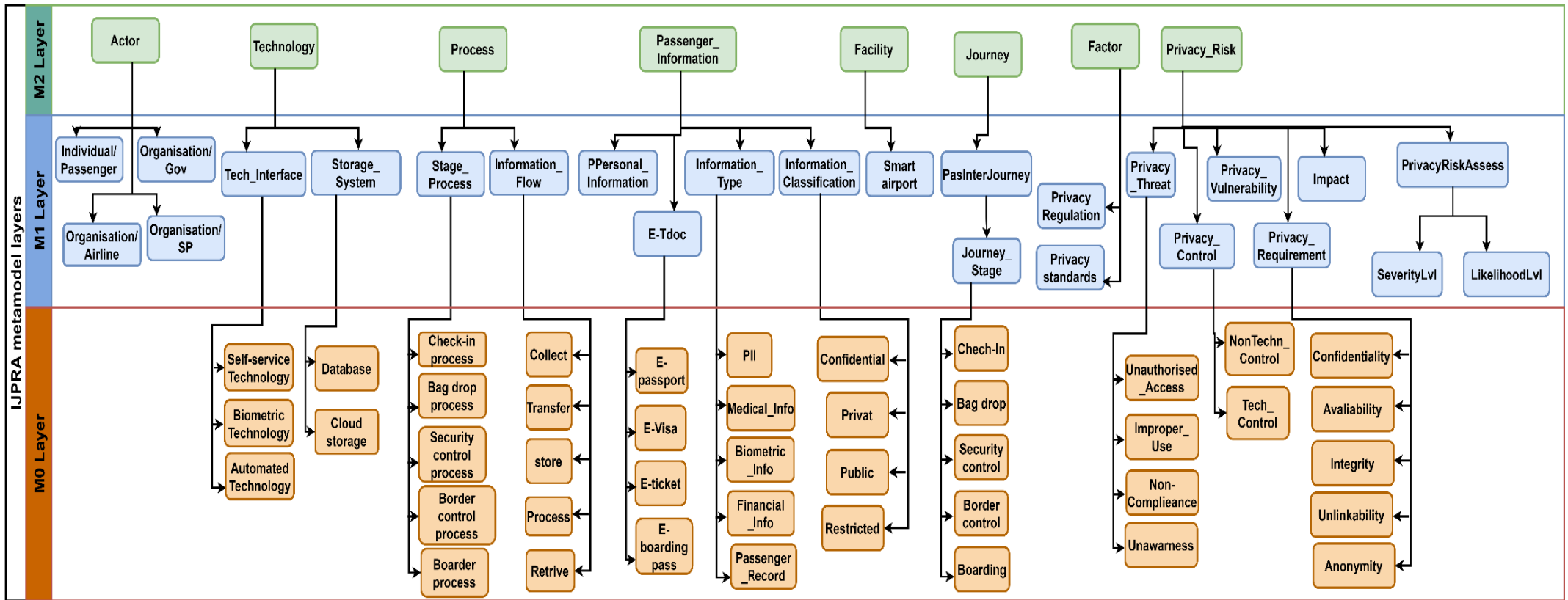


Figure 4.9 Organising the IJPRa concepts into metamodel layers (M2, M1, M0)

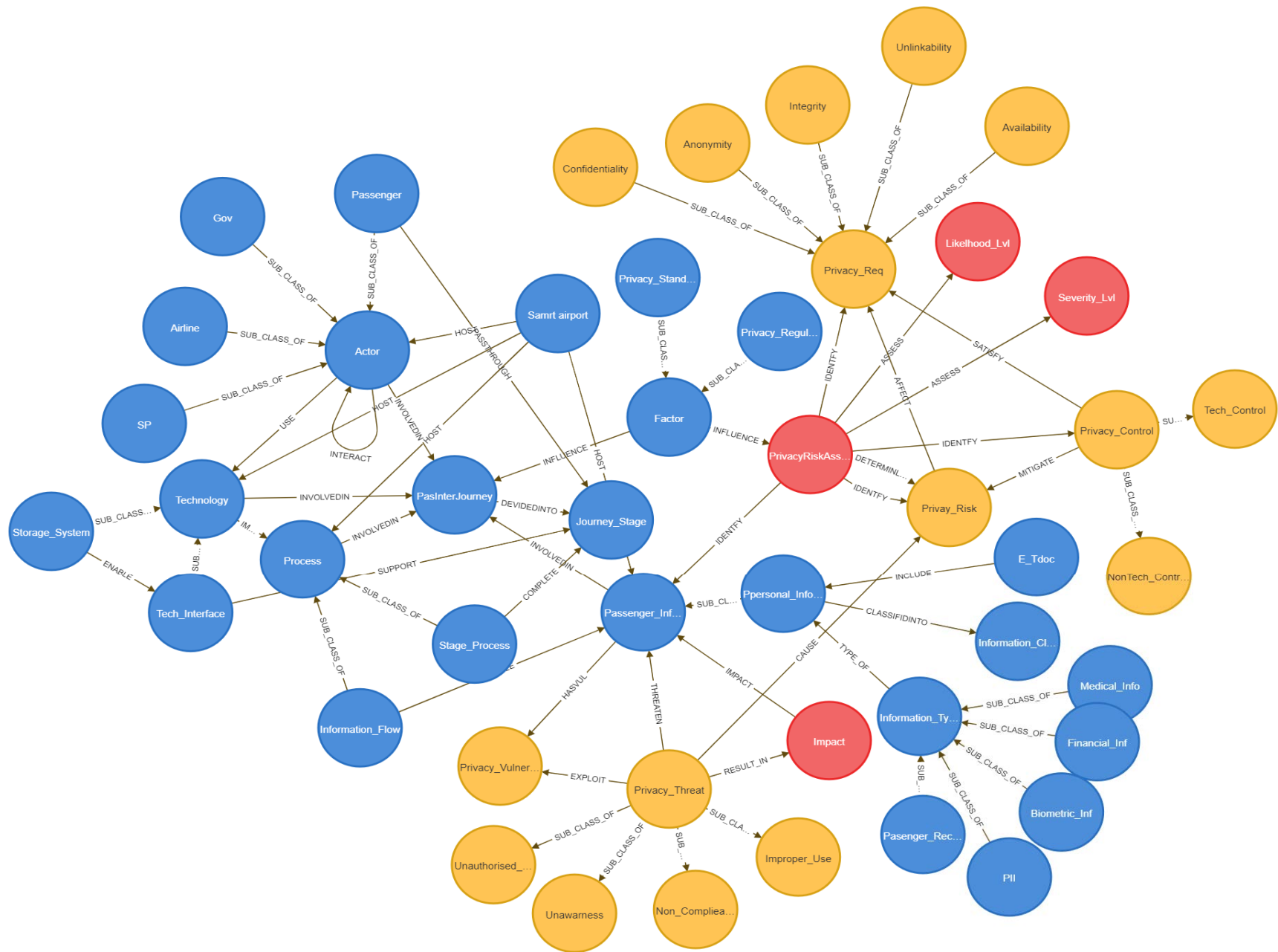


Figure 4.10 IJPRA graph-based model

As shown in Figure 4.10, the passenger interaction journey in the IJPRA ontology illustrates who and what is involved in the journey. The passenger interaction journey is divided into several stages, as represented by the “Journey\_Stage” concept. The actor represents people interacting during the passenger journey, including organisations and individuals. Organisations encompass airlines, government agencies, and service providers who offer various services to passengers during their journey, whereas individuals refer to passengers who benefit from these services in the context of a smart airport. The technology refers to the technologies used by the passenger to implement the processes. It includes technological interfaces and a digital infrastructure; hence, this research focuses on storage systems as a type of digital infrastructure. Technological interfaces include biometric, self-service, and automated technologies, whereas storage systems include databases and cloud storage that enable the technological interfaces. The process comprises two major processes: the stage process and the information flow. These processes represent how passengers complete their journey stages, including handling passenger information during their journey. The passenger information includes e-travel documents and personal information of different types (represented by the “Information\_Type” concept, and classifications (described by the “Information\_Classification” concept). Various types of passenger personal information, such as PII, biometric information, passenger records, medical information, and financial information, are handled during the journey in smart airports. These types of information are classified based on their sensitivity level into private, confidential, and restricted. Additional classifications can also be used. It is important to mention that this research focuses on passenger personal information – non-personal information is beyond the scope of this research. The smart airport represents the facility that hosts actors, technology, processes, and information. The IJPRA ontology was designed to understand, identify, and assess the privacy risks associated with passenger personal information in smart airports. The risk assessment process starts by identifying privacy risks, controls, and requirements related to the passenger information asset. Thus, the privacy risk caused by privacy threats. There are different types of privacy threats, such as unauthorised access, unauthorised use, non-compliance, and unawareness. A privacy threat may exploit vulnerabilities in information handling. Privacy control represents several technical and non-technical controls to mitigate the identified privacy risks and satisfy the privacy requirements. The privacy requirements include obligation arising from privacy law and other sources to meet passenger privacy needs. The identified privacy requirements are confidentiality, availability, integration,



unlikability, and anonymity. These requirements are affected by the identified privacy risk. The identification process was followed by assessing the likelihood and severity levels to measure the overall risk level. This will help appropriate decisions to be made and appropriate controls to be chosen to mitigate the identified risk. Hence, the scope of this research is limited to risk identification and risk analysis under the privacy risk assessment process, and risk mitigation process is out of the scope of this research. The factor concept represents privacy-related regulations and standards, relevant to the aviation industry, influencing passenger journeys and the privacy risk assessment process.

### 4.3 The IJPRA architecture

The IJPRA architecture is designed based on the concepts of IJPRA ontology (see Section 4.2). According to Ameller & Franch (2011); Gill (2022), architectural models can be designed utilising ontology, which encompasses capturing concepts and their corresponding relationships. Figure 4.11 presents the conceptual view of IJPRA architecture gamma version as far as the scope of this research is concerned. As shown in Figure 4.11, the IJPRA architecture involves two main layers: the IJ layer and the PR layer, both of which are influenced by the legal factors representing privacy law relevant to aviation industry. The information about each layer in the IJPRA architecture gamma version is defined using the IJPRA ontology concepts in layers M2, and M1(see Figure 4.9). The definitions of these concepts are presented in Tables 4.3,4.4, and 4.7.

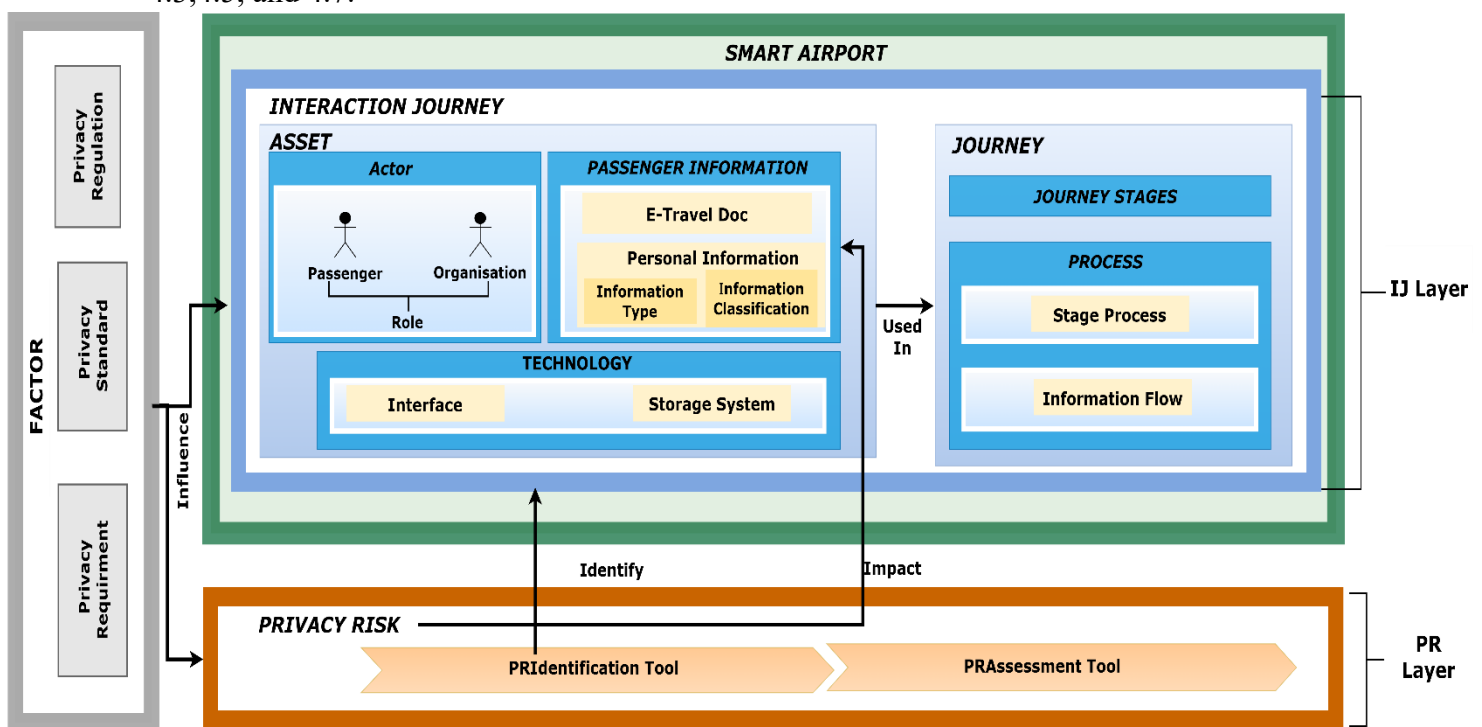


Figure 4.11 IJPRA architecture conceptual view

The IJPRA architecture development went through two increments (Table 4.1) to develop the IJ layer in increment 4, and the PR layer, based on the activities in increment 5. Details on the development of each layer are given below.

#### 4.3.1 Increment 4- IJ layer

The IJ layer is the first layer in the IJPRA architecture and was developed to provide the architecture of the passenger interaction journey in a smart airport to address **RQ2: How to design the passenger interaction journey architecture in a smart airport?** (see Chapter 1 Section 1.3). The IJ layer was designed and organised based on AEA (Gill 2022), and CJM (Rosenbaum, Otalora & Ramírez 2017) (see Table 4.2) as theoretical lenses. This layer consists of two components: assets and journeys, as shown in Figure 4.11. The asset component involves actors, technology and information. The actors and technology interact to handle passenger information during the journey. The journey component represents the main stages of the passenger travel journey as well as the process of the main activities undertaken to complete the journey stages and handle passenger information. The IJ layer is influenced by privacy laws relevant to the aviation industry. The IJ layer was further organised into five views: IJ-Actor, IJ-technology, IJ-Process, IJ-Information, and IJ-Factor views. These views aim to represent and provide details about the asset, journey components in the IJ layer, and privacy laws that influence the handling of passenger information during the interaction journey. This helps in better understanding who and what are involved in the journey. This understanding enables the identification of privacy risks arising during the journey and the development of effective privacy solutions. The IJ layer focuses on the passenger interaction journey in the check-in, bag drop, security control, border control, and boarding stages on the departure side, primarily emphasising the digital handling of passenger personal information. The passenger interaction journey on the in-flight and arrival side, and other information, such as flight information or the non-digital handling of passenger information, is beyond the scope of this research, as discussed in the research limitations.

##### ***IJ- Actor view***

The IJ-Actor view aims to represent the details of actors: individuals and organisations involved and interacting at each stage of the journey as per their role. The IJPRA ontology concepts used to design the IJ-actor view are Actor, Individual/Passenger, Organisation/SP, Organisation/Airline, Organisation/Gov, PasInterJourney, and Journey\_Stage (Table 4.10). The definitions of these concepts are presented in Table 4.3.

Table 4.10 IJPRA ontology concepts used to design the IJ-Actor view

IJ layer views	Relevant ontology concepts
IJ-Actor view	Actor, Individual/Passenger, Organisation/SP, Organisation/Airline, Organisation/Gov, PasInterJourney, and Journey_Stage.

Figure 4.12 presents the IJ-Actor view representing journey stages, who are involved and interacting based on their roles at each stage of the passenger journey. As shown in Figure 4.12, the passenger interaction journey is divided into the following journey stages: check-in, bag drop, security control, border control, and boarding. Throughout each stage, passengers interact with various organisations according to their roles in handling passenger information and providing services specific to that stage. For instance, during the check-in, bag drop, and boarding stages, passengers interact with airline companies and provide the required passenger information to complete these stages, whereas during the security control and border control stages, passengers interact with government agencies for the same purposes. It is crucial to emphasise the significant role of service providers in all passenger stages. These providers play a vital role by offering the necessary services to facilitate the operations of other actors involved in each stage. The actor view facilitates a holistic understanding of the actors involved and interacting in the passenger journey.

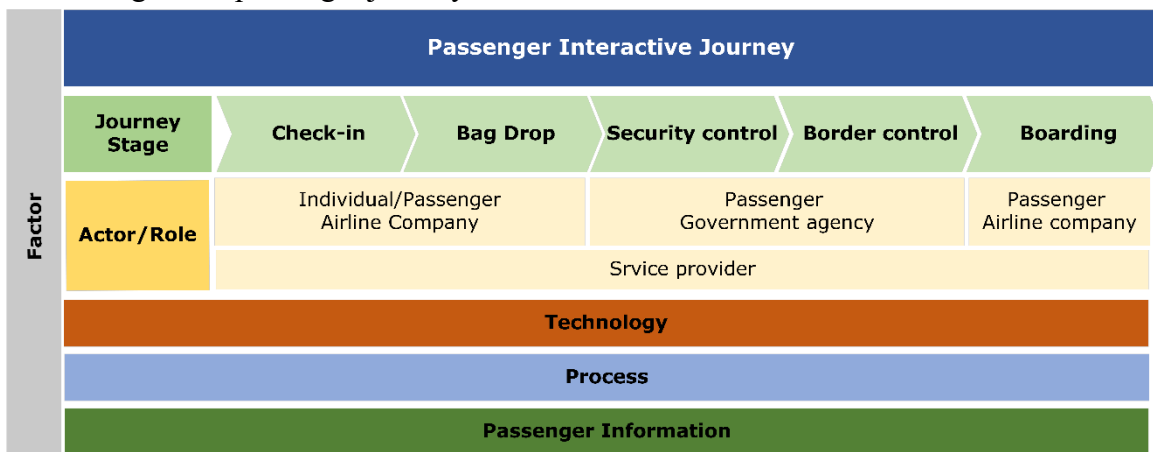


Figure 4.12 IJ-Actor view

### ***IJ-Technology view***

The IJ-Technology view aims to represent the detailed level of technologies, including technological interface and storage systems, involved in each stage of the journey, with a specific emphasis on handling passenger personal information. The IJPRA ontology concepts used to design IJ-Technology view are Actor, PasInterJourney, Journey\_Stage, Technology, Tech\_Interface, and Storage\_System, process, Passenger\_Information, and Factors (Table 4.11). The definitions of these concepts are presented in Table 4.3.

Table 4.11 IJPR ontology concepts used to design the IJ-Technology view

IJ layer views	Relevant ontology concepts
IJ-Technology view	Actor, PasInterJourney, Journey_Stage, Technology, Tech_Interface, and Storage_System, process, Passenger_Information, and Factors

Figure 4.13 presents the IJ-technology in a manner that shows the details of the technology involved in the passenger interaction journey. In smart airports, the passenger interaction journey is divided into several stages that are supported by several interfaces, such as self-service technologies, automated technologies, and biometric technologies, that enable passengers to interact with the system at each stage of the journey. It also facilitates the collection and processing of passenger information, allowing them to provide the necessary details required at each stage. The information collected by these interfaces is transferred between the relevant systems and actors in the smart airport. Integration between airline systems, airports, and government databases allows for streamlined information transfer that may occur in real-time or at a predetermined time, depending on the specific requirements at each stage of the journey. The passenger information is then stored in storage systems, including cloud-based storage and databases, relevant to airlines, airports, or government agencies. Finally, this information is delivered as needed to optimise and enhance the passenger travel experience.

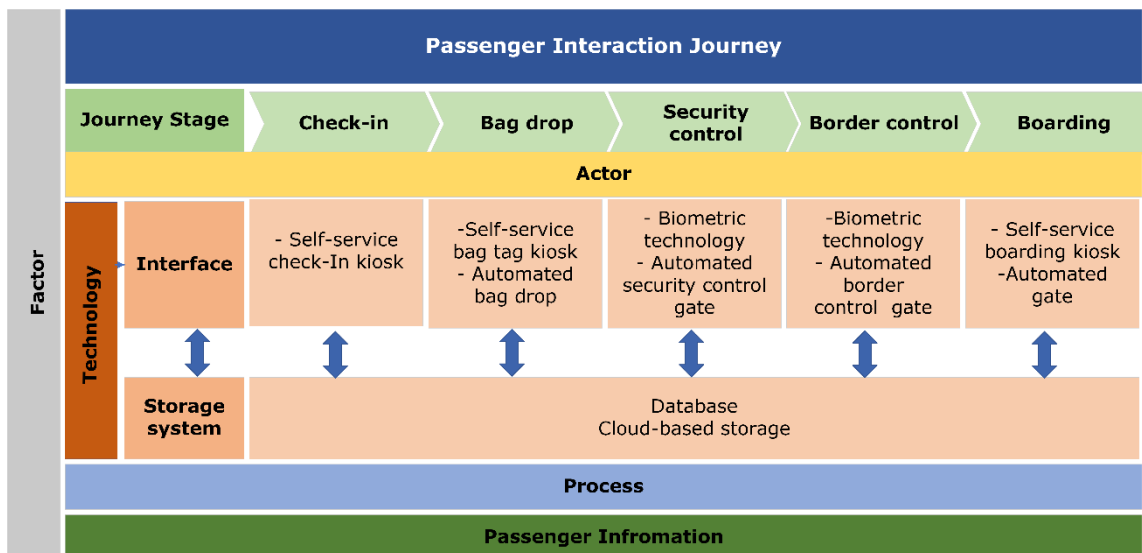


Figure 4.13 IJ-Technology view

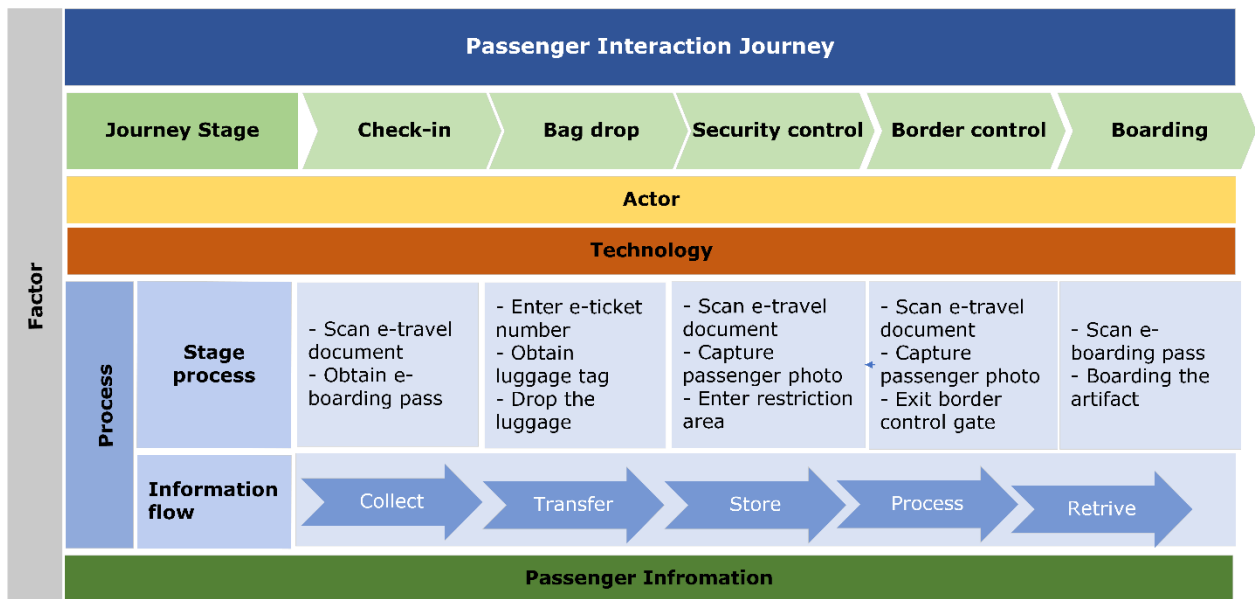
***IJ- Process view***

The IJ-Process view aims to give a detailed view of the processes (activities), including stage processes and information flow, that occur at each stage of the passenger journey. The IJPRA ontology concepts used to design the IJ-process view are Actor, PasInterJourney, Journey\_Stage, Technology, Process, Stage\_Process, Information\_Flow, Passenger\_Information, and Factor (Table 4.12). The definitions of these concepts are presented in Table 4.3.

*Table 4.12 IJPRA ontology concepts used to design IJ-Process view*

IJ layer views	Relevant ontology concepts
IJ-Process view	Actor, PasInterJourney, Journey_Stage, Technology, Process, Stage_Process, Information_Flow, Passenger_Information, and Factor

Figure 4.14 presents the IJ-Process view, showing the details of the processes involved in the passenger interaction journey. The IJ-process view plays a key role in depicting the interaction between actors and technologies to complete the journey stages and handle passenger information by defining the activities in each journey stage.



*Figure 4.14 IJ-Process view*

As shown in Figure 4.14, the stage process involves a series of activities that passenger perform to complete the stages of their journey. On the other hand, the information flow shows the handling of passenger information activities, such as collecting, transferring, storing, processing, and retrieving in each journey stage. It is important to mention that actors interact with technologies (discussed in the IJ-Technology view) to handle passenger information.

Understanding the processes performed in each stage of the journey enables a better understanding of the information flow activities. This understanding helps identify the

associated privacy risks that may impact passenger information during their interaction journey. Table 4.13 outlines the processes for each journey stage along with the corresponding activities. Understanding the processes performed in each stage of the journey enables a better understanding of the information flow process, the other type of process in the passenger interactive journey.

Table 4.13 Process stages and its activities

Journey Stage	Process Stage	Activities
Check-in	Check-in process	Scan e-travel document. Verify scanned e-documents. Obtain e-boarding pass.
Bag drop	Bag drop process	Enter e-ticket number. Obtain luggage tag. Drop the luggage.
Security control	Security control process	Scan e-travel document. Capture passenger photo. Enter restricted area in smart airport.
Border control	Border control process	Scan e-travel document. Capture passenger photo. Exit border control e-gate.
Boarding	Boarding process	Scan e-boarding pass. Board the aircraft.

### ***IJ-Information view***

The IJ-information view aims to show the detail of passenger information that is handled throughout each stage of the journey. The IJPRA ontology concepts used to design the IJ-information view are Actor, PasInterJourney, Journey\_Stage, Technology, Process, Passenger\_Information, E\_Tdoc, Ppersonal\_Information, Information\_Type, PII, Medical-Info, Biometric\_Info, Financial\_Info, and Passenger\_Record, Information\_Classification, and Factor (Table 4.14). The definitions of these concepts are presented in Table 4.3.

Table 4.14 IJPRA ontology concepts used to design the IJ-Information view

IJ layer views	Relevant ontology concepts
IJ-Information view	Actor, PasInterJourney, Journey_Stage, Technology, Process, Passenger_Information, E_Tdoc, Ppersonal_Information, Information_Type, PII, Medical-Info, Biometric_Info, Financial_Info, and Passenger_Record, Information_Classification, and Factor

Figure 4.15 shows the IJ-information view that presents the detailed level of passenger information involved in the passenger interaction journey. This view helps provide a comprehensive understanding of passenger information, including the use of e-travel documents along with the types of passenger personal information involved and its classification based on its sensitivity level.

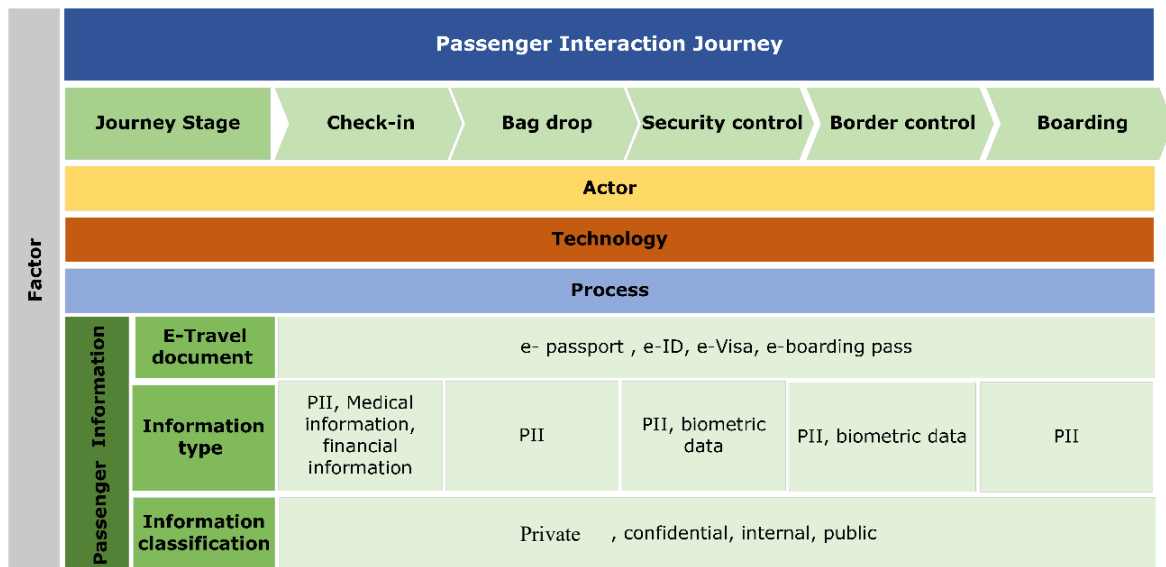


Figure 4.15 IJ-Information view

As shown in Figure 4.15, the e-travel documents include the e-passport, e-ID, e-boarding pass, and e-visa which are utilised by passengers. These documents embed several types of passenger personal information. Depending on the specific stage process (see IJ-Process view) and the technologies (see IJ-Technology view) that support this stage, a passenger may be required to use their e- travel document or provide their personal information. In this case, the personal information encompasses several information types, such as PII, medical information, financial information, and biometric information. Passenger personal information is classified based on its sensitivity level into private, confidential, internal, or public. This classification ensures that appropriate security measures and privacy controls are applied to each category of information.

***IJ-Factor view***

In the IJPRA architecture, the legal factor is an influencing factor that plays a key role in both the IJ layer and PR layer. These factors influence and guide the interaction journey, the use and handling of passenger information during their journey, and privacy risk assessment, as shown in Figure 4.11. These factors includes several privacy laws, such as privacy regulations and standards, as well as privacy requirements (as shown in Figure 4.16). Actor, Technology, Process, Passenger\_Information, Factor, Privacy\_Regulation, Privacy\_Standard, Privacy\_Requirement, PasInterJourney, Journey\_Stage are the IJPRA concepts that are used to design this view (Table 4.15). The definitions of these concepts are presented in Tables 4.3 and 4.5.

Table 4.15 IJPRA ontology concepts used to design the IJ-Factor view

IJ layer views	Relevant ontology concepts
IJ-Factor view	Actor, Technology, Process, Passenger_Information, Factor, Privacy_Regulation, Privacy_Standard, Privacy_Requirement, PasInterJourney, Journey_Stage

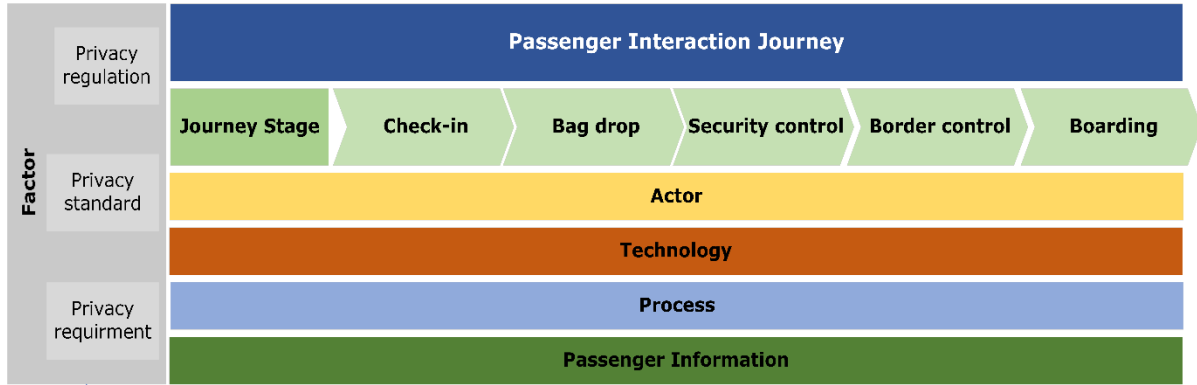


Figure 4.16 IJ-Factor view

By considering the factor view in the architecture, organisations in smart airport including airlines, government agencies, and service providers can align their processes and technologies with the relevant privacy regulations, standards, and requirements. This ensures compliance with privacy legal requirements, promotes data privacy and security, and enhances overall passenger experience. This research focuses on understanding the legal factors that influence the interaction journey, aiming to offer a comprehensive perspective on how privacy-related legal factors guide the overall passenger experience. Details about these factors, such as specifying the privacy regulations and standards and how they influence the interaction journey, are out of the scope of this research, as discussed in the research limitations.

#### 4.3.2 Increment 5 - PR layer

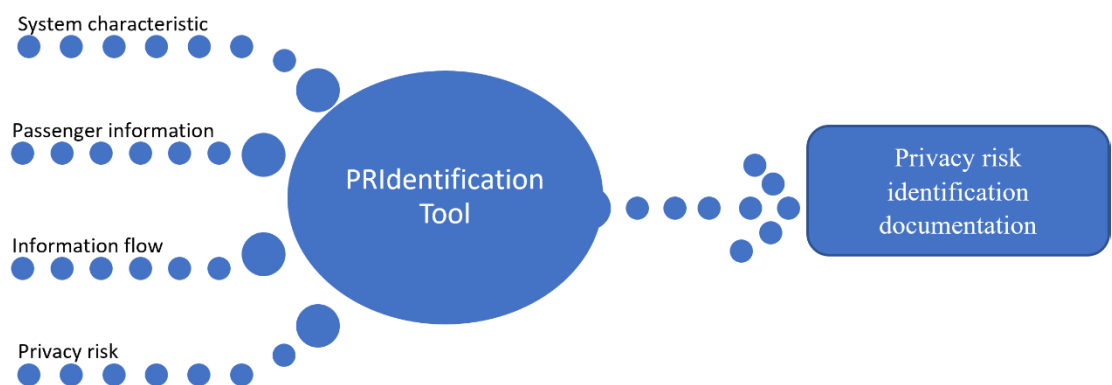
To assess the privacy risks associated with passenger personal information in smart airports, a layer called “Privacy Risk” is introduced in the IJPRA architecture, as shown in Figure 4.11. Privacy\_Threat, Privacy\_Vulnerability, Privacy\_Control, Privacy\_Requirement, Unauthorised\_Access, Improper\_Use, Non-compliance, Unawareness, Confidentiality, Integrity, Availability, Anonymity, Unlinkability, PrivacyRiskAssess, SeverityLvl, LikelihoodLvl, and Impact concepts in the IJPRA ontology are used to design this layer. The definitions of these concepts are presented in Tables 4.5 and 4.7 (see Sections 4.2.2 and 4.2.3). The PR layer in the IJPRA architecture addresses **RQ3: How to assist in the assessment of privacy risks associated with passenger’s information during their interaction journey in a smart airport?** (see Chapter 1). The PR layer can involve different aspects, including (**PR**Identification) and (**PR**Assessment) tools (presented in Figure 4.11), that guide the



identification and assessment of the privacy risks associated with passenger information in the smart airport. The scope of the privacy risk layer is limited to identifying and assessing the privacy risk. However, risk mitigation and compliance analysis are out of the scope of this research, as discussed in the research limitations and future works. The description of each tool in the PR layer is given below.

***Privacy risk identification (PRIdentification) tool***

The privacy risk identification (PRIdentification) tool has been developed to assist in identifying and documenting the privacy risks associated with passenger information in smart airport. This research focuses on privacy risks impact the passenger personal information. Also, in this thesis, privacy risk is defined as the probability of the passenger personal information being disclosed and resulting in impact to the passenger and their information in the smart airport (Xu et al. 2011). The comprehensive privacy threat analysis framework discussed by (Deng et al. 2011) and CFIP (Smith, Milberg & Burke 1996) used as theoretical lens for the PRIdentification tool development. In addition, the NIST standards, specifically NIST 800-30 (National Institute of Standard and Technology 2013) and the NIST Privacy Framework (National Institute of Standard and Technology 2020) , are used as a practical lens to guide the tool development. The description of these theoretical and practical lenses are presented in Table 4.2. The reason for using the mentioned theoretical and practical lenses is that they provide a systematic and structured approach to identify the privacy threats and vulnerabilities, privacy requirements, and current existing privacy controls as the main elements of privacy risk identification. Figure 4.17 presents the input and output of the **PRIdentification** tool.



*Figure 4.17 Input and Output of PRIdentification tool*

The input consists of four elements. The initial three elements are system characteristics, information flow, and passenger information. These elements represent the initial phase of risk identification, defining actors and technologies that interact to handle passenger information. These elements further demonstrate the information flow activities and passenger personal information types.

These elements are described and discussed in the IJ layer (see Section 4.3.1). The fourth element of the input is the privacy risk, which is discussed and identified under the PR layer. As shown in Figure 4.17, the output of this tool is the privacy risk identification documentation, which offers a comprehensive record of the identification results.

In order to identify privacy risks, a risk identification process is proposed as illustrated in Figure 4.18. The identification process was designed based on relevant concepts in IJPRA ontology, as shown in Table 4.16. Accordingly, the identification process involves identifying privacy threats, vulnerabilities, privacy requirements, and existing privacy controls.

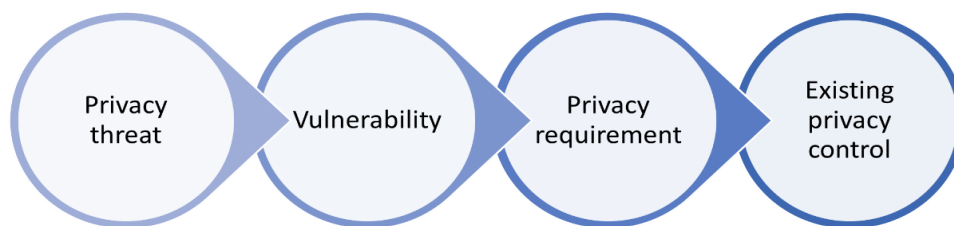


Figure 4.18 Process of privacy risk identification

Table 4.16 includes the description of the privacy risk identification step in PRIdentification tool along with relevant concepts from the IJPRA ontology used in identification step. These concepts are defined in Tables 4.3, 4.5, and 4.7.

Table 4.16 Description of privacy risk identification step

Identification step	Description	IJPRA ontology concepts (defined in Tables 4.3,4.5,4.7)
Privacy threat identification	Privacy threat identification aims to identify the privacy threats by systematically going over the passenger information flow at each stage of the journey to determine which privacy threats are posed. The privacy threats are identified using a list of applicability questions presented in Table 4.17	Privacy_Threat, Privacy_Vulnerability, Privacy_Control, Privacy_Requirement, Unauthorised_Access, Improper_Use, Non-compliance, Unawareness, Confidentiality, Integrity, Availability,

Identification step	Description	IJPRA ontology concepts (defined in Tables 4.3,4.5,4.7)
Privacy vulnerability identification	Vulnerability identification includes identifying a list of vulnerabilities that might be exploited by the identified threat.	Anonymity, Unlinkability, Actor, Technology, Process, Information_Flow, Factor
Privacy requirements identification	Privacy requirements identification includes identifying a list of privacy requirements derived from relevant privacy laws to meet passenger privacy needs.	
Privacy Control identification	Privacy control identification provides a list of existing privacy controls to satisfy the identified privacy requirements.	

A list of applicability questions adopted from the LUDDING GO toolkit proposed by (Wuyts, Sion & Joosen 2020) is provided to help identify several types of privacy threats that may arise during the passenger interaction journey and cause a privacy risk, impacting the privacy of passengers and their information in smart airports. In addition, these applicability questions assist in identifying the privacy requirements that may be affected by the identified privacy threats. Table 4.17 presents applicability questions along with the corresponding privacy threats and some of the affected privacy requirements.

*Table 4.17 Applicability Questions*

Applicability questions	Yes	No	Privacy threat types	Privacy requirements
Does passenger data transferred from self-service systems to actors' (airline, government agencies) storage system contain identity information?			Unauthorised use, unauthorised access, data misuse	Confidentiality, integrity, availability, anonymity, unlikability
Are passenger records sufficiently unique to distinguish them?			Unauthorised use, unauthorised access, data misuse	Confidentiality, integrity, availability, anonymity, unlikability
Is information collected using several self-service technologies or shared among actors able to reveal passenger personal information?			Unauthorised use, unauthorised access, data misuse threats	Confidentiality, integrity, availability, anonymity, unlikability
Is passenger information handled during the journey more sensitive than necessary?			Unauthorised use, unauthorised access, data misuse, non-compliance threats	Confidentiality, integrity, availability, anonymity, unlikability

<b>Applicability questions</b>	<b>Yes</b>	<b>No</b>	<b>Privacy threat types</b>	<b>Privacy requirements</b>
Is the amount of collected passenger information necessary?			Non-compliance threats	Confidentiality, integrity, availability, anonymity, unlikability
Is passenger information stored in storage systems longer than necessary?			Non-compliance threats, Unauthorised use, unauthorised access, data misuse threats	Confidentiality, integrity, availability, anonymity, unlikability
Is the passenger information necessary to share with other actors during journey?			Non-compliance threats, Unauthorised use, unauthorised access, data misuse threats	Confidentiality, integrity, availability, anonymity, unlikability
Is the passenger sufficiently aware of what personal information is being handled at each stage of their journey, for what purposes, in what manner, and how?			Non-compliance, unawareness threats	Confidentiality, integrity, availability, anonymity, unlikability
Does the passenger lack access to their personal information being handled or the ability to correct or delete their stored personal information?			Non-compliance and unawareness threats	Confidentiality, integrity, availability, anonymity, unlikability
Is the consent freely given, informed, specific, unambiguous, and can it be withdrawn and demonstrated by the passenger?			Non-compliance threats	Confidentiality, integrity, availability, anonymity, unlikability
Does the handling of passenger personal information rely on valid, appropriate, lawful grounds for a specific purpose?			Non-compliance threats	Confidentiality, integrity, availability, anonymity, unlikability
Is there a process in place to manage security and security risks and determine the necessary countermeasures, and does the system have appropriate countermeasures in place to secure the handling of passenger personal information?			Non-compliance threats	Confidentiality, integrity, availability, anonymity, unlikability

### **Privacy risk assessment (PRAssessment) tool**

To assess the privacy risk associated with passenger personal information at each stage of the journey, a privacy risk assessment tool (PRAssessment) is proposed. This tool helps assess the overall risk level. The risk-based framework discussed by Iguchi, Uematsu & Fujii (2018) is adopted as a theoretical lens to develop the PRAssessment tool. The reason for adopting this framework in developing the PRAssessment tool is that the assessment approach provides a simple, systematic, and structured method for conducting privacy risk assessments. In this thesis, the privacy risk is defined as the probability of the passenger personal information being disclosed and resulting in harm to the passenger and their information in the smart airport context (Xu et al. 2011). As shown in Figure 4.19, the input of the **PRAssessment** tool is the privacy risk documentation, resulting from **PRIdentification** tool, and the output is the overall risk level matrix.

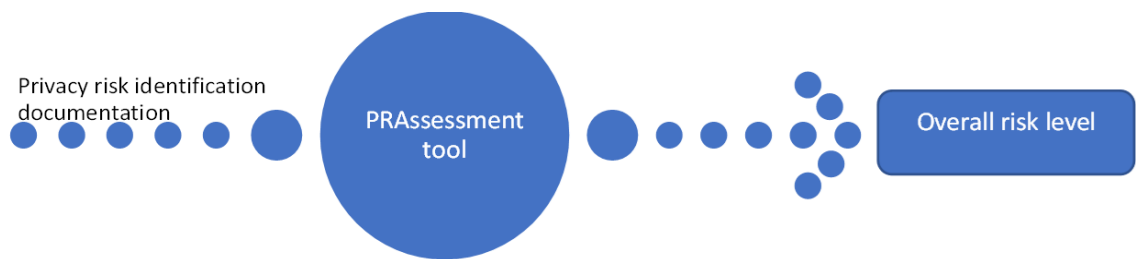


Figure 4.19 Input and output of PRAssessment tool

The process in the PRAssessment tool proposed is based on the adopted theoretical lens (Iguchi, Uematsu & Fujii 2018) and consists of: (1) Assess Severity level, (2) Assess Likelihood level, (3) Assess overall level, as shown in Figure 4.20.

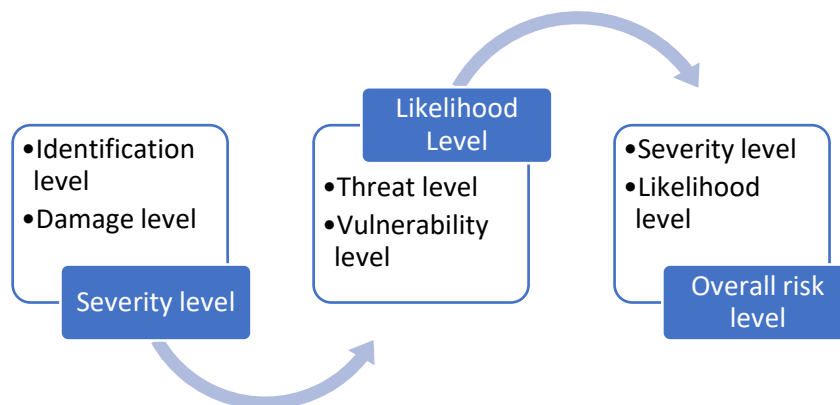


Figure 4.20 Process of privacy risk assessment

The description of the process of the risk assessment under PRAssessment tool and the relevant concepts in the IJPRA ontology used in each step of the process is presented in Table 4.18

Table 4.18 Description of privacy risk assessment process

Step	Description	IJPRA ontology (defined in Tables 4.3,4.5,4.7)
Assessment of severity level	The severity level indicates the potential harm that would occur if the handled passenger personal information is disclosed (see Table 4.7). It is scored as low, medium, or high based on the combination of the identification level and impact level (Iguchi, Uematsu & Fujii 2018). The identification level evaluates the difficulty of re-identifying the passenger based on their handled information, and its score can be low, medium, and high. The damage level evaluates the extent of damage, including physical, material, and moral damage occurring due to the disclosure of passenger information. Its score is also categorised as low, medium, or high. Detailed descriptions of the assessment levels for each assessment are provided in Table 4.19.	PrivacyRiskAssess SeverityLvl Impact Passenger, Passenger_Information, E_Tdoc, Ppersonal_Information, Information_Type, PII, Medical-Info, Biometric_Info, Financial_Info, and Passenger_Record
Assessment of likelihood level	The likelihood level indicates the probability of handled passenger personal information being disclosed (see Table 4.7). The likelihood level is determined by the combination of the threat level and vulnerability level (Iguchi, Uematsu & Fujii 2018). The level score categorised into low, medium, and high. The threat level evaluates the probability of threat source, either internal or external, disclosing passenger information handled during their journey by considering the source motivation, its trustworthiness, and the number of people that the handled information disclosed to. On the other hand, the vulnerability level indicates the weakness of handled passenger information during the journey by considering the privacy controls implemented to secure the information.	Privacy_Threat, Privacy_Vulnerability, PrivacyRiskAssess Privacy_Control LikelihoodLvl, Passenger_Information, E_Tdoc, Ppersonal_Information, Information_Type, PII, Medical-Info, Biometric_Info, Financial_Info, and Passenger_Record
Assessment of overall risk level	The overall risk level is evaluated based on the combination of severity level and likelihood level. The levels are Low, Medium, and High (Iguchi, Uematsu & Fujii 2018).	PrivacyRiskAssess SeverityLvl LikelihoodLvl, Privacy_Risk

To guide the assessment, the description of the assessment levels, either low, medium, or high, of severity, likelihood, and overall risk, is presented in Table 4.19. The description is adopted from (Iguchi, Uematsu & Fujii 2018).

Table 4.19 Description of the assessment level of each assessment component

Assessment component	Assessment level		
Severity level= Identification level * Damage level	Low	Medium	High
Identification level	It is impossible to identify passenger based on their information handled during the journey by the identified threat	It is not impossible to identify passenger based on their information handled during the journey by the identified threat	It is easy to identify passenger based on their information handled during the journey by the identified threat
Damage level	Passenger may encounter little damage that affects them, and their information caused by the identified threat.	Passenger may encounter medium damage that affects them, and their information caused by the identified threat.	Passenger may encounter significant damage that affects them, and their information caused by the identified threat
Likelihood level= Threat level* Vulnerability level	Low	Medium	High
Threat level	Chance of threat source attempting to disclose the handled passenger personal information is low.	Chance of threat source attempting to disclose the handled passenger personal information is medium	Chance of threat source attempting to disclose the handled passenger personal information is high.
Vulnerability level	The current privacy controls are insufficient to secure the handled passenger information.	The current privacy controls are working but need to be improved to secure the handled passenger information.	The current privacy controls are sufficient to secure the handled passenger information.
Overall risk level= severity level * likelihood level	Low	Medium	High
Overall risk level	Privacy risk is low, and no action will be taken.	Privacy risk is acceptable, and it might need to be reduced to low.	Privacy risk is critical, and it needs to be mitigated.

#### 4.4 Summary

The main contribution of the present research has been outlined in this chapter. The proposed IJAPRA framework introduced in this chapter offers a practical solution to the research

questions identified in Chapter 1. The proposed IJAPRA framework was developed using the well-known DSR methodology discussed in Chapter 3. This chapter presented an overview of the proposed IJAPRA framework and its components. These components comprise the IJPRA ontology and the IJPRA architecture. In addition, this chapter it discussed the incremental development of the gamma version of the IJAPRA framework. The adopted theoretical and practical lenses in framework development is explained in this chapter. The evaluation of the IJAPRA framework is discussed in the next chapter (Chapter 5).



## 5 Chapter 5: The IJAPRA framework evaluation

This chapter discusses the integrated development and evaluation of the alpha and beta versions of the framework. It also explains the evaluation results that led to the development of the gamma version of the IJAPRA framework (as discussed in Chapter 4). As discussed in Chapter 4, the IJAPRA framework involves two components: IJPRA ontology and IJPRA architecture. The evaluation is conducted using two DSR evaluation methods: the illustrative scenarios and expert evaluation via a field survey. First, this chapter discusses the illustrative scenarios to demonstrate the applicability of the IJPRA ontology, which is the first component of the IJAPRA framework, in capturing domain knowledge. The results of the illustrative scenarios evaluation resulted in the alpha version of the IJAPRA framework being developed to the beta version of the IJAPRA framework. Second, this chapter details the results of the expert evaluation via a field survey conducted with experts in the information privacy/security and data protection fields. The expert evaluation method was employed to evaluate the IJPRA architecture, which is the second component of the IJAPRA framework. The survey data were analysed for the final evaluation of the IJAPRA framework. The generalisability, applicability, usefulness, and understandability of the IJAPRA framework are evaluated based on the feedback collected from the field survey, then the gamma version of the IJAPRA framework is developed based on the field survey results (as discussed in Chapter 4).

### 5.1 The IJAPRA framework evaluation overview

As discussed in Chapter 4, the IJAPRA framework consists of two components that were developed in five increments. The first component of the IJAPRA framework is the IJPRA ontology, which was developed to represent the knowledge of the domain, and the second component is the IJPRA architecture. The IJPRA architecture includes two layers, the IJ and PR layers, which were designed based on the IJPRA ontology. The IJPRA ontology was developed in three increments (see Section 4.2, Chapter 4), comprising the following activities: (1) IJ ontology development, (2) PR ontology development, and (3) integrated IJPRA ontology development. On the other hand, the IJPRA architecture was developed in the remaining two increments: (4) development of the IJ layer, and (2) PR layer development (as discussed in Section 4.3, Chapter 4). A conceptual view of the IJAPRA framework is shown in Figure 4.1 in Chapter 4.

This section presents the evaluation of the IJAPRA framework through three iterations using two evaluation methods to determine whether it meets the evaluation criteria presented in Table

3.2 in Chapter 3. The evaluation methods are illustrative scenarios, and expert evaluation via field survey. Each iteration results in an updated version of the IJAPRA framework: alpha, beta, and gamma, based on the evaluation results. The gamma version is the final version of the IJAPRA framework, as discussed in Chapter 4. A description of the evaluation iterations and the version of the IJAPRA resulting from each iteration is presented in Figure 5.1.

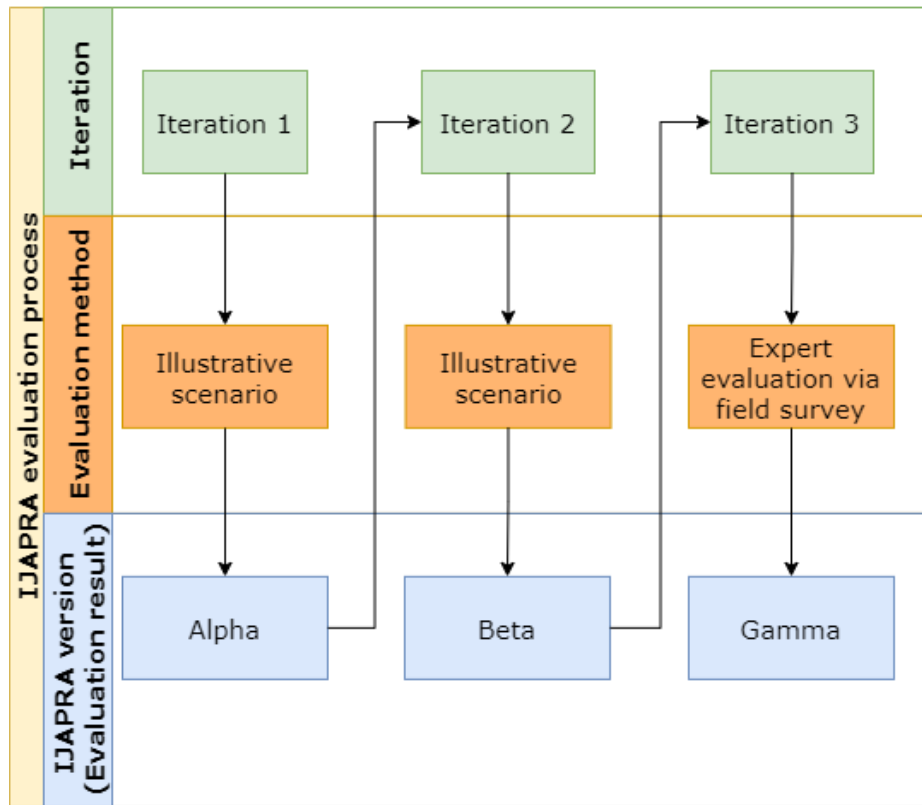


Figure 5.1 IJAPRA evaluation iterations and methods

As shown in Figure 5.1, the evaluation was performed over three iterations.

### 5.1.1 Iteration 1

Iteration 1 (Section 5.2) discusses the development of the alpha version of the IJAPRA framework. The development of the alpha version of the IJAPRA framework went through 5 increments (as illustrated in Chapter 4, Table 4.1). In this iteration, the alpha IJPRA ontology was partially evaluated using an illustrative scenario. This was performed to evaluate the alpha version of the IJ ontology, which was developed in the first increment of the IJAPRA framework development. The goal was to measure its applicability in capturing knowledge about passenger journey in a smart airport. The evaluation result in this iteration led to the development of the beta version of the IJ ontology. Although the framework was partially evaluated in this iteration, it was still considered alpha, as shown in Figure 5.1.

### 5.1.2 Iteration 2

In iteration 2, as outlined in Section 5.3, the alpha version of the IJPRA ontology, which resulted in iteration 1, was evaluated. Five illustrative scenarios were used to evaluate its applicability in capturing the knowledge of the domain of passenger information and the associated privacy risks in the smart airport. This evaluation iteration led to further improvements, resulting in the beta version of the IJAPRA framework, including IJPRA ontology and IJPRA architecture. The framework update is denoted as the beta version in Figure 5.1.

### 5.1.3 Iteration 3

In iteration 3 (see Section 5.5), the beta version of the IJPRA architecture, which is the second component of the IJAPRA framework, was evaluated using an expert evaluation method via a field survey. The survey was distributed via LinkedIn and email to 230 experts to obtain their opinions and feedback on the beta version of the framework. The participants were selected based on their experience in the field of information privacy/security and data protection, with a minimum of three years of experience. Of the 230 distributed surveys, 35 were completed. The responses from these 35 participants were included in the data analysis for the evaluation. The expert feedback was used to improve the IJAPRA framework. The resulting final version is referred to as the gamma version in Figure 5.1. Furthermore, the experts' suggestions were used to identify the scope for future work. The gamma version of the IJAPRA framework is discussed in Chapter 4.

Table 5.1 presents a summary of these iterations, highlighting the evaluation methods applied in each, the specific framework component being evaluated, and the resulting version of the framework based on the evaluation results.

*Table 5.1 Summary of evaluation iterations methods and results*

<b>Iteration</b>	<b>Evaluation method</b>	<b>Framework evaluated component</b>	<b>Resulting framework version</b>	<b>Source</b>
1	1 illustrative scenario	IJ ontology (alpha version)	IJAPRA framework (alpha version), including IJPRA ontology and IJPRA architecture	Section 5.2
2	5 illustrative scenarios	IJPRA ontology (alpha version)	IJAPRA framework (beat version), including IJPRA ontology and IJPRA architecture	Section 5.3
3	Field survey	IJPRA architecture (beta version)	IJAPRA framework (gamma version), including IJPRA ontology and IJPRA architecture	Section 5.5. Chapter 4

Details of each evaluation iteration are discussed in the following sections.

## 5.2 Iteration 1- IJAPRA framework alpha version

As discussed in Chapter 4, the IJAPRA framework is incrementally developed through the stages of DSR and consists of two main components: IJPRA ontology and IJPRA architecture. The alpha version of the IJPRA framework was developed based on a comprehensive review of the studies in both academic and industrial fields (see Chapter 2) and pre-determined kernel theories, including frameworks and well-known standards that were adopted as theoretical and practical lenses (see Table 4.2 in Chapter 4). Details of the development of the alpha version the IJAPRA framework components and the evaluation performed in this iteration are discussed as follows.

### 5.2.1 The IJPRA ontology alpha version

The alpha IJPRA ontology, which is the first component of the IJAPRA framework, was developed in this iteration. The activities of each increment in framework development are discussed in Chapter 4 and Table 4.1.

#### ***Increment 1***

The alpha version of the IJ ontology was developed in the first increment of the IJAPRA framework. This version of IJ ontology included the identification of key concepts and relationships relevant to the passenger journey in the smart airport. These were identified based on existing studies, along with the AEA (Gill 2022) and CJM (Rosenbaum, Otalora & Ramírez 2017) frameworks as theoretical lenses. The description of the adopted AEA and CJM frameworks and how they were used in developing the IJ ontology are discussed in Chapter 4 (see Table 4.2). The identified concepts, sub-concepts, and their definitions for IJ ontology alpha version are presented in Table 5.2.

*Table 5.2 IJ ontology (alpha) concepts and their definitions*

<b>Concept</b>	<b>Definition</b>	<b>Ref</b>
Actor	Individual and organisation interact with each other as per their role in the smart airport.	(Gill 2022)
Individual/Passenger	An individual who benefits from services provided by several organisations in a smart airport.	New
Organisation/Airline	An airline company that offers air transport services to passengers.	(European Union Agency for Network and Information Security 2016)

Concept	Definition	Ref
Organisation/Gov	A government that operates security services for passengers at several stages of their journey.	(European Union Agency for Network and Information Security 2016)
Passenger_Information	Passenger data, in digital format, that is handled during the interaction journey in a smart airport.	(Gill 2021b)
Technology	Technological interface and digital infrastructure involved in the passenger interaction journey.	New
Tech_Interface	Interfaces, for example, self-service technology, automated technology, and biometric technology, used by actors to implement the processes during the passenger interaction journey.	(Gill 2022; Rajapaksha & Jayasuriya 2020)
Storage_System	A type of digital infrastructure that enables a technological interface in a smart airport. Examples of storage systems are databases and cloud-based storage.	New
Smart airport	A facility that hosts the elements involved and interacts in the passenger interaction journey.	(Gill 2022)
PasInterJourney	Elements involved and interacting during the passenger travel journey in a smart airport.	New
Journe_Stage	Several zones of the passenger travel journey in the smart airport.	(Willemsen & Cadee 2018)
Process	A set of activities during the passenger journey.	(Gill 2022)
Stage_Process	The activities to complete each stage of the passenger journey.	(Gill 2022; Rosenbaum, Otolara & Ramírez 2017)
Legal	Internal and external legal influences to guide the passenger journey and the use and handling of their information, such as privacy regulations, privacy standards, and privacy policies.	(Gill 2022)

The alpha version of IJ ontology was represented by graph-based modelling approach, as shown in Figure 5.2. The graph model is implemented with Neo4j (Figure 5.2).

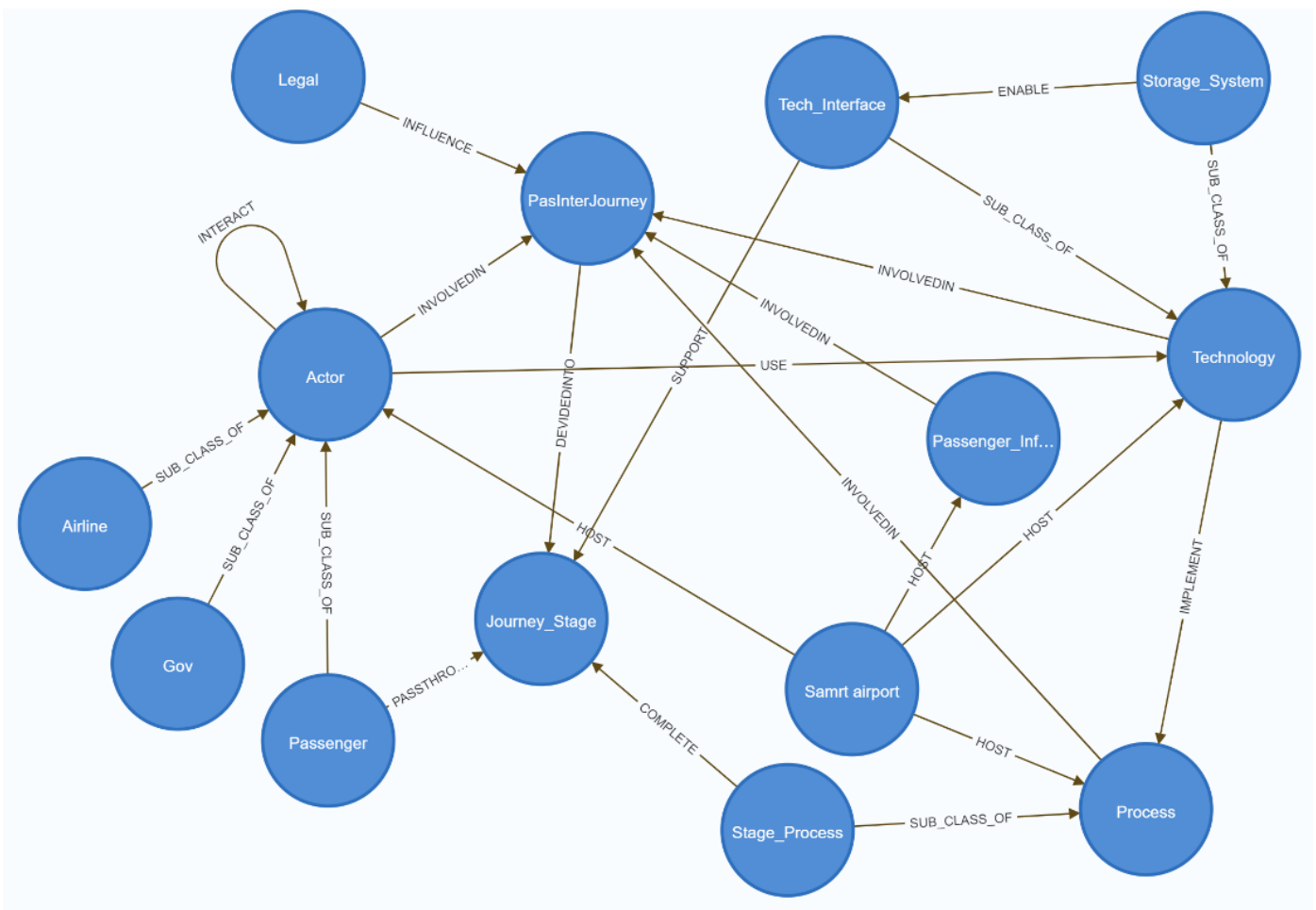


Figure 5.2 IJ graph-based model (alpha version)

The alpha version of the IJ ontology was evaluated using one illustrative scenario to test its applicability to capturing knowledge in the domain of passenger interaction journey in the smart airport. This means the ontology adequately covers the necessary concepts and relationships under the passenger journey in smart airports. The evaluation results will lead to refinement of the alpha version of the IJ ontology to the beta version. The following scenario is developed based on the proposed scenario documentation methodology (discussed in Section 3.5.4, Chapter 3)

**Scenario 1:** Adam’s vacation has just started, and finally, he can spend some time with his family. He has booked a flight from M to J. On the day of his flight, he arrives at PMAS airport and heads to Terminal 1, goes through the SA Airline's check-in procedure, uses a self-service kiosk, and enters the e-ticket number and his phone number to obtain his e-boarding pass. Adam’s personal identifiable information, including his phone number and e-ticket number, is extracted from the kiosk, and transferred to the airline’s system to obtain the service. In addition, it is stored in the airline’s data system as part of his passenger records. Adam’s

experience at the smart airport was comfortable and convenient, however, concerns about the privacy of his information that was handled to complete the check-in stage were raised.

The alpha version of the IJ ontology is applied to the above scenario. It is represented in IJ graph model, as shown in Figure 5.3. In Figure 5.3, the instances are represented by grey nodes and the relationship “INSTANCE\_OF” is used to specify the connection between concepts and their instance.

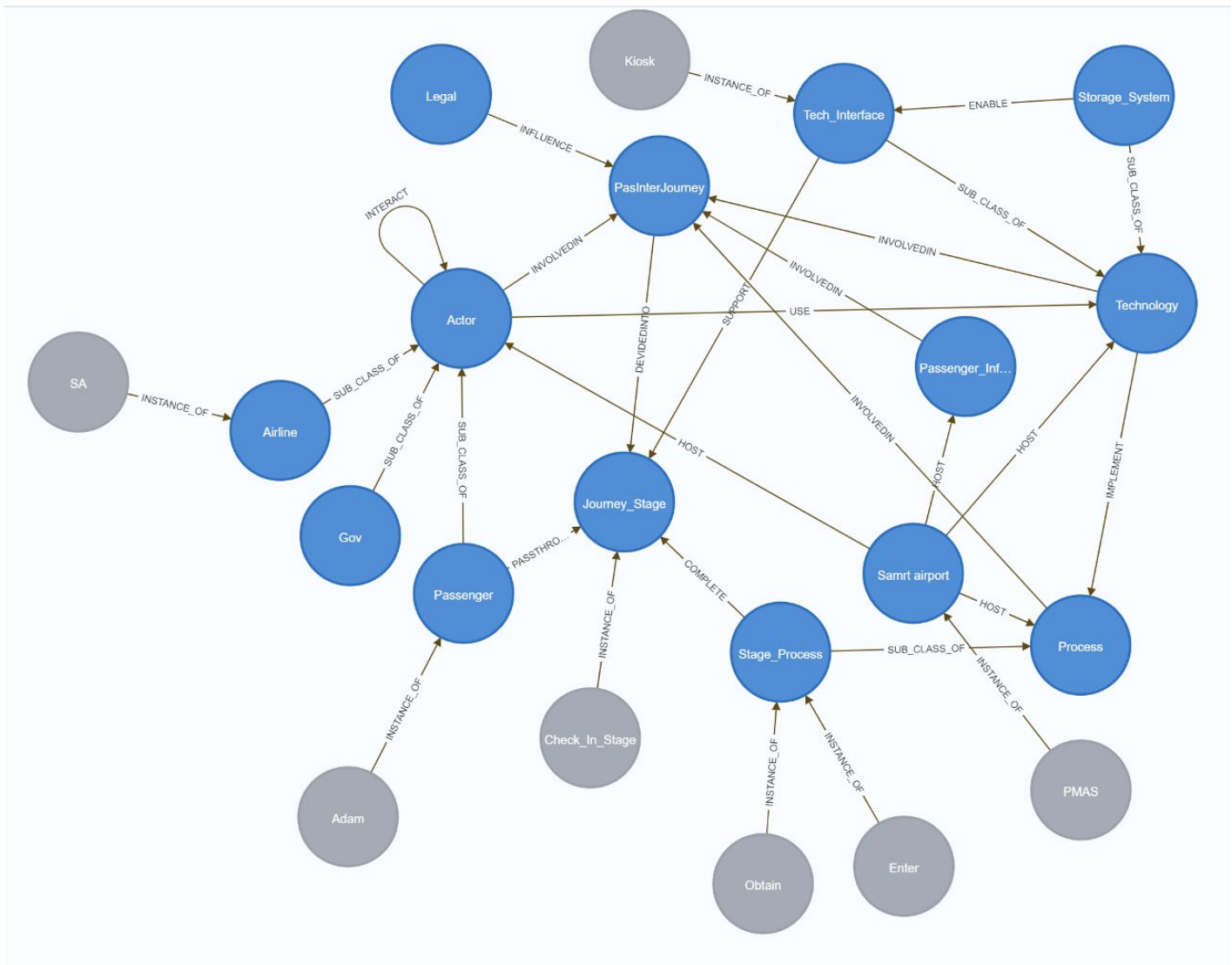


Figure 5.3 Scenario Implementation – iteration 1

**Results:** As shown in Figure 5.3, the alpha IJ ontology does not have concepts that represent the information handling process, the type of information mentioned in the scenario, or the type of e-travel document mentioned in the scenario.

To address these gaps, a new concept called “Information\_Flow” was introduced. Additionally, to represent specific types of passenger information during the journey, the "PII" concept was emerged. Another new concept, "E\_Tdoc", was incorporated to denote the e-travel document.



As a result, the alpha version of the IJ ontology was refined to the beta version that included the three emerged concepts. The concepts and their definitions are shown in Table 5.3. The refined IJ ontology based on the results of the scenario is presented using a graph-based modelling approach, as shown in Figure 5.4. This refined version is called beta. The concepts that emerged are represented in light purple nodes.

Table 5.3 Emerged concepts and their definitions based on scenario results

Emerged concept	Definition	Ref
Information_Flow	The process of handling passenger data during each stage of the journey.	(Gill 2022)
PII	Personally identifiable information, which is a type of passenger information that is linked to passenger directly or indirectly.	(Chuleeporn 2008; ISACA n.d.)
E_Tdoc	Numerous kinds of travel documents in their electronic versions such as e-passport, e-visa, e-boarding pass, e-ID, and e-ticket that include passenger information.	New

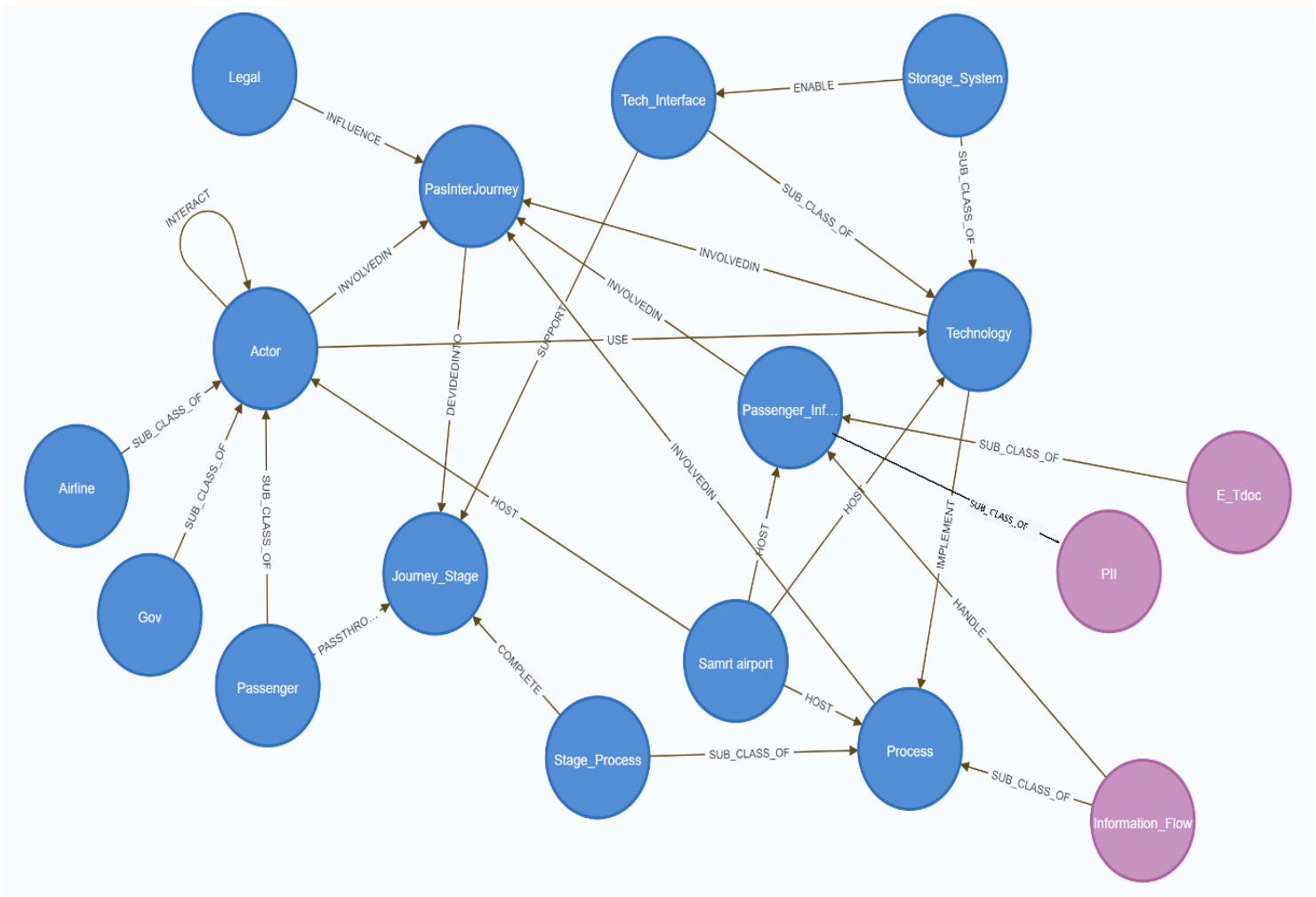


Figure 5.4 Scenario 1 results- iteration 1



## Increment 2

Following the development of the beta version of the IJ ontology, the alpha version of the PR ontology was developed. The development of alpha PR ontology drew from the review of the existing studies (see Chapter 2) and incorporated both theoretical and practical lenses. The theoretical lenses included the CFIP (Smith, Milberg & Burke 1996), and (2) and the privacy threat analysis framework (Deng et al. 2011). The practical lenses used were the NIST 800-30 standard (National Institute of Standard and Technology 2013) , and NIST privacy framework (National Institute of Standard and Technology 2020). The description of these lenses is provided in Chapter 4, Table 4.2. Table 5.4 presents the identified concepts and their definitions in the PR alpha version.

*Table 5.4 PR ontology (alpha) concepts and their definitions*

<b>Concept</b>	<b>Description</b>	<b>Ref</b>
Privacy_Risk	Probability of the passenger information being disclosed by a potential event and resulting in impact to passengers and their information in the smart airport context.	(National Institute of Standard and Technology 2013, 2020; Xu et al. 2011)
Privacy_Threat	Undesired potential events, either internal or external, that cause a privacy risk.	(National Institute of Standard and Technology 2013)
Unauthorised_Access	A type of access threat to passenger information by unauthorised people.	(Smith, Milberg & Burke 1996)
Improper_Use	A type of threat where stored information is modified and/or collected passenger information is used for other than an authorised purpose (secondary use), and/or sharing information with unauthorised parties.	(Smith, Milberg & Burke 1996)
Non-Compliance	A type of threat where the handling of passenger information in the smart airport context does not comply with privacy regulations.	(Deng et al. 2011; Smith, Milberg & Burke 1996)
Unawareness	A threat type where a passenger is unaware of the reasons why their information is being collected, what information is being collected and how their information is handled.	(Deng et al. 2011)
Privacy_Requirement	Obligations arise from law and other sources to meet passenger privacy needs to protect passenger information handled during their journey.	(National Institute of Standard and Technology 2013, 2020)
Confidentiality	A privacy requirement to maintain authorised constraints on accessing and	(National Institute of Standard and Technology 2013, 2020)

Concept	Description	Ref
	disclosing passenger information to protect their privacy.	
Integrity	A privacy requirement to prevent unauthorised changes and ensure the authenticity and non-repudiation of passenger information.	(National Institute of Standard and Technology 2013, 2020)
Availability	A privacy requirement to guarantee timely and dependable access to and the utilisation of passenger information.	(National Institute of Standard and Technology 2013, 2020)
Anonymity	A privacy requirement to ensure a passenger's identity is not identifiable by others.	(Deng et al. 2011; Pfitzmann & Hansen 2010)
Unlinkability	A privacy requirement to conceal the connection between two or more types of passenger information.	(Deng et al. 2011; Pfitzmann & Hansen 2010)
Privacy_Control	Safeguards to mitigate the privacy risk and satisfy the privacy requirements relevant to passenger information in the smart airport.	(National Institute of Standard and Technology 2020)
Tech_Control	A type of privacy control that includes security-based solutions.	(National Institute of Standard and Technology 2020)
NonTech_Control	A type of privacy control that includes administrative safeguards.	(National Institute of Standard and Technology 2020)
Privacy_Vulnerability	A weakness in handling passenger information that may be exploited by a privacy threat.	(National Institute of Standard and Technology 2013)

### ***Increment 3***

Increment 2 was followed by a third increment to integrate the IJ and PR ontologies to develop the alpha version of the IJPRA ontology. Table 5.4 shows the concepts for the development of the integrated IJPRA ontology alpha version. The NIST 800-30 standard was used as a practical lens for integration as it offers a structured process to assess the privacy risks (National Institute of Standard and Technology 2013).

The IJPRA ontology was represented using graph-based modelling approach, as shown in Figure 5.5. This version of the IJPRA ontology resulted from iteration 1 of the IJPRA framework evaluation. In Figure 5.5, IJ ontology concepts are represented by blue nodes, PR ontology concepts are yellow, and emerging concepts and emerging concepts for integration purposes are red.

Table 5.5 Emerged concepts for IJPRA ontology (alpha version)

<b>Concept</b>	<b>Definition</b>	<b>Ref</b>
<b>PrivacyRiskAssess</b>	The process of identifying and assessing the privacy risks associated with passenger information in the smart airport.	(National Institute of Standard and Technology 2013)
<b>SeverityLvl</b>	The level of potential impact on passengers and their information due to the occurrence of privacy risks.	(National Institute of Standard and Technology 2013)
<b>LikelihoodLvl</b>	The probability of passenger information being disclosed.	(National Institute of Standard and Technology 2013)

The figure of alpha version IJPRA is shown in the next page (Figure 5.5).

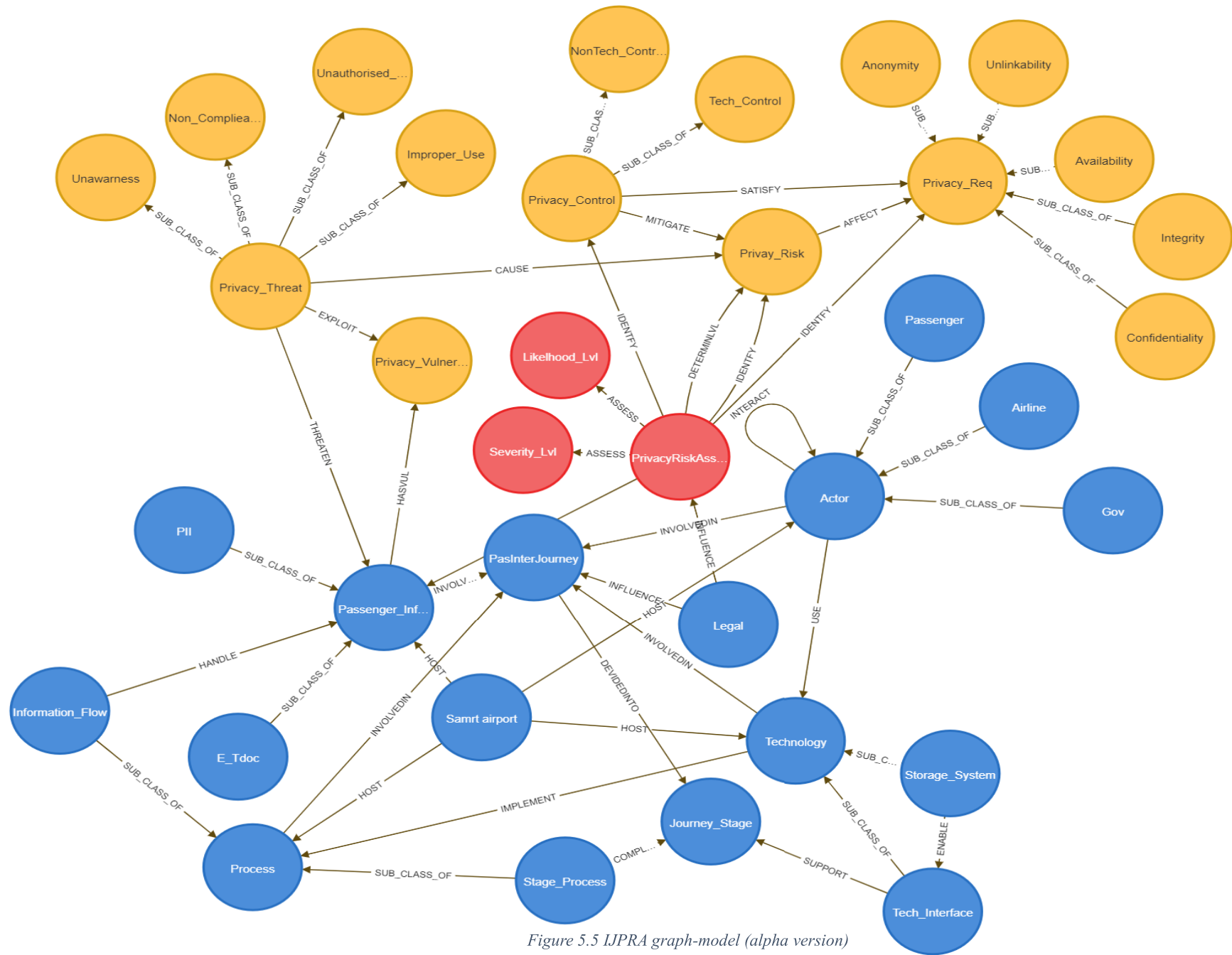


Figure 5.5 JPRA graph-model (alpha version)

### 5.2.2 The IJPRA architecture alpha version

In the alpha version of the IJPRA framework, the architecture had two layers, the IJ layer and the PR layer, as shown in Figure 5.6. The IJPRA architecture was developed in two increments, namely, increments 3 and 4, as previously discussed (see Chapter 4, Table 4.1).

#### ***Increment 4***

The IJ layer was designed using the AEA framework as a theoretical lens (described in Chapter 4, Table 4.2). Consequently, this layer encompasses five fundamental concepts: actor, technology, process, information, and Legal (Figure 5.6). These concepts were defined based on the theoretical lens used (see Table 5.1).

#### ***Increment 5***

The second layer, PR, was introduced in increment 5. This layer contains two concepts: Risk Identification and Risk Analysis (Figure 5.6), which represent the process of the privacy risk assessment.

Figure 5.6 shows the alpha version of IJPRA architecture. Due to the limited scope of the alpha version of the IJPRA architecture, it included only the layers and their relevant foundation concepts. However, this version of the architecture laid the groundwork for further development and refinement in the second evaluation iteration.

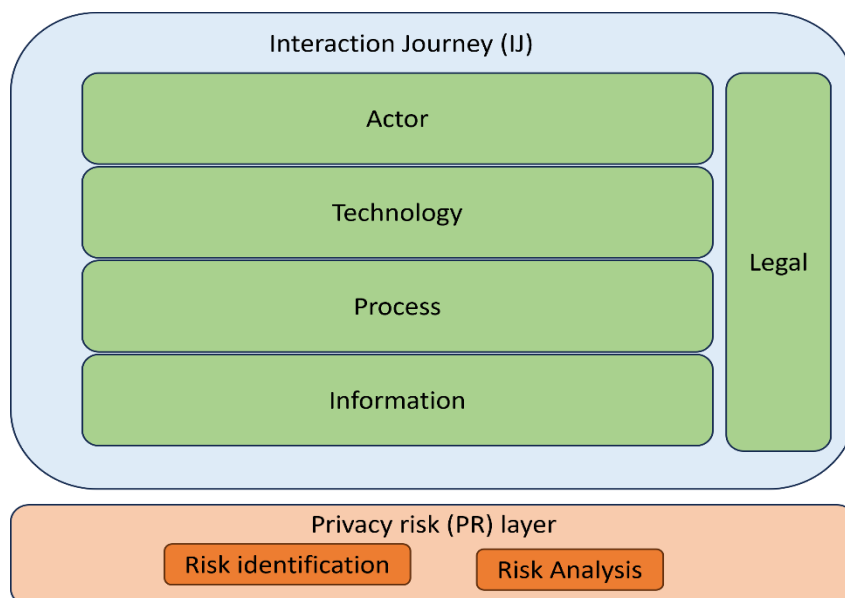


Figure 5.6 IJPRA architecture (alpha version)

The next section discusses iteration 2 of the IJPRA framework evaluation process that led to the development of the IJPRA framework beta version.

### 5.3 Iteration 2- IJAPRA framework beta version

In iteration 2, the alpha version of the IJAPRA ontology was evaluated. The evaluation results led to the beta version of the IJAPRA framework components, including the IJAPRA ontology and IJAPRA architecture. The details are discussed below.

#### 5.3.1 IJAPRA ontology beta version

The alpha version of the IJAPRA ontology was evaluated using the illustrative scenario evaluation method to demonstrate its applicability in describing and representing the domain within the scope of this research (See Chapter 3, Table 3.2). A set of hypothetical privacy risk analysis and assessment scenarios were developed following the proposed scenario documentation methodology (see Figure 3.6, Chapter 3). Table 5.6 displays the steps of the scenario development, along with the activities associated with each step.

*Table 5.6 Scenario development process*

Scenario development steps	Activities
Step 1: Identify scenario elements	The scenario elements, including passenger persona types, were identified, and a fictitious case study was developed to describe the smart airport environment.
Step 2: Analyse existing relevant scenarios	A review of the existing scenarios in privacy risk analysis and assessment, and smart airports in both academic and industry fields was conducted to develop scenarios relevant to this research (Alghanim, Rahman & Hossain 2017; Cano et al. 2016; European Network and Information Security Agency (ENISA) 2010; European Union Agency for Network and Information Security 2016; Kalakou, Psaraki-Kalouptsidi & Moura 2015; Labati et al. 2016; Lykou, Anagnostopoulou & Gritzalis 2019; Williams et al. 2016)
Step 3: Create suitable scenarios.	Five hypothetical scenarios were developed to simulate the smart airport in the case study. The scenarios reflect different passenger persona types and the privacy risks that affect their information and privacy.
Step 4: Measure the relevance and quality of the emerged scenarios.	The quality and relevance of the developed scenarios were evaluated in two ways. First, walkthrough review sessions were conducted with the supervisors. Second, the developed scenarios were reviewed with external experts in privacy risk and data protection. The scenarios were refined based on the feedback received.

The scenarios were documented in textual form. The documentation included a scenario overview, implementation, and results. The scenario overview described passenger personas, processes, technologies, and their interactions. In addition, it described the problem and the appropriate solutions. The personas are fictitious and do not represent real people.

### ***Case study***

PMAS is a major international airport that supports a large number of domestic and international flights to several destinations. PMAS smart airport terminals, both domestic and international, are equipped with the underlying digital technologies that enable several smart applications to support and facilitate the passenger journey. It provides passengers with self-service, biometric and automated services to move through the process without human assistance. During the journey, a vast amount of the passenger's digital information is collected, processed, and stored in airport and airline systems, which is also shared among several actors (carriers and government agencies). Although the intent of passenger information sharing is to enhance passenger experience, a passenger might be adversely impacted by the disclosure of their information to unauthorised systems and people. Therefore, it is important to assess the potential passenger information privacy risks with a view to reducing the risks and their impacts on individuals.

This case study example is further augmented with five hypothetical scenarios that describe the ready-to-fly process, including airport check-in, boarding control, and boarding on the departure side, using different self-service and automated systems. The scenarios involve examples of different types of passenger personas and the various privacy threats that affect their information. Table 5.6 presents descriptions of the passenger persona types used in the scenarios. It is important to note that the persona information in Table 5.7 and used in the scenarios is fictitious and does not represent real information about actual passengers.

*Table 5.7 Description of persona types used in scenarios.*

<b>Persona 1: Individual passenger</b>	
Name	Adam
Age	30 years
Occupation	Dentist
Travel purpose	Vacation
<b>Persona 2: Special needs passenger</b>	
Name	Linda
Age	50
Occupation	Engineer
Travel purpose	Job opportunity
<b>Persona 3: Diplomatic passenger</b>	
Name	William
Age	45
Occupation	Diplomat
Travel purpose	Conference
<b>Persona 4: Merchant passenger</b>	

Name	Jon
Age	60
Occupation	Businessman
Travel purpose	Trading
<b>Persona 5: Teenager passenger</b>	
Name	Omar
Age	16
Occupation	Student
Travel purpose	Vacation

### 5.3.2 Scenario 1: Individual adult passenger

#### **Overview**

Adam's vacation has just started, and finally, he can spend some time with his family. He has booked a domestic flight from M to J. On the day of his flight, he arrives at Terminal 1 at PMAS smart airport and goes through the smart check-in self-service kiosk, which helped him to move through the check-in process. He scanned his national ID and entered his e-ticket number and phone number to obtain his e-boarding pass. Adam's collected information is extracted from the kiosk and transferred to SA airline's system for identification purposes. In addition, it is stored in the airline's data system as a part of his passenger records.

Unauthorised access by an airline staff member to Adam's passenger record leads to his personal identifiable information being revealed. This is likely to impact Adam, who could suffer from both information disclosure and identity fraud.

There is a need to mitigate the information disclosure risk and protect Adam's privacy, after determining the classification of the information that was revealed. According to the data classification, various identity and privacy controls can be implemented, for example (but not limited to) identity and access mechanisms, privacy policies, or data encryption. The EU's GDPR, Saudi Arabia's Personal Data Protection Law (PDPL), and the Privacy Act 1988 are privacy regulations which influence and guide the protection, use, and disclosure of PII.

#### **Implementation**

This scenario is implemented and represented using a graph-based modelling approach as noted by the IJPRA ontology.

For this purpose, the Neo4j graph database was used to represent the instances, denoted by the green-coloured nodes, based on the scenario, and the relationship "INSTANCE\_OF" is used to specify the relationship between concepts and their instance, as shown in Figure 5.7.



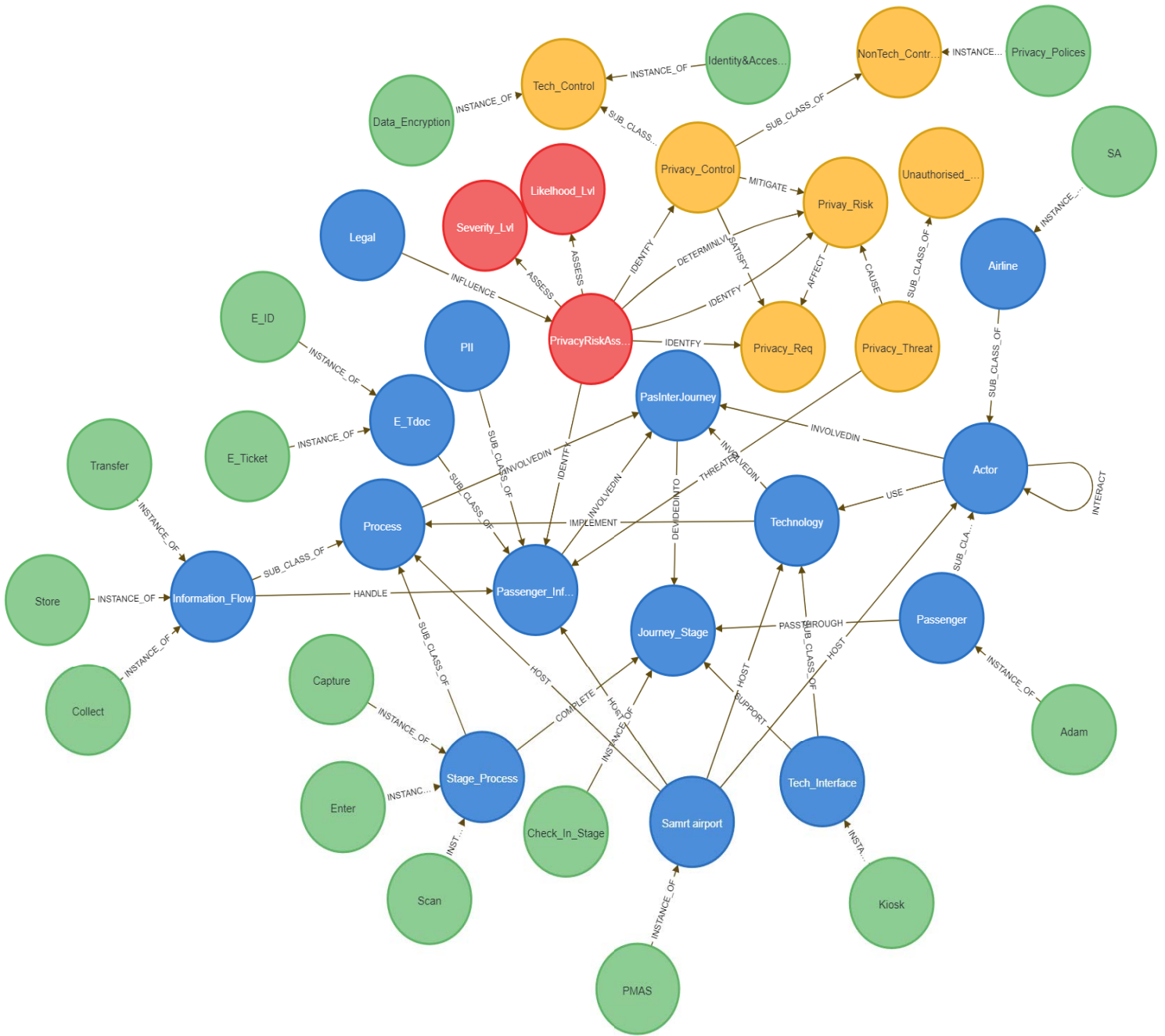


Figure 5.7 Scenario 1 implementation – iteration 2

## Results

The result of applying Scenario 1 to the IJPRA ontology shows that the current version of the ontology needs to be refined. To address this gap, six concepts were introduced as follows. The first concept is “Information\_Type”, representing the type of passenger information discussed in the scenarios. This concept then formed a “TYPE\_OF” relationship with “Passenger\_Information” concept. Another notable change was the introduction of “Passenger\_Record” concept to signify a type of passenger data mentioned in the scenario. The relationship “SUB\_CLASS\_OF” that previously connected “PII” and “Passenger\_Information” was eliminated because “PII” now aligns under the “Information\_Type”. Another concept, called “Information\_Classification” emerged to represent the classifications of passenger information, and a relationship called “CLASSIFY” was added, linking “Passenger\_Information” and “Information\_Classification” concepts. In the current alpha IJPRA ontology, there was an absence of a concept representing the impact of the risk on the passenger and their information. To cover this gap, a new concept called “Impact” emerged with a relationship “RESULTED\_IN” to connect it with “Privacy\_Threat” concept, and another relationship named “IMPACT”, connecting “Impact” concept to both “Passenger” and “Passenger\_Information” concepts. Also, a new concept called “Privacy\_Regulation” emerged as a sub-concept of the existing “legal” concept to represent the regulation specified in the scenario. Accordingly, the IJPRA ontology was refined to include these new concepts and relationships. The emerged concepts and their definitions are shown in Table 5.8. It is important to note that the “Passenger\_Record” and “Information\_Classification” are newly emerged concepts that can be mapped to closely related definitions in relevant studies but may not be exactly defined. Therefore, they are labelled as “new” in the ref column in Table 5.8. The refined ontology is represented using graph-based modelling approach, as shown in Figure 5.8. The emerged concepts denoted by the purple-coloured nodes in Figure 5.8.

Table 5.8 Emerged concepts and their definitions based on scenario 1 results

Emerg ed concept	Definition	Ref
Information_Type	The category of passenger information collected by a smart airport, such as PII, medical, or financial information, as well as passenger records and biometric data.	(Chua, Ooi & Herbland 2021)
Passenger_Record	The type of passenger information which includes information about a passenger booking and their identity in an electronic record.	New

Emerg concept	Definition	Ref
Impact	The potential damage to passengers and their information due to the occurrence of privacy risks.	(National Institute of Standard and Technology 2013)
Information _Classification	The way passenger information is classified based on its sensitivity level, 159or example, confidential, public, private, and restricted.	New
Privacy Regulation	The law that influences and guides the purpose behind collecting passenger information and its intended use.	(ISACA n.d.)



Figure 5.8 Scenario 1 results- refined IJ graph-based model (alpha version)

### 5.3.3 Scenario 2: Teenage passenger

#### **Overview**

Omar is a teenager who is studying in high school. During the school holidays, he wanted to visit his grandparent, who lives in another city. Omar’s father booked the domestic flight for his son from C to D. On the day of his flight, Omar arrived at Terminal 2 at PMAS smart airport, and went through all the stages prior to the boarding stage. At the boarding stage, he scanned his e-boarding pass using boarding kiosks. After verification, the automated door opened, and he was ready to board the aircraft. Omar’s information is extracted from the kiosk and stored in SA airline’s system. Omar’s passenger record is amended by the service providers offering the server cloud to airlines to store passenger information which leads to his information being revealed. This is likely to impact Omar, who could suffer from information disclosure.

There is a need to mitigate the information disclosure risk and protect Omar’s privacy by implementing the appropriate privacy control depending on the classification of the data.

#### **Implementation**

In figure 5.9, this scenario is implemented to the IJPRA ontology and represented using a graph-based modelling approach. The Neo4j graph database was employed to represent the instances, which are shown in green nodes (Figure 5.9). The relationship “INSTANCE\_OF” is used to define the connection between the concepts and their instance, based on the scenario (Figure 5.9).

#### **Results**

After applying the scenario to the developed IJPRA ontology, the results show that the alpha version lacks concept that represent the service provider as a type of actor in the passenger journey. To address this gap, a new concept named “Organisation/SP” emerged. The current alpha IJAPR ontology was refined to include the emerged concept. Table 5.9 includes the emerged concept and its definition. The improved version of the IJPRA ontology is represented in a graph-based model in Figure 5.10, and the emerged concept, denoted by the purple node.

*Table 5.9 Emerged concepts and their definitions based on scenario 2 results*

<b>Emerg ed concept</b>	<b>Definition</b>	<b>Ref</b>
Organisation/SP	A service provider that offers several services for passengers and airlines, and government in a smart airport.	(European Union Agency for Network and Information Security 2016)

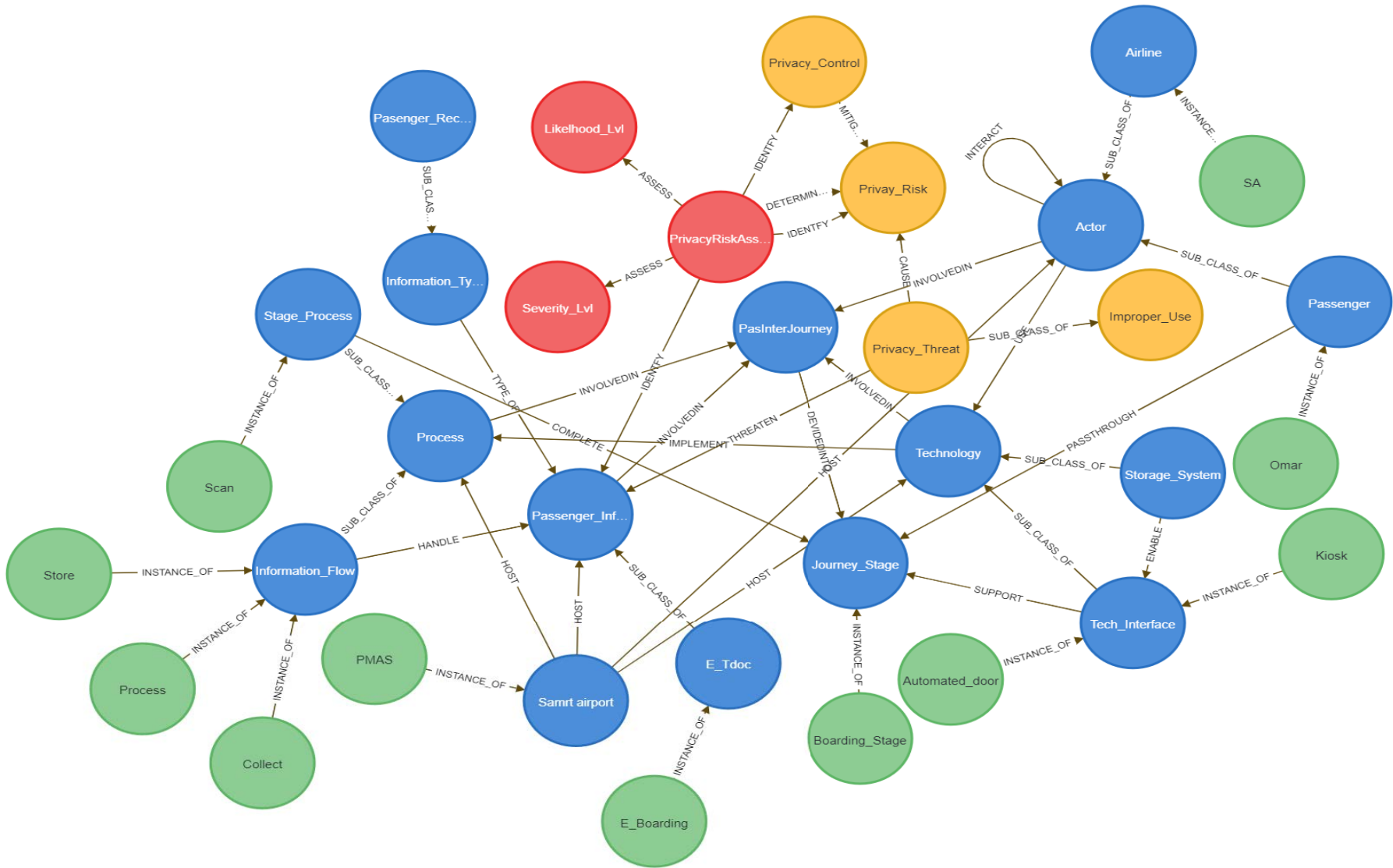


Figure 5.9 Scenario 2 implementation – iteration 2

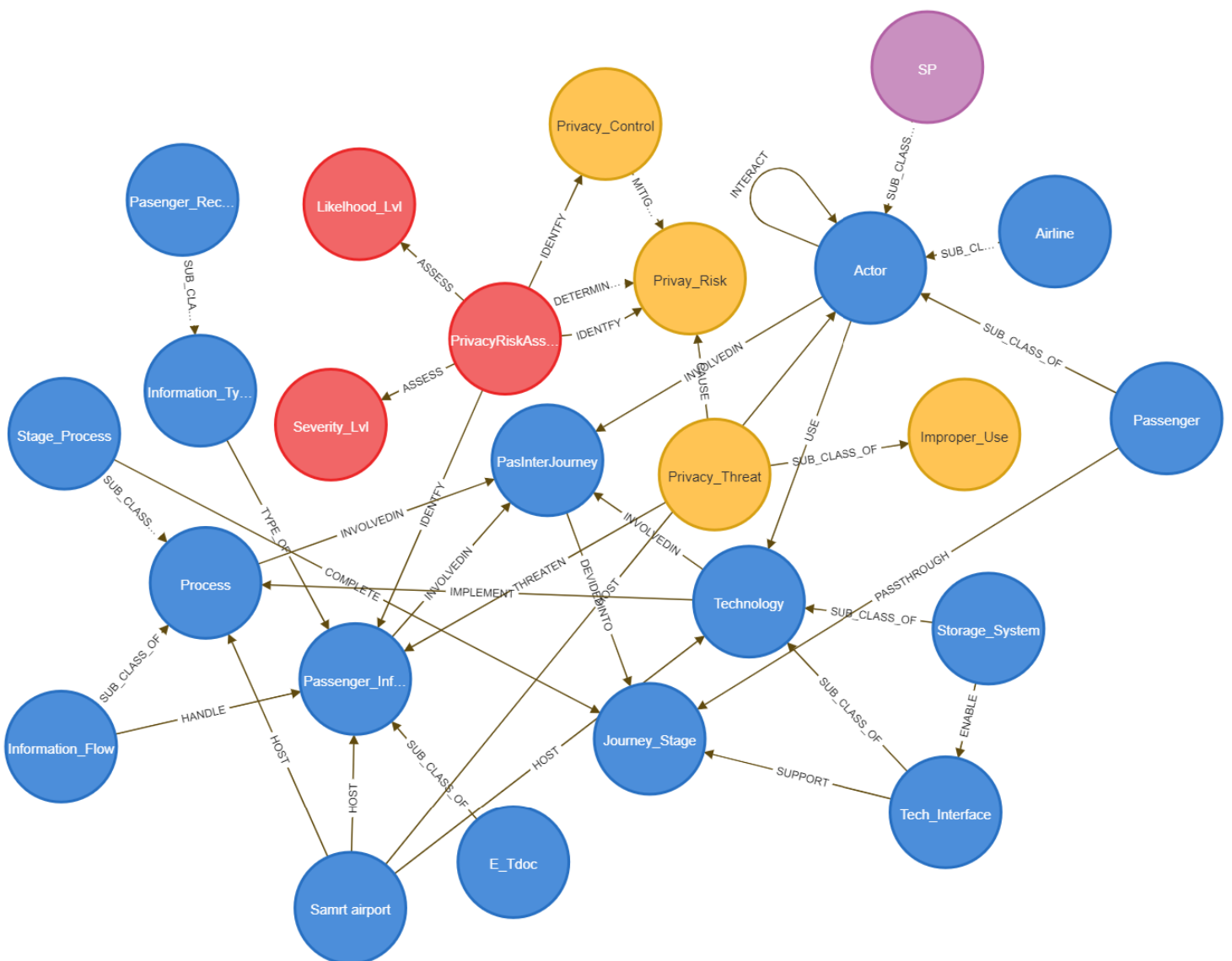


Figure 5.10 Scenario 2 results- refined IJPRG graph-based model (alpha version)

### 5.3.4 Scenario 3: Merchant passenger

#### Overview

Jon is merchant and has booked a domestic flight for his journey from point M to D. On the day of his flight, he arrived at Terminal 1 at PMAS smart airport, and went through the smart check-in self-service, and used a kiosk which helped him to move through the check-in process. He entered his e-ticket number and phone number, inserted his credit card for a flight upgrade, and obtained his e-boarding pass after the verification process. Jon’s information is extracted from the kiosk and transferred to SA airline’s system. In addition, his credit card information is added to his record, which is stored in the airline’s data system. Jon’s credit card information is intentionally shared with an unauthorised person by an airline staff member, revealing his

financial information. This is likely to impact Jon, who could suffer from both information disclosure and financial loss.

There is a need to mitigate information disclosure risk and protect Jon’s privacy based on the classification of his data. According to the data classification, several identity and privacy controls can be implemented, such as privacy policies, and data encryption. The PDPL guides the protection, use, and disclosure of financial information. In addition, the Payment Card Industry Data Security Standard (PCI-DSS) is a set of guidelines designed to enhance the security of credit card transactions and safeguard cardholders' personal information.

**Implementation**

The graph-based modelling approach was used to implement and represent this scenario, as noted by the IJPRA ontology, using Neo4j graph, as shown in Figure 5.11. The instances, presented by the green nodes, and connected with relevant concepts by “INSTANCE\_OF” relationships is (Figure 5.11).

**Results**

After applying the scenario to the developed IJPRA ontology, the results revealed that the current alpha version of IJPRA ontology does not include concept representing privacy standard mentioned in the scenario. The privacy standard is crucial for ensuring data protection and compliance with privacy regulations. To cover this gap, a new concept called "Privacy\_Standard" emerged as a sub-concept of the existing “legal” concept. On the other hand, a concept named “Financial\_Info” was identified. This concept is considered as a sub-concept of the existing concept “Information\_Type” in the IJPRA ontology. Table 5.10 includes the emerged concepts and their definitions. The emerged concepts are denoted by the purple nodes in Figure 5.12, which presents the refined version of IJPRA graph-based model based on this scenario results.

*Table 5.10 Emerged concepts and their definitions based on scenario 3 results*

<b>Emerged concept</b>	<b>Definition</b>	<b>Ref</b>
Financial_Info	A type of passenger information that identifies financial details, such as credit cards, assets, income, bank accounts, and expenses.	(Chua, Ooi & Herbland 2021)
Privacy_Standard	The guidelines which establish the requirements for handling passenger information, implementing data security, and compliance with privacy regulations in smart airports.	(ISACA n.d.)



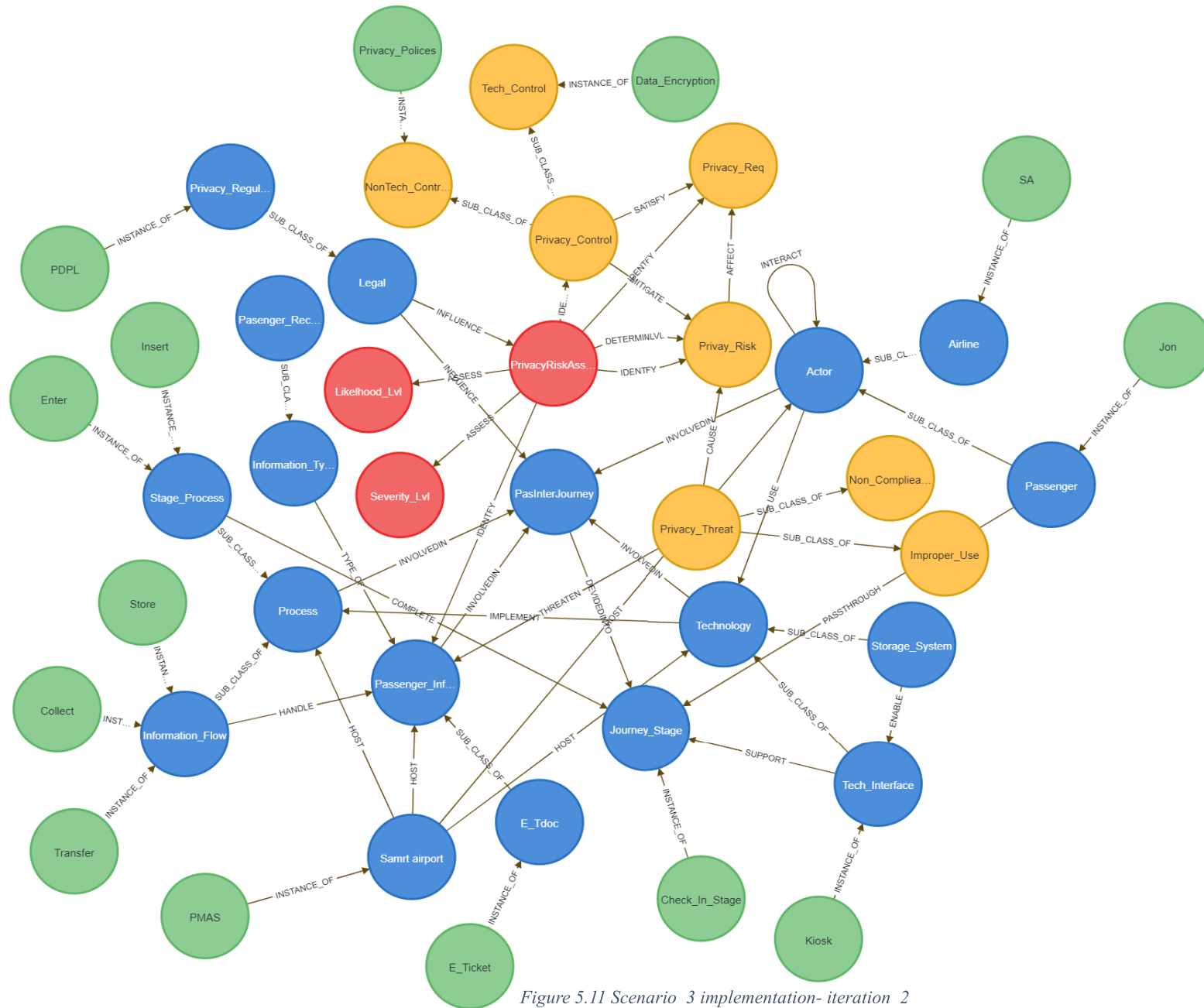


Figure 5.11 Scenario 3 implementation- iteration 2





airline's system for verification based on her stored record in the airline's data system. Her passenger record includes medical information about her disability.

Information leakage caused by a cybercriminal attack on the airline's data storage resulted in Linda's medical information being leaked. This is likely to impact Linda, who could suffer from information disclosure and lose control of her confidential information.

There is a need to mitigate the information disclosure risk and protect Linda's privacy based on the classification of the revealed information. According to the data classification in the scenario, several privacy controls can be implemented, for example but not limited to data minimisation, privacy policies, or data encryption. The US Health Insurance Portability and Accountability Act (HIPAA) is a privacy regulation which guides the protection, use and disclosure of medical information.

### ***Implementation***

The scenario is implemented and represented using a graph-based modelling approach, as noted by the IJPRA ontology. For this purpose, the Neo4j graph database was used to represent the instances, denoted by the green nodes based on the scenario, and the relationship "INSTANCE\_OF" is used to specify the relationship between concepts and their instance, as shown in Figure 5.13.

### ***Results***

While applying the scenario to the developed IJPRA ontology, an emerging concept "Medical\_Info" providing a sub-concept of the existing concept "Information\_Type" in the IJPRA ontology. The emerged concept definition is presented in Table 5.11. The emerged concept is denoted by the purple node in refined IJPRA graph model based on this scenario results (Figure 5.14).

*Table 5.11 Emerged concepts and their definitions based on scenario 4 results*

<b>Emergед concept</b>	<b>Definition</b>	<b>Ref</b>
Medical_Info	A type of passenger information that identifies their health or medical conditions.	(Chua, Ooi & Herbland 2021)

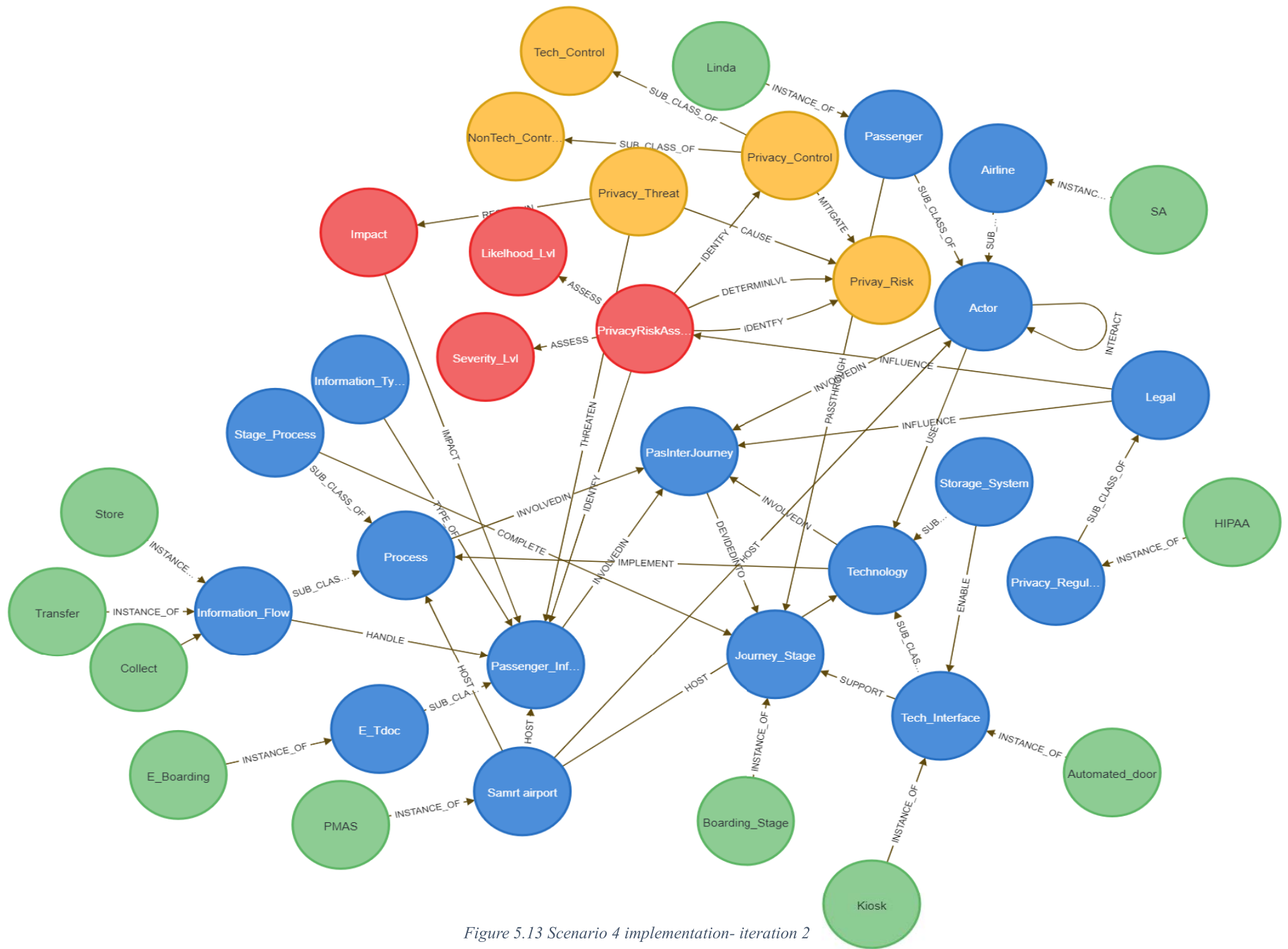


Figure 5.13 Scenario 4 implementation- iteration 2



Figure 5.14 Scenario 4 results- refined IJPRA graph model (alpha version)

### 5.3.6 Scenario 5: Diplomatic passenger

#### Overview

William is a diplomat who representing his country as a delegation member at a conference held overseas. He booked an international flight and obtained his e-boarding pass before arriving at PMAS international airport. He arrived at Terminal 5 of PMAS smart airport and headed to border control after completing the check-in. To complete this stage, he scanned his e-passport and stood in front of the camera that captured his photo. The collected information, including his passport number and photo (biometric data), was transferred to the government agency's system, and processed to verify his identity. After verification, he entered the restricted area.

A secondary use of William's biometric data by the government agency for other purposes resulted in a leakage of his biometric data. This is likely to impact William, who could suffer from information disclosure and a loss of control over his biometric data.

There is a need to mitigate the information disclosure risk and protect William's private information based on the classification of his data. According to the data classification, various privacy controls can be implemented, for example (but not limited to) biometric matching, informed consent, privacy policies, or secure storage. The EU GDPR, and the Privacy Act 1988 are privacy regulations which guide the protection, use, and disclosure of PII.

### ***Implementation***

The IJPRA ontology was represented using graph modelling approach to implement this scenario, as depicted in Figure 5.15. Using Neo4j graph database, the instances were denoted by the green-coloured nodes, as seen in Figure 5.15, whereas the relationship "INSTANCE\_OF" was used to specify the relationship between concepts and their instance.

### ***Results***

The IJPRA ontology was applied to scenario 5 as shown in Figure 5.15. As a result, a concept named "Biometric\_ Info" was introduced as a sub-concept under the existing concept "Information\_Type", as shown in (Figure 5.16). The emerged concept is denoted by the purple node in the refined IJPRA graph model based on this scenario results (Figure 5.16) and its definition is given in Table 5.12.

*Table 5.12 Emerged concepts and their definitions based on scenario 5 results*

<b>Emerged concept</b>	<b>Definition</b>	<b>Ref</b>
Biometric_ Info	A type of passenger information that refers to information about the biological characteristics of a passenger.	(Morosan 2018; Patel 2018)

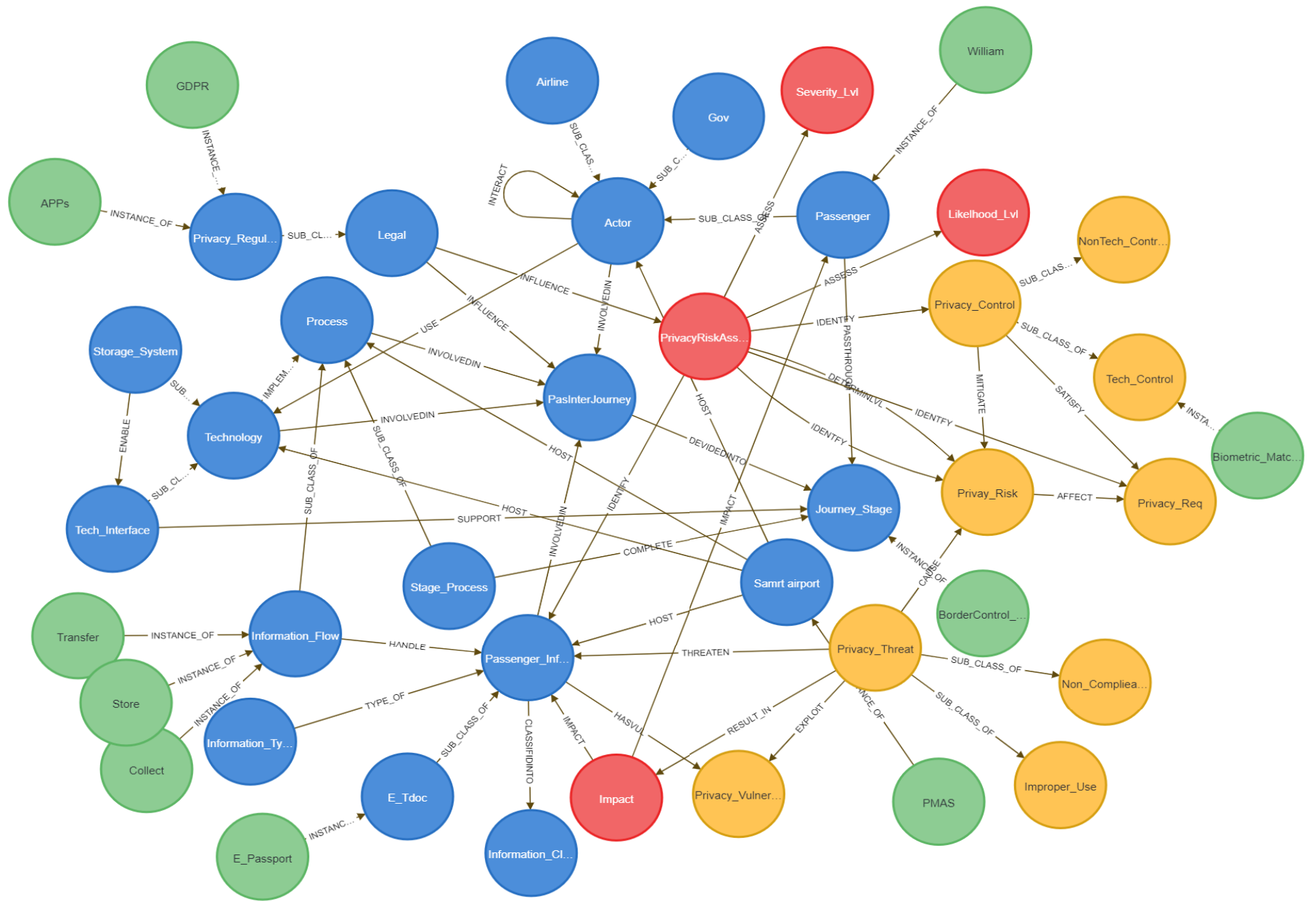


Figure 5.15 Scenario 5 implementation- iteration 2

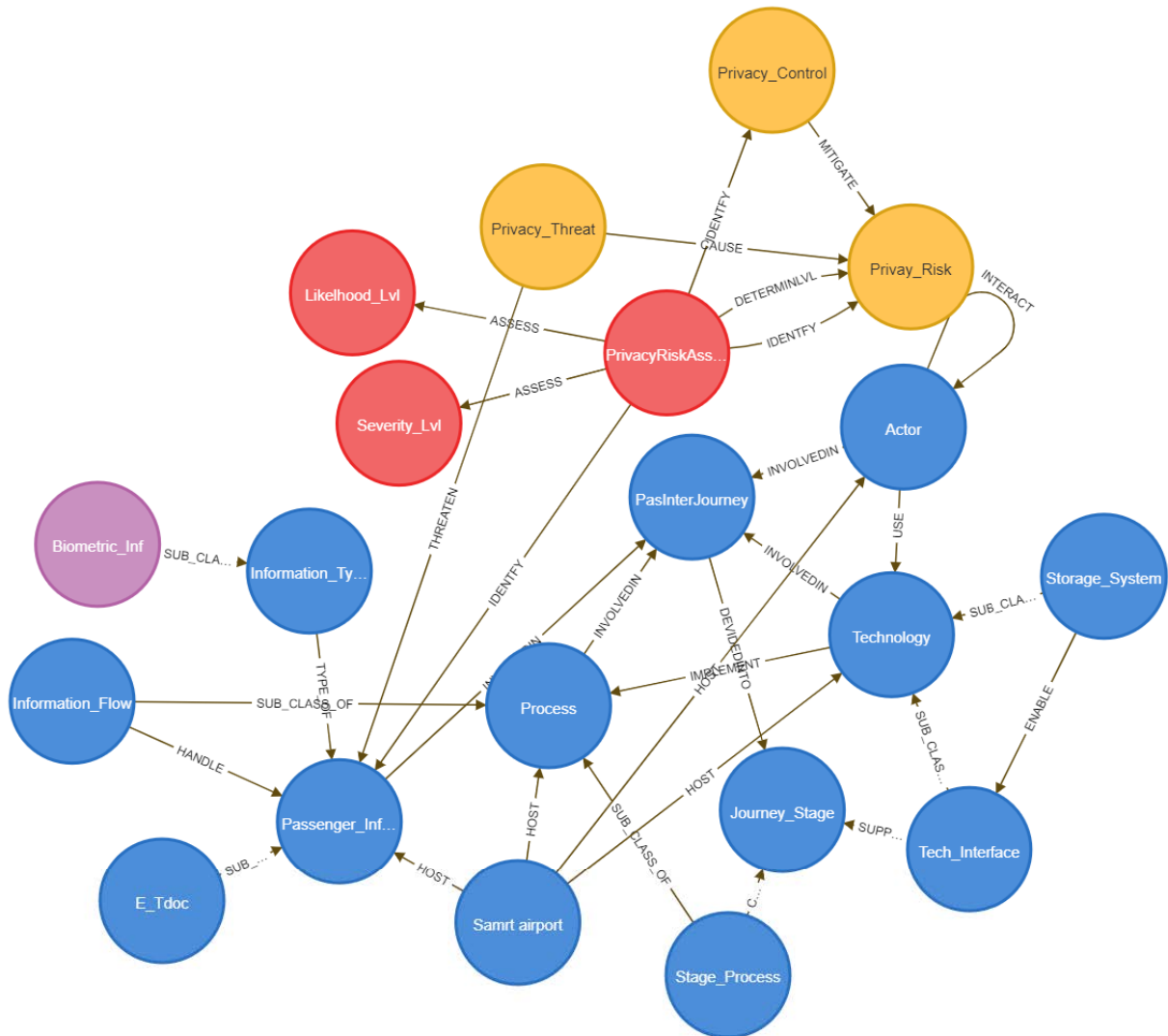


Figure 5.16 Scenario 5 results- refined IJPR graph model (alpha version)

### 5.3.7 Evaluation results in iteration 2

The evaluation of the alpha version using the illustrative scenario evaluation method led to the development of the beta version of the IJPR ontology (Figure 5.17). The beta version of the IJPR ontology is applicable to cover the domain of privacy risks in a smart airport, providing sufficient concepts and relationships to represent and capture information and the risks in the evaluation scenario relevant to privacy risk analysis and assessment. Figure 5.17 shows the beta IJPR ontology represented by the graph-based modelling approach.

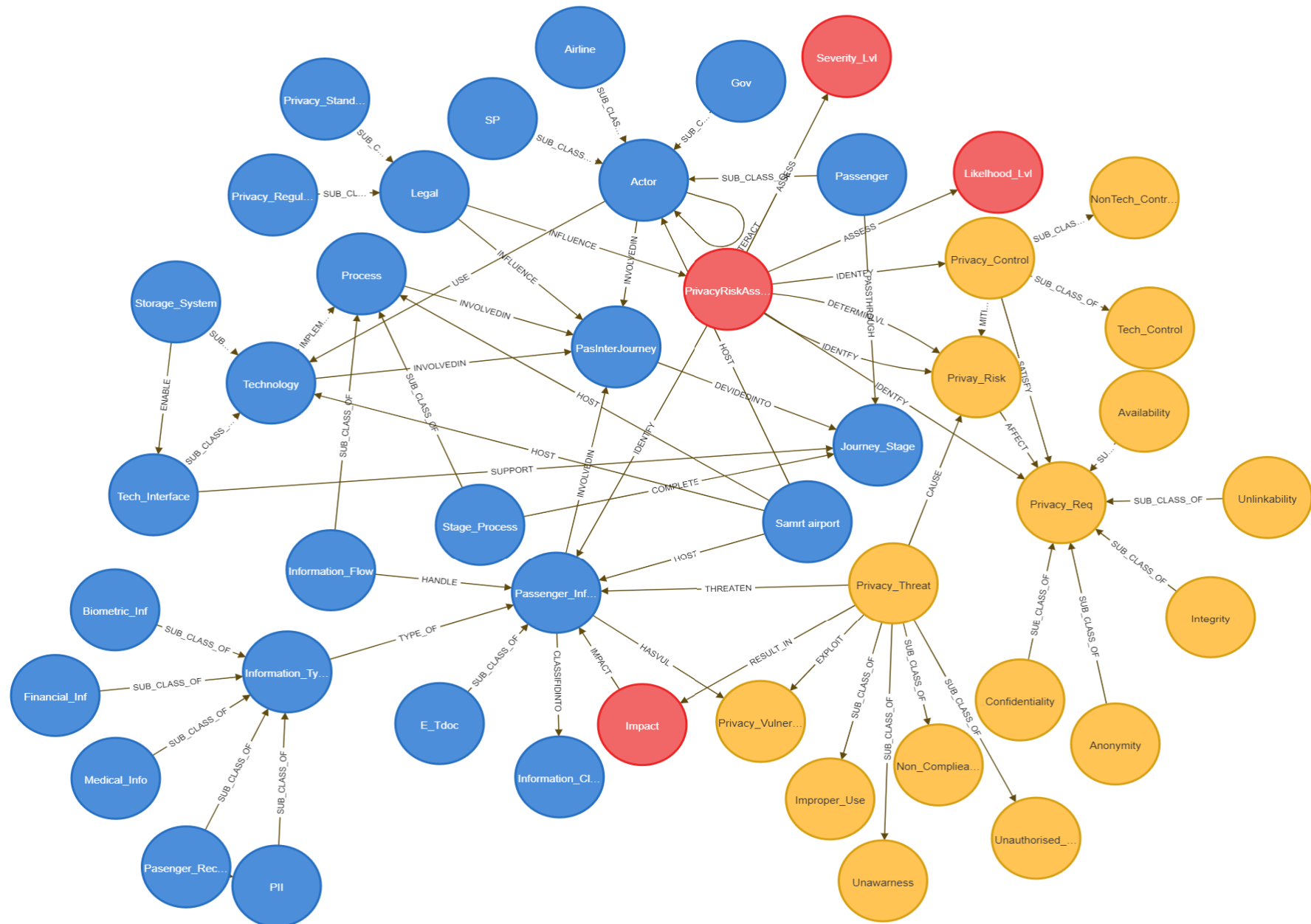


Figure 5.17 IJPRA ontology beta version



### 5.3.8 The IJPRA architecture beta version

The alpha version of the IJPRA architecture was improved based on the analysis of the IJPRA ontology using the illustrative scenarios in iteration 2 (as previously discussed). The beta version of the architecture was developed by including concepts from the beta version of the IJPRA ontology. This means that the IJ and PR layers, the two layers in the IJPRA architecture, were designed using the IJPRA ontology concepts and sub-concepts represented in the IJPRA graph model in Figure 5.17. Figure 5.18 presents the beta version of IJPRA architecture.

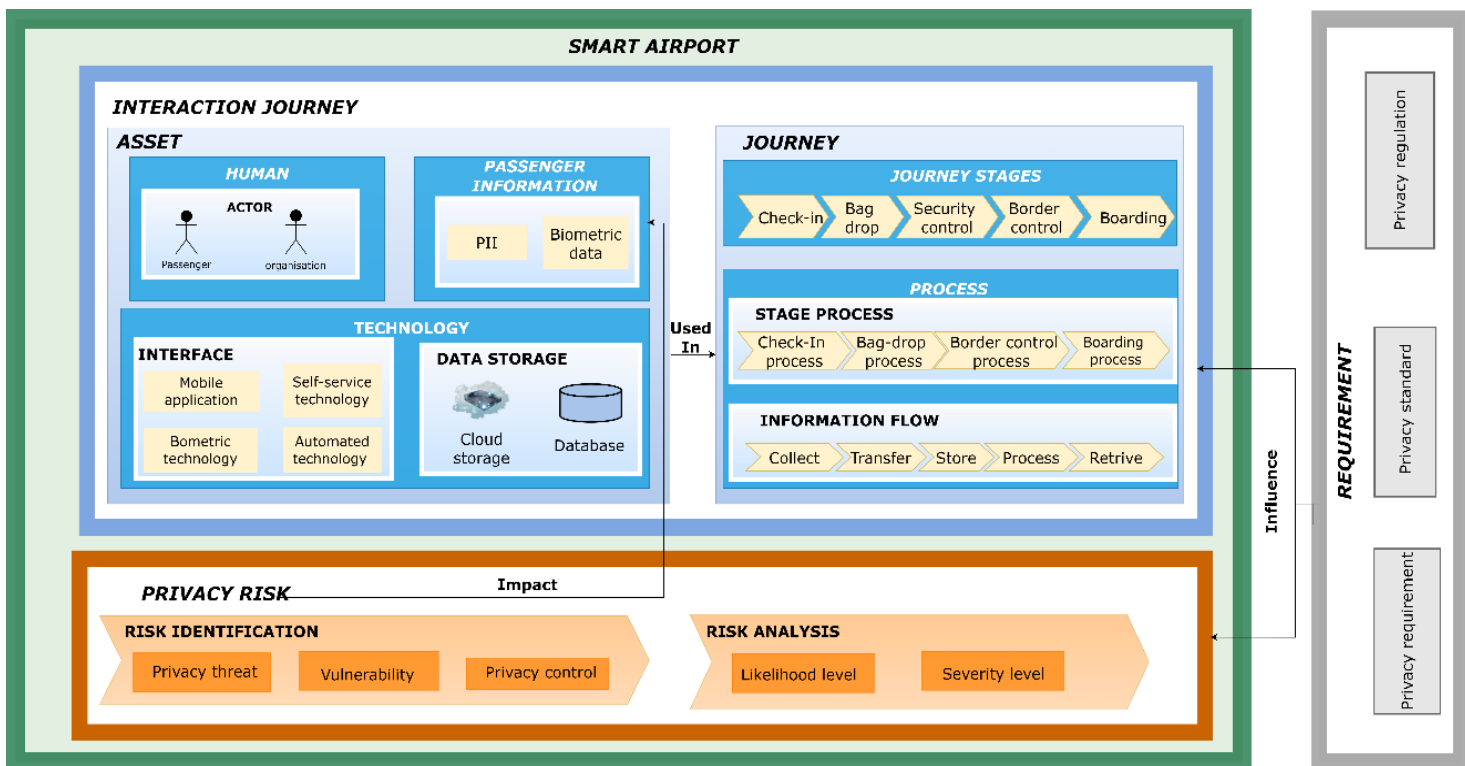


Figure 5.18 IJPRA architecture beta version

As shown in Figure 5.18, the IJPRA architecture comprises two layers: the IJ layer and the PR layer. Both layers were influenced by a list of requirements relevant to privacy law in smart airports. The IJ layer comprises two components: asset and journey, as shown in Figure 5.18. Information about these components was defined using the beta version of the IJPRA ontology concepts (see Figure 5.17). The IJPRA ontology concepts used to design this layer are Actor, Technology, Passenger, Organisation/airline, Organisation/Gov, Passenger\_Information, PII, Tech\_Interface, Storage\_System, Smart airport, PasInterJourney, Journe\_Stage, Process, Stage\_Process, Information\_Flow, and Biometric\_Info. The asset component evolves three concepts: Actor, Technology, and Passenger\_Information and instances of these concepts. The actor includes passengers and Organisations (airlines and governments), who are involved and

interact in the passenger journey (Figure 5.18). The technology concepts presented in Figure 5.18 represent the technological interface and data storage involved in the passenger interaction journey. This covers several technological interfaces that support each stage of the passenger journey and data storage that enable the interfaces. This beta version of the IJPRA architecture includes instances of the technological interfaces used by passengers in each stage of the journey, including self-service technology, automated technology, biometric technology, mobile application, and database, and cloud-based storage as instances of data storage. The passenger information includes the passenger's PII, and biometric information as instances of the passenger information handled during the passenger journey.

The Journey component presented two concepts in the IJPRA ontology beta version, including journey stages, process, and their instances. Journey stages shows the stages of the passenger journey on the departure side including check-in, bag-drop, security control, border control, and boarding (Figure 5.18). Process is another concept under the journey component that represent a set of activities during the passenger journey. It includes two types of processes: (1) process stages to represent the passenger activity in each stage, and (2) information flow that shows the process of handling passenger information during the journey stages. Also, the instance of these processes was represented in this version of the architecture (Figure 5.18).

The privacy risk layer uses concepts in the IJPRA ontology beta version presented in Table 5.3 and Table 5.4. This layer mainly focuses on the risk assessment process used to assess the privacy risks associated with passenger information during the journey. The process consists of two steps: risk identification and risk analysis. The risk identification step involves the identification of privacy threats, privacy vulnerability associated with passenger information, and existing privacy controls, either technical or non-technical, as countermeasures of the identified risk (Figure 5.18). Following the identification step, a risk analysis step is conducted to evaluate the severity and likelihood levels to determine the overall risk level.

The IJ and PR layers are influenced and guided by an influencing factor named requirement, as shown in Figure 5.18. It includes privacy law, including regulation and standard and requirements relevant to the aviation industry. The *Privacy\_Regulation*, *Privacy\_Standard*, and *Privacy\_Requirement* concepts in the IJPRA ontology beta version were used to design this influencing factor. The definitions of these concepts are listed in Tables 5.4, 5.8, and 5.10. The requirement in the IJPRA architecture beta version (Figure 5,18) guides the use and handling of passenger information during the interaction journey and the risk assessment process. This

guarantees adherence to privacy-related regulations, enhances data privacy and security, and improves the overall passenger experience. Hence, this research focuses on understanding privacy law as an influencing factor that guides the interaction journey and privacy risk assessment process. Details about how they influence the interaction journey are out of the scope of this research, as discussed in the research limitations.

In summary, the beta version of the IJPRA architecture shown in Figure 5.18 includes relevant concepts and their instances under each component in the architecture, the IJ and PR layers. These layers were designed using the IJPRA ontology beta version. However, further improvement and details about the view of actors, technology, process, information, and legal under the IJ layer, as well as risk identification and assessment tools, will be developed in the architecture's gamma version after evaluating this version in the third iteration using an expert evaluation method via field survey.

The next section discusses iteration 3 of the IJAPRA framework evaluation that led to the development of the IJAPRA framework gamma version discussed in Chapter 4

#### 5.4 Analysis of the alpha and beta versions of the IJAPRA framework.

This section discusses the IJAPRA framework refinement and evolution from the alpha version to the improved version (beta) based on evaluation results of each iteration of the analysis, as explained Table 5.13. As previously discussed, the IJAPRA framework consists of two components: IJPRA ontology and IJPRA architecture. Table 5.13 details the iteration of the evaluation process, the version of the IJAPRA framework that is evaluated, the description of the improved framework version based on the evaluation result in each iteration., and diagrams of each version of IJAPRA framework components.

Table 5.13 Description of the IJPRA framework evaluation results in iteration 1 and 2

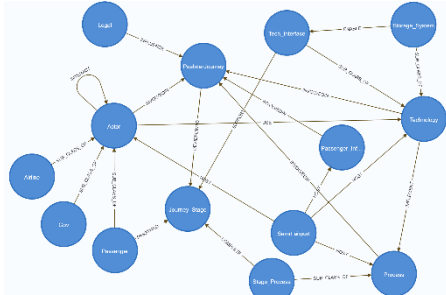
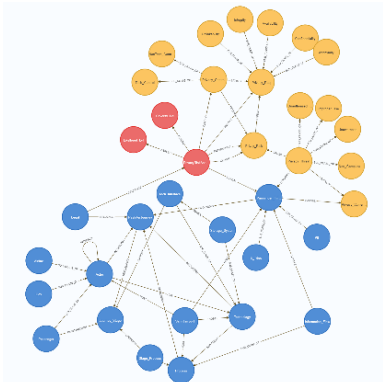
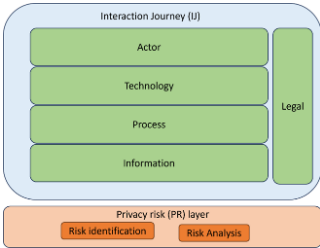
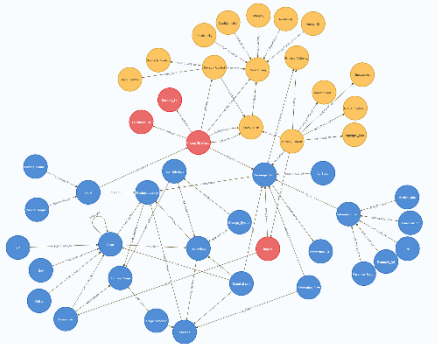
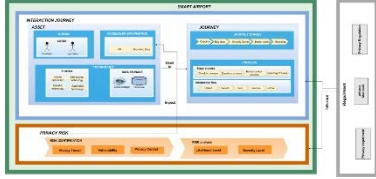
Iteration	Version	Description	Diagram
Iteration 1	IJPRA ontology-alpha version	<p>In this version of the IJPRA ontology, the IJ ontology was initially developed as a first increment of framework development. The IJ development relied on the review of relevant existing studies and pre-determined kernel theories, including AEA and the CJM framework adopted as a theoretical lens. In the alpha version of the IJ ontology, 14 concepts were identified (see Table 5.2) and connected by several identified relationships. Figure 5.2 presents the alpha version of the IJ ontology represented using the graph-based modelling approach.</p>	
		<p>The developed IJ ontology (alpha) was evaluated using an illustrative scenario to measure its applicability in capturing knowledge of the passenger interaction journey. The evaluation led to improving the alpha IJ ontology to a beta version that included three more concepts and their relevant relationships as a result of the evaluation. Following the improvement of the IJ ontology from the alpha to the beta version, the PR ontology alpha version was developed in increment 2 based on existing studies and the adopted theoretical and practical lenses (see Section 5.2.1). In the alpha version of the PR ontology, 16 concepts were identified (see Table 5.4) and connected with relevant relationships. Then the IJ and PR ontology were integrated to develop the IJPRA ontology in increment 3 (see Section 5.2.1). Three concepts were identified (see Table 5.5) and connected by associated relationships for integration purposes. Figure 5.5 shows the alpha version of the IJPRA ontology represented using the graph-modelling approach.</p>	

Figure 5.2(recalled) IJ graph-based model (alpha version)

Figure 5.5(recalled) IJPRA graph-based model (alpha version)

Iteration	Version	Description	Diagram
	IJPRA architecture - alpha version	<p>The IJPRA architecture's alpha version comprised two layers: IJ and PR, as shown in Figure 5.6. The IJ layer was developed using the adopted AEA framework as a theoretical lens. This layer includes five core concepts: Actor, Technology, Process, Information, and Legal. The PR has two elements: risk identification and risk analysis that represent the risk assessment process. The alpha version of the IJPRA architecture primarily encompasses two layers and their foundational elements. As depicted in Figure 5.6, this preliminary IJPRA architecture establishes the groundwork for additional enhancements in the second iteration.</p>	 <p>The diagram illustrates the IJPRA architecture (alpha version). It consists of two main layers. The top layer is the Interaction Journey (IJ), which is a light blue rounded rectangle containing four stacked green boxes labeled Actor, Technology, Process, and Information. To the right of these boxes is a vertical green bar labeled Legal. Below the IJ layer is the Privacy Risk (PR) layer, which is an orange rounded rectangle containing two stacked orange boxes labeled Risk identification and Risk Analysis.</p> <p><i>Figure 5.6(recalled) IJPRA architecture (alpha version)</i></p>
Iteration 2	IJPRA ontology-beta version	<p>The alpha version of the IJPRA ontology was evaluated with five scenarios pertinent to privacy risk analysis related to passenger information in smart airports. Based on this evaluation, the IJPRA ontology was improved from its alpha version, incorporating 10 additional concepts derived from each scenario's evaluation result. The refined beta ontology demonstrated its applicability to represent the domain by encompassing the necessary concepts and relationships to capture the information and privacy risk in the scenarios. This indicates that the beta version of the IJPRA ontology is applicable for privacy risk analysis and assessment. Figure 5.17 shows the beta version of the IJPRA ontology represented using the graph-modelling approach.</p>	 <p>The diagram shows a graph-based model of the IJPRA ontology (beta version). It features a complex network of interconnected nodes. The nodes are represented by circles of various colors: blue, yellow, and red. The connections between nodes are shown as thin, light-colored lines, forming a dense web of relationships. The overall structure is roughly circular, with many nodes clustered together and some extending outwards.</p> <p><i>Figure 5.17 (recalled)IJPRA graph-based model (beta version)</i></p>
	of IJPRA architecture -beta version	<p>Following the development of the IJPRA beta ontology, the alpha version of the IJPRA architecture was improved. Drawing insights from the beta version of the ontology, the architecture included more concepts and their instances, becoming more comprehensive and relevant. In the alpha version, the architecture comprised only two layers, IJ and PR, and their corresponding foundation</p>	

Iteration	Version	Description	Diagram
		<p>elements that were designed based on the adopted AEA framework used as theoretical lens. This version of the architecture was refined to include additional details and instances under the layers derived from the IJPRA ontology beta version. This improvement transformed the IJPRA architecture from the alpha version's limited scope to the more elaborate and encompassing architecture. The beta version of the architecture is more comprehensive and is poised to assist on assessing privacy risks in a smart airport. Figure 5.18 shows the beta version of the IJPRA architecture.</p>	 <p>The diagram illustrates the IJPRA architecture (beta version) as a multi-layered system. At the top, it is divided into 'REGULATION AGENCY' and 'TRAVEL AGENCY'. Below these are 'ASSET' and 'JURISDICTION' components. The bottom layer is labeled 'PRIVACY RISK' and includes 'IDENTIFICATION', 'ASSESSMENT', 'MITIGATION', and 'REPAIR' stages. A vertical bar on the right side represents 'PERSONAL DATA' with 'ACCESS' and 'PROTECTION' sub-sections.</p> <p><i>Figure 5.18 IJPRA architecture (beta version)</i></p>

## 5.5 Iteration 3- IJAPRA framework Gamma version

Following the development of the beta version in Iteration 2, the IJAPRA framework was subjected to a field survey for expert evaluation purposes. This survey was the third iterative evaluation undertaken in this thesis to obtain the gamma version of the IJAPRA framework (discussed in Chapter 4). In this iteration, the beta version of the IJAPRA architecture, the second component in the IJAPRA framework, was evaluated to measure its applicability, usefulness, generalisability, and understandability (see Table 3.2 in Chapter 3). Based on the evaluation results in this iteration, both IJAPRA framework components were improved. According to Runeson & Höst (2009), a survey constitutes the gathering of particular information offered to specialists and to specific population groups. The field survey was presented online to global and local experts in the field of information privacy/security and data protection. The survey was constructed using a common survey design proposed by Hyndman (2008) as discussed below. The evaluation results were used to improve and refine the IJAPRA framework on the basis of expert feedback.

### *Survey planning*

The purpose of this survey was to gather expert feedback and opinions about the beta version of the IJAPRA framework which were used to improve and refine the IJAPRA to develop the gamma version. The plan for the survey was to gather qualitative and quantitative data from the experts. The survey data analysis seeks to ensure that the IJAPRA satisfies the evaluation criteria (see Chapter 3, Table 3.2).

### *Designing the sampling procedure*

The online field survey (Appendices D and F include the survey link) was presented to participants who are experts in the field of information privacy/security and data protection. The participants were from Australia, the US, the UK, the KSA, Dubai, and India. The invitation letter and the online information sheet approved by the UTS ethics approval (**UTS HREC REF NO. ETH20-5093**) (Appendices B, C, and D) were used to contact with the participants via LinkedIn and email. The online survey information sheet (Appendix D) outlined the motivation and rationale for this research, as well as the risks, privacy considerations, advantages, and rights of the participants. Additionally, it provided information on the reason for selecting participants and the benefits of their involvement in the survey. Also, it included a link to enable participants to access the online survey, and as clearly specified, submission of the online questionnaire/s constituted an indication of their consent. As outlined in the online survey

information sheet in Appendix D, no personal information was gathered pertaining to the participants. The survey data were stored in UTS systems in full compliance with the UTS research data management policy.

The participants comprised industry and research experts. Table 5.14 shows the percentage of the participants' years of experience in the field of information privacy/security and data protection. According to Table 5.14, about 49% of experts have more than 10 years of experience, while around 37% have experience ranging from 5 to 10 years. Around 14% of experts have less than 5 years of experience, with a minimum of 3 years. This indicates that a significant majority of experts possess at least five years of experience or more. This implies that the participants have the ability to provide valuable feedback and numerous comments in light of their length of experience and their corresponding expertise in the relevant fields. It is important to emphasise that the responses of the participants were not arranged in any particular order, with the purpose being to avoid comparing the differing perceptions and opinions held by researchers and industry experts.

*Table 5.14 Participants' years of experience*

<b>Years of experience in the field</b>	<b>Percentage</b>
More than 10 years	49%
Between 5 and 10 years	37%
Less than 5 years	14%

### ***Survey method selection***

The IJPRA architecture, the second component of the IJAPRA framework, was evaluated using an expert evaluation via field survey. The survey was available online and sent to participants via LinkedIn and email. The survey was open from September 2022 to February 2023. The online survey was completed by 35 participants in total.

### ***Questionnaire development***

The survey consists of six questionnaire sets in six categories, as follows (see Appendix E) :

- QS1 set: IJPRA applicability (4 question)
- QS2 set: IJPRA understandability (1 question)
- QS3 set : IJPRA usefulness for privacy experts (3 question)
- QS4 set: IJPRA generalisability (1 question)
- QS5 set: Subjective feedback and evaluation (2 question)
- QS6 set: IJPRA overall feedback and rating (1 question)



### ***Questionnaire pretest***

The questionnaire was developed in four iterations, based on discussions with and feedback from the supervisor of this thesis, followed by a pilot test conducted with three participants to evaluate the research instrument construction and relevance. Based on the feedback received from the pilot study the questionnaire and the IJPRA architecture description were refined and improved.

### ***Collection and analysis of data***

Two types of data were produced from the survey questionnaire sets (see Appendix E):

- Quantitative data: ratings or categories of data converted into numerical data from closed-end questions (ratings of the participants' responses in sets QS1, QS2, QS3, QS4, QS6)
- Qualitative data: subjective responses to open-ended questions (participants' subjective feedback in set QS5)

The survey evaluation includes two steps: data collection and data analysis discussed below.

#### **5.5.1 Survey data collection**

The procedure used for data collection is presented as follows. The data gathered from the survey can be grouped into quantitative and qualitative data.

- Quantitative data sources are the ratings gathered in response to the close-ended questions in survey questionnaire sets QS1, QS2, QS3, QS4, and QS6 (see Appendix E)
- Qualitative data source are the subjective feedback gathered in response to the open-ended questions in survey questionnaire set QS5 (See Appendix E).

##### ***5.5.1.1 Quantitative data collection***

The survey questionnaire sets QS1 to QS4, and QS6 give the participants the opportunity to evaluate the IJPRA architecture against the evaluation criteria in Table 3.2 in Chapter 3. The questions in these sets are organised into Tables 5.15 to 5.19 and grouped based on their relevance to the evaluation criteria (applicability, understandability, usefulness, and generalisability)(Table 3.2 in Chapter 3). The questions are grouped as follows:

Table 5.15 Questionnaire set QS1-Applicability questions group

Question	Description	Evaluation criteria
Q1	The Asset defined in the interaction journey (IJ) includes necessary assets used in the passenger journey in a smart airport.	Applicability
Q2	The Journey defined in the interaction journey (IJ) includes key concepts needed to represent the stages and processes of the passenger journey in a smart airport.	Applicability
Q3	The Privacy Risk Assessment (PRA) represents an appropriate process to assess the privacy risks associated with passenger information in a smart airport.	Applicability
Q4	The Requirement includes concepts needed to influence the handling of passenger information during the journey and the risk assessment process.	Applicability

Table 5.16 Questionnaire set QS2-Understandability questions group

Question	Description	Evaluation criteria
Q1	IJPRA architecture is clear and easy to understand.	Understandability

Table 5.17 Questionnaire set QS3- Usefulness questions group

Question	Description	Evaluation criteria
Q1	IJPRA architecture is useful for privacy architects.	Usefulness
Q2	IJPRA architecture is useful for privacy solution designers	Usefulness
Q3	IJPRA architecture is useful for researchers.	Usefulness

Table 5.18 Questionnaire set QS4- Generalisability question group

Question	Description	Evaluation criteria
Q1	IJPRA architecture can be used in another smart context	Generalisability

Table 5.19 Questionnaire set QS6- Overall question group

Question	Description	Evaluation criteria
Q1	On a scale of 1 to 5 (5 being the highest), please provide an overall rating for the IJPRA architecture.	Applicability, understandability, usefulness, generalisability

### 5.5.1.2 Qualitative data collection

The qualitative data sources are the subjective feedback collected from the open-ended questions in survey questionnaire set QS5 (see Appendix E). The questions in set QS5 elicit expert subjective feedback to determine if the IJPRA architecture meets the evaluation criteria (see Table 3.2) and is useful to fill the research gaps and address research questions (see Sections 1.2 and 1.3, in Chapter 1) . In addition, the questions in set QS5 elicit expert suggestions for improvement of the IJPRA architecture, which was used to improve the IJPRA framework, including both its components and to identify future work. Survey questionnaire set QS5 is presented in Table 5.20.

Table 5.20 Questionnaire set QS5- Subjective feedback

Question	Description
Q1	What aspects are useful or valuable about the IJPRA architecture?
Q2	What improvements, including modifications, additions, deletions, or any additional feedback, would you suggest for the IJPRA architecture?

### 5.5.2 Survey data analysis

The survey evaluation process comprises two phases:

- Survey quantitative evaluation: The participants' response ratings, presented in Table 3.3 in Chapter 3, are converted from qualitative to quantitative data (numerical values). The numbers are then plugged into statistical formulas (Equations 3.1- 3.3) to evaluate the survey outputs.
- Survey qualitative evaluation: The participants' subjective response is processed using the general hypothesis confirmation analysis technique (Runeson & Höst 2009)(Runeson & Höst 2009). The hypotheses are designed based on the evaluation criteria adopted from (Prat, Comyn-Wattiau & Akoka 2014) (see Table 3.2). Participants' feedback was cross-examined against the evaluation criteria via drawing out the occurrences of these criteria in the text. Tables are used to organise experts' feedback.

#### 5.5.2.1 Survey quantitative evaluation

The quantitative evaluation process has two sections:

- Categorical evaluation based on the data collected from sets QS1–QS4.
- Overall evaluation result based on the data collected from set QS6.

### a) Categorical evaluation

The categorical evaluation has five steps to evaluate the questionnaire sets QS1–QS4. The evaluation process for categorical data is as follows:

- Gather and map the ratings of the participant's responses to each question under each questionnaire set relevant to specific evaluation criteria (see Tables 5.15 to 5.18 ) into survey tables, labelled **CT[m]**.
- Plot the CT [m] tables into a bar chart of the data, labelled **CF[m]**.
- Calculate the FAA and PAA statistics for all CT [m] tables (see Equation 3.2 and 3.3) to determine if the IJPRA architecture meets the evaluation criteria.
  - FAA to find the sum of the participants' responses that were either average or strongly agreed to questions under the questionnaire set to determine if the IJPRA architecture satisfies the evaluation criteria relevant to the questionnaire set.
  - PAA to find the percentage of the participants' responses that were average or strongly agreed to questions under the questionnaire set to determine if the IJPRA architecture satisfies the evaluation criteria relevant to the questionnaire set.
- Group the ordinal (statistical) data from the rating tables CT[m] into the category rating table named **GT[m]** on the basis of the assessment items assessed in the questionnaire set.
- Calculate the goodness-of-fit Chi2 and p-value (see Equation 3.1) to determine whether the IJPRA satisfies the evaluation criteria (see Table 3.2):
  - goodness-of-fit Chi2 and p-value for each question (see Equation 3.1).

***H0 (null hypothesis):*** *There is no association between the IJPRA and the evaluation criteria.*

***H1 (alternative hypothesis):*** *The IJPRA satisfies the evaluation criteria.*

If  $p\text{-value} < \alpha$ , then  $H_0$  is rejected and  $H_1$  is accepted, meaning that the IJPRA satisfies the evaluation criteria (applicability, understandability, usefulness, generalisability) .

[If  $p\text{-value} < 0.000\epsilon$  ( $\epsilon$  being a small number), then the criterion is amended to:  $p < 0.001$ ].

*i. Applicability*

Table 5.21 IJPRA applicability survey rating (CT1)

	Asset (Q1)	Journey (Q2)	Privacy (Q3)	Requirement (Q4)	Row Total	Percentage
Strongly agree	13	14	7	9	43	30.71
Agree	19	18	19	23	79	56.43
Average	2	2	8	3	15	10.71
Disagree	1	1	1	0	3	2.14
Strongly disagree	0	0	0	0	0	0.00
Column Total	35	35	35	35	140	100.00

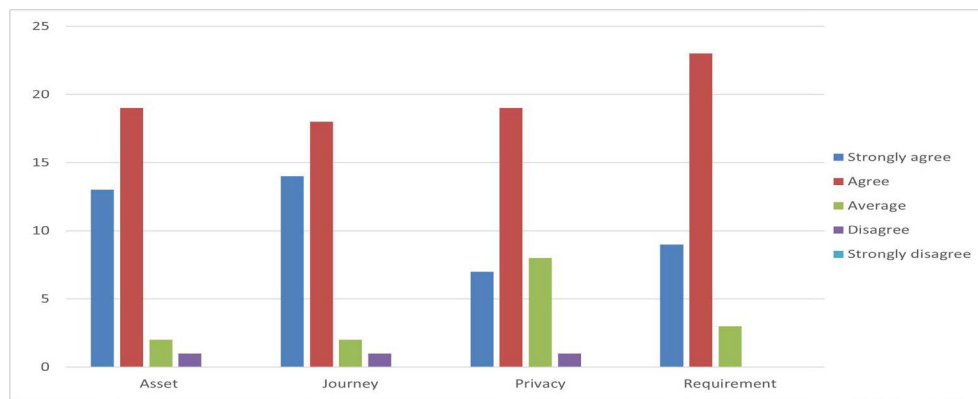


Figure 5.19 IJPRA applicability rating graph (CF1)

Table 5.22 IJPRA applicability category rating (GT1)

Assessment item									
	Asset (Q1)		Journey (Q2)		Privacy (Q3)		Requirement (Q4)		
<b>N=5</b> <b>E=∑O/N</b>	O	E	O	E	O	E	O	E	
Strongly agree	13	7	14	7	7	7	9	7	
Agree	19	7	18	7	19	7	23	7	
Average	2	7	2	7	8	7	3	7	
Disagree	1	7	1	7	1	7	0	7	
Strongly disagree	0	7	0	7	0	7	0	7	
<b>H0 is rejected for p &lt; 0.01</b>	<b>Chi² =41.429</b>	<b>P&lt;0.0001</b>	<b>Chi²=40.000</b>	<b>P&lt;0.0001</b>	<b>Chi²=32.857</b>	<b>P&lt;0.0001</b>	<b>Chi²=53.429</b>	<b>P&lt;0.0001</b>	

**Analysis**

Based on the numerical data in Tables 5.21 (CT1) and 5.22 (GT1), generating statistical values from participants' responses to questions Q1, Q2, Q3, Q4 under QS1, which was collected from 35 participants, the applicability evaluation result is interpreted as follows:

- FAA gives 137 out of 140 total responses from 35 participants indicating that a large majority of participants agree that the IJPRA architecture satisfies the applicability evaluation criteria (Figure 5.19).
- AAP equals 97.86% , indicating that a large percentage of participants agree that the IJPRA architecture satisfies the applicability evaluation criteria (Figure 5.19).
- The p-value for the assessment items:
  - Asset p-value is set at  $0.001 < \alpha=0.01$ , meaning H0 is rejected, H1 is accepted, which indicates that the asset under IJ in the IJPRA architecture satisfies the applicability evaluation criteria.
  - Journey p-value is set at  $0.001 < \alpha=0.01$ , meaning H0 is rejected, H1 is accepted, which indicates that the journey under IJ in the IJPRA architecture satisfies the applicability evaluation criteria.
  - Privacy p-value is set at  $0.001 < \alpha=0.01$ , meaning H0 is rejected, H1 is accepted, which indicates that the privacy risk assessment in the IJPRA architecture satisfies the applicability evaluation criteria.
  - Requirement p-value is set at  $0.001 < \alpha=0.01$ , meaning H0 is rejected, H1 is accepted, which indicates that the requirement in the IJPRA architecture satisfies the applicability evaluation criteria

The statistical values indicate that the participants consider the IJPRA architecture applicable to represent key concepts relating to the passenger interaction journey in smart airports and key process to assess relevant privacy risk. Figure 5.19 illustrates the frequency of the participants' responses to provide further visual insight into the results.

### I. Understandability

Table 5.23 IJPRA understandability survey rating (CT2)

	Q1	Row Total	Percentage
Strongly agree	13	13	37.14
Agree	16	16	45.71
Average	5	5	14.29
Disagree	1	1	2.86
Strongly disagree	0	0	0.00
<b>Column Total</b>	<b>35</b>	<b>35</b>	<b>100%</b>

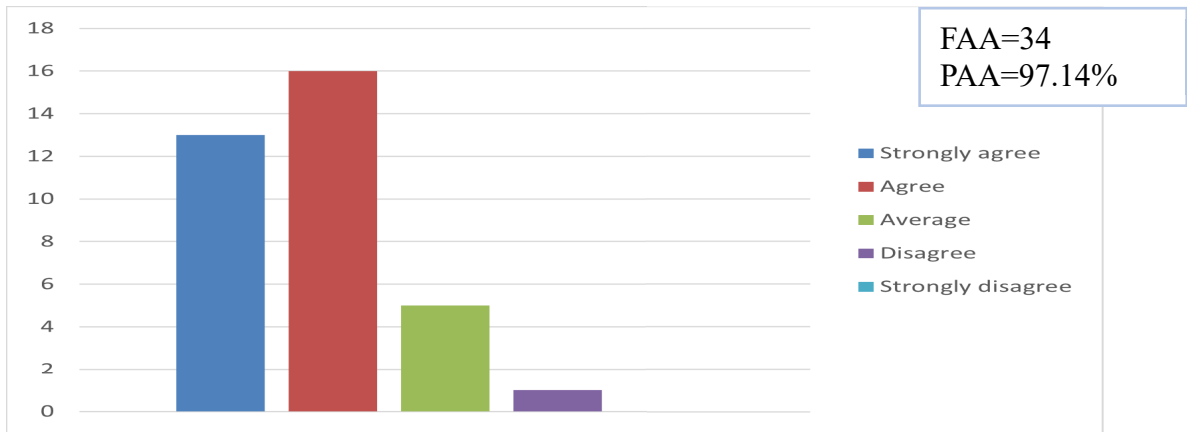


Figure 5.20 IJPRA understandability rating graph (CF 2)

Table 5.24 IJPRA understandability category rating (GT 2)

Assessment item		
	The whole IJPRA architecture	
<b>N=5</b> <b>E=ΣO/N</b>	O	E
Strongly agree	13	7
Agree	16	7
Average	5	7
Disagree	1	7
Strongly disagree	0	7
<b>H0 is rejected for</b> <b>p &lt; 0.01</b>	<b>Chi<sup>2</sup>=29.429</b>	<b>P&lt;0.001</b>

### Analysis

From the numerical data in Tables 5.23 CT2) and 5.24 (GT2), which generates key statistical values from the participants' responses to one question under QS2 for the understandability criteria, the understandability evaluation result is interpreted as follows:

- The FAA equals 34 out of 35 responses from 35 participants, indicating that the majority of participants agree that the IJPRA architecture satisfies the understandability evaluation criteria (Figure 5.20).
- PAA is 97.14%, indicating that a large percentage of participants agree that the IJPRA architecture satisfies the understandability evaluation criteria (Figure 5.20).
- The p-value for the assessment items:
  - understandability p-value is set at  $0.001 < \alpha=0.01$ , so H0 is rejected, H1 is accepted, which indicates that the IJPRA architecture meets the understandability evaluation criteria.

The statistical values indicate that the participants view the IJPRA architecture as clear and easy to understand. Figure 5.20 presents the frequency of the participants' responses to offer further visual insight into the results

## II. Usefulness

Table 5.25 IJPRA usefulness survey rating (CT3)

	Q1	Q2	Q3	Row Total	Percentage
Strongly agree	11	10	12	33	31.43
Agree	16	15	20	51	48.57
Average	7	9	3	19	18.10
Disagree	1	1	0	2	1.90
Strongly disagree	0	0	0	0	0.00
Column Total	35	35	35	105	100.00

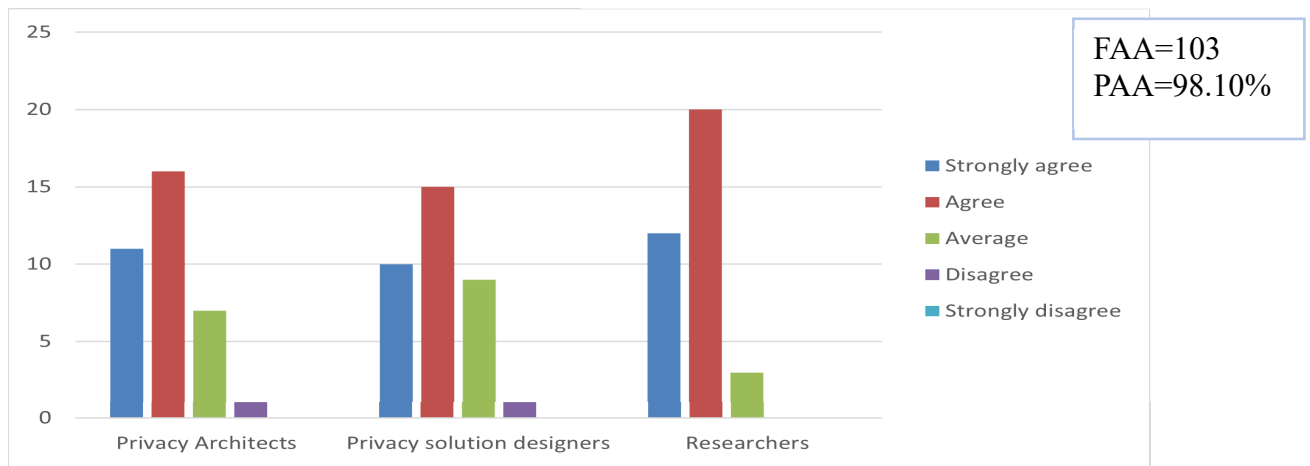


Figure 5.21 IJPRA Usefulness Rating Graph (CF3)

Table 5.26 IJPRA Usefulness category Rating (GT 3)

Assessment Item						
	Privacy architects		Privacy solution designers		Researcher	
N=5 E=ΣO/N	O	E	O	E	O	E
Strongly agree	11	7	10	7	12	7
Agree	16	7	15	7	20	7
Average	7	7	9	7	3	7
Disagree	1	7	1	7	0	7
Strongly disagree	0	7	0	7	0	7
<b>H0 is rejected for p &lt; 0.01</b>	<b>Chi²=26</b>	<b>P&lt;0.0001</b>	<b>Chi²=23.143</b>	<b>P&lt;0.001</b>	<b>Chi²=44</b>	<b>P&lt;0.0001</b>



## Analysis

From the numerical data in Tables 5.25 (CT3) and 5.26 (GT3), which generates key statistical values from the participants' responses to three questions under QS3 relevant to the usefulness criteria, the usefulness evaluation result is interpreted as follows:

- FAA gives 103 out of 105 responses from 35 participants indicating that the majority of participants agree that the IJPRA architecture satisfies the usefulness evaluation criteria.
- PAA is 98.10% which indicates that a large percentage of participants agree that the IJPRA architecture satisfies the usefulness evaluation criteria.
- The p-value for the assessment items:
  - Privacy architects' p-value is set at  $0.001 < \alpha=0.01$ , meaning H0 is rejected, H1 is accepted, which indicates that the IJPRA architecture satisfies the usefulness evaluation criteria (in regard to usefulness for privacy architects).
  - Privacy solution designer p-value is set at  $0.001 < \alpha=0.01$ , so H0 is rejected, H1 is accepted, which indicates that the IJPRA architecture satisfies the usefulness evaluation criteria (in regard to usefulness for privacy solution designers).
  - Researcher p-value is set at  $0.001 < \alpha=0.01$ , meaning H0 is rejected, H1 is accepted, which indicates that the IJPRA architecture satisfies the usefulness evaluation criteria (in regard to usefulness for researchers).

The statistical values indicate that the participants' view the IJPRA architecture as useful for privacy architects, privacy solution designers, and researchers. Figure 5.21 shows the frequency of the participants' responses to give more graphic detail of the results.

### III. Generalisability

Table 5.27 IJPRA generalisability survey rating (CT4)

	Q1	Row Total	Percentage
Strongly agree	11	11	11
Agree	18	18	18
Average	3	3	3
Disagree	3	3	3
Strongly disagree	0	0	0
<b>Column Total</b>	<b>35</b>	<b>35</b>	<b>100%</b>

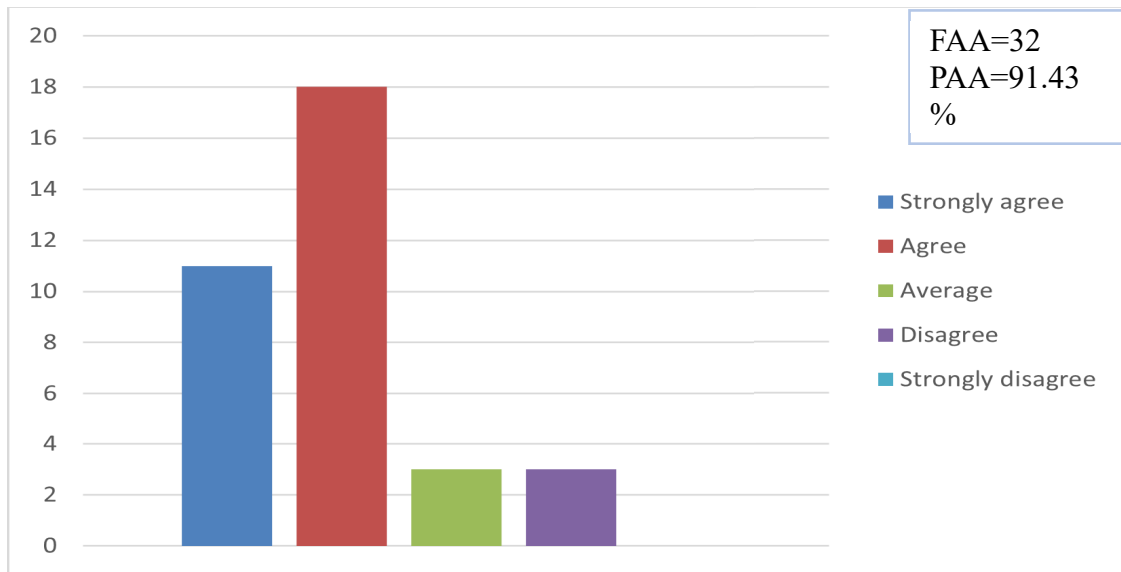


Figure 5.22 IJPRA Generalisability rating (CF 4)

Table 5.28 IJPRA Generalisability category rating (GT 4)

Assessment item		
	The whole IJPRA architecture	
N=5 E=ΣO/N	O	E
Strongly agree	11	7
Agree	18	7
Average	3	7
Disagree	3	7
Strongly disagree	0	7
<b>H0 is rejected for p &lt; 0.01</b>	<b>Chi<sup>2</sup>=31.143</b>	<b>P&lt;0.0001</b>

### Analysis

From the numerical data in Tables 5.27 (CT4) and 5.28 (GT4), which generates key statistical values from the participants' responses to one question under QS4 relevant to the generalisability criteria, the Generalisability evaluation results are as follows:

- FAA equals 32 out of 35 responses from 35 participants, indicating that a large percentage of participants agree that the IJPRA architecture satisfies the generalisability evaluation criteria.
- PAA is 91.43%, indicating that a large percentage of participants agree that the IJPRA architecture satisfies the generalisability evaluation criteria.
- The p-value for the assessment items:

- Generalisability p-value is set at  $0.001 < \alpha=0.01$ , meaning  $H_0$  is rejected,  $H_1$  is accepted, which indicates that the IJPRA architecture meets the generalisability evaluation criteria.

The statistical values indicate that the participants consider the IJPRA architecture to be general and able to fit different smart environments or contexts. Figure 5.22 illustrates the frequency of the participants' responses to give further visual insight into the results.

### b) Overall evaluation

This section evaluates the participants' overall ratings of the IJPRA architecture. The evaluation process is as follows:

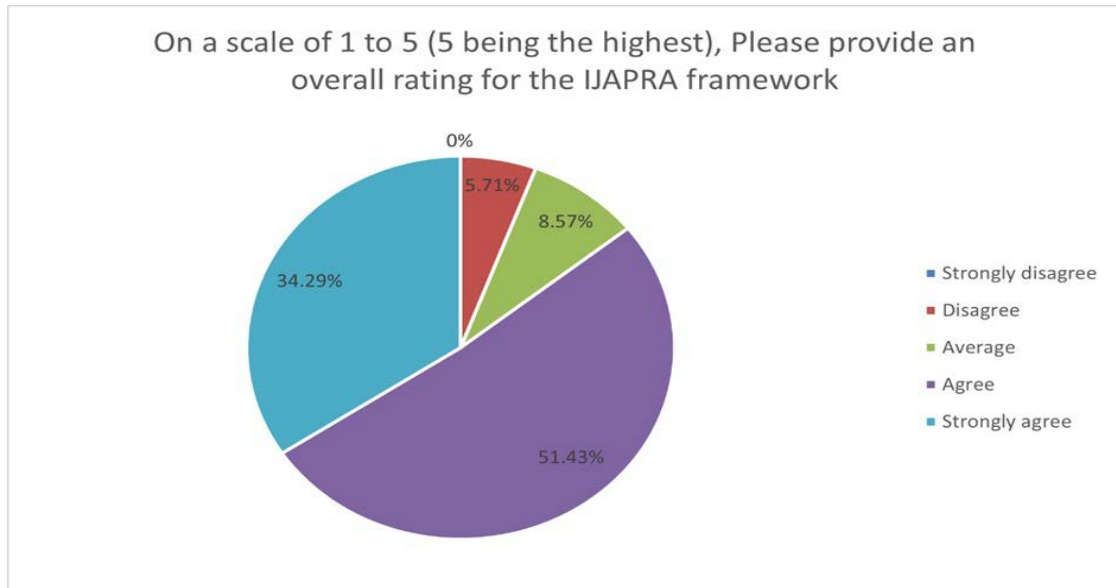
- Collect IJPRA overall ratings and map them as numerical data, as shown in Table 5.29, labelled ORT 1.
- Plot Table 5.29 (ORT 1) data into a bar chart representation, as shown in Figure 5.23, labelled ORF 1.
- Calculate the statistical values FAA and PAA for ratings of “average” and above from Table 5.29 (ORT 1) data (see Equation 3.2 and Equation 3.3)
  - FAA indicates the percentage of participants satisfied with the IJPRA overall.
  - PAA indicates the percentage of participants satisfied with the IJPRA overall.

Table 5.29 Overall IJAPRA framework rating (ORT 1)

<b>On a scale of 1 to 5 (5 being the highest), please provide an overall rating for the IJAPRA framework</b>		
<b>Rating</b>	<b>Frequency</b>	<b>Percentage</b>
Strongly disagree	0	0%
Disagree	2	5.71%
Average	3	8.57%
Agree	18	51.43%
Strongly agree	12	34.29%
Total	35	100.00%

Overall FAA=33

Overall PAA=94.29%



*Figure 5.23 Overall IJPRA architecture overall rating Graph (ORF 1)*

### **Analysis**

From the numerical data in Table 5.29 - statistical values based on 35 participants who responded to one question in QS6 - the overall rating indicates that:

- PAA is 94.29%, indicating that a high percentage of participants agree that the IJPRA architecture satisfies the evaluation criteria (applicability, understandability, usefulness, generalisability). Figure 5.23 presents the percentages of the participants' responses to aid the visualisation of the results.
- FAA gives a value of 33 (Figure 5.23), indicating that the majority of participants agree that the IJPRA architecture satisfies the evaluation criteria (applicability, comprehensibility, usefulness, generalisability).

#### *5.5.2.2 Survey qualitative evaluation (subjective evaluation)*

This section presents the qualitative analysis of questionnaire set Q5, which contains open-ended questions to gather participants' subjective feedback with the aim of determining the usefulness and applicability of the IJPRA architecture in the IJAPRA framework, as well as summarises the suggestions which include improvements, additions, and deletions suggested for the IJPRA architecture, provided by the experts. The participants' suggestions have been addressed by the researcher and are reflected in the updated IJAPRA framework gamma version discussed in Chapter 4.

The qualitative evaluation is grouped into the following categories:

- IJPRA overall subjective feedback (for filling the research gaps)
- Suggested changes (improvements, additions, and deletions) and responses to them.

### a) IJPRA architecture overall subjective feedback

This section analyses the participants’ responses to Q1 in QS6 to obtain their subjective feedback on the IJPRA architecture. This feedback was analysed to measure the applicability, understandability, Generalisability, as well as the usefulness of the IJPRA architecture in addressing the research gaps and research questions (see Table 3.2). The evaluation process is as follows:

- Collect and map the subjective feedback on IJPRA, collected from 35 participants who responded to Q1 in the QS5, in Table 5.30, labelled ST1.
- Analyse the feedback that is mapped in Table 5.30 (ST1) in light of the occurrences of the evaluation criteria, including applicability, usefulness, understandability, generalisability (see Table 3.2) in the responses using the cross-examination method (see Section 3.5.4, Chapter 3).
- Calculate the frequency and percentage of the appearance of each criteria in the participants’ responses.

Table 5.30 Subjective feedback on IJPRA (ST1)

	Participant’s comment (What aspects of the IJPRA framework are useful or valuable?)	Criteria			
		Applicability	Understandability	Usefulness	Generalisability
1	“ <b>All aspects</b> overall”	☐	☐	☐	☐
2	“The part of asset, you mostly <b>cover</b> all asset related to this framework”	☐		☐	
3	“The <b>interaction between components</b> of the framework and the <b>risk assessment process</b> ”	☐		☐	
4	“The interaction journey is really <b>appealing</b> ”	☐	☐	☐	☐
5	“This is an <b>excellent framework</b> and would be good if there is a unified framework that can be implemented in all airport operations. “	☐	☐	☐	☐
6	“It <b>helps</b> in <b>determining</b> the limits and boundaries of			☐	

	Participant's comment (What aspects of the IJAPRA framework are useful or valuable?)	Criteria			
		Applicability	Understandability	Usefulness	Generalisability
	privacy”				
7	“PRA”			☐	
8	“ <b>Key concepts</b> of passenger travel journey in smart airport, including actors, information, process, technology, journey stages, and concerns that arise during the journey”	☐		☐	
9	“The risk assessment framework”			☐	
10	“It provides a <b>holistic perspective</b> of a process”	☐		☐	
11	“The framework <b>provides</b> a foundation based on <b>which smart and AI enabled services</b> can be designed factoring in the <b>compliance and regulatory requirements</b> alongside privacy risks”	☐		☐	
12	“The framework <b>contextualises</b> the information lifecycle in the airport journey”	☐		☐	
13	“Simple to <b>understand</b> ”		☐		
14	“The interaction between framework component is insightful for me! how you capture the components interaction. Also, for the privacy risk assessment part”	☐	☐	☐	
15	“Easy to be understood”		☐		
16	“The IJAPRA Framework <b>helps</b> guide key decision points about 1. <b>Interaction journey (IJ)</b> , 2. <b>Privacy risk assessment (PRA)</b> , The Framework	☐	☐	☐	☐

	Participant's comment (What aspects of the IJAPRA framework are useful or valuable?)	Criteria			
		Applicability	Understandability	Usefulness	Generalisability
	<b>provides a common language</b> and systematic methodology for managing IJAPRA. The Framework is <b>designed to complement</b> existing business and Information Security & Privacy Risk operations, and can be used to for different purposes”				
17	“Applicability”	☐			
18	“In general, whenever anything is defined -> that by itself is an added value because it <b>allows</b> stakeholders to really <b>understand</b> what is happening. Specifically, with the IJAPRA framework, one can understand the interactions happening while highlighting the separation between different phases -> <b>allowing</b> a clear and more concentrated risk assessment”	☐	☐	☐	
19	“ <b>Provides</b> a high-level overview of the <b>entities and actors</b> involved in the privacy risk assessment process”	☐		☐	
20	“1. Easy to understand 2. Easy to follow up”		☐	☐	
21	“The breakdown of the <b>components</b> and sub-components of the IJAPRA framework is encompassing”	☐		☐	
22	“Assets and journey seem to <b>cover the domain well</b> . Requirements also seems to <b>cover most aspects and can be</b>	☐		☐	

	Participant's comment (What aspects of the IJAPRA framework are useful or valuable?)	Criteria			
		Applicability	Understandability	Usefulness	Generalisability
	<b>extendable</b> for any further future requirements”				
23	“That is looking for <b>overall aspects</b> from a Security and privacy point of view”	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
24	“These days, private and public organizations that process PII must comply with personal data regulations as GDPR is becoming a risk. By developing a <b>framework</b> for smart cities and airports, the risks that airports share every minute would be <b>mitigated</b> ”	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	
25	“I understand that this framework tends to be applied for airports as it handles or deals with passengers' personal information, but however I see this framework is in <b>general useful</b> for privacy experts or professionals, it would be helpful in terms of <b>capturing</b> the idea of privacy processes”	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
26	“The IJAPRA Framework components <b>cover</b> the relevant areas of the passengers' journey. This is very <b>useful</b> as most of the time the passengers are not aware that somewhere along their journey, they assets and PII's can be compromised”	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	
27	“Risk identification and risk analysis”	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	
28	“ <b>The overall categorisation</b> of the	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	



	Participant's comment (What aspects of the IJAPRA framework are useful or valuable?)	Criteria			
		Applicability	Understandability	Usefulness	Generalisability
	<b>key components.</b> As a framework, shown at a high level, it does provide a <b>useful</b> overview. This is a good visualization and starting point for privacy professionals when conducting a statutory 'data protection impact assessment' under various laws such as the GDPR etc.”				
29	“Generalisability”				<input checked="" type="checkbox"/>
30	“Privacy risk assessment “	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	
31	“In this framework, privacy risks were <b>sufficiently managed</b> to <b>allow</b> the development of innovative services without compromising individual privacy”	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	
32	“It is an IJAPRA framework, not a prescriptive standard * <b>Common Language</b> * <b>Adaptable</b> * <b>Collaboration</b> Opportunities * <b>Ability to Demonstrate Due Care</b> * <b>Easily Maintain Compliance</b> The Framework can be <b>tailored to meet each Airport's needs</b> ”	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
33	“ <b>Great work</b> ”	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
34	“I believe it <b>covers the key components</b> , i.e., the Interaction Journey and what are the external influences to govern them. Anything I can think of I have found where it can fall/classified especially	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	

Participant's comment (What aspects of the IJAPRA framework are useful or valuable?)	Criteria			
	Applicability	Understandability	Usefulness	Generalisability
in the technology.”				
<b>Total</b>	<b>27</b>	<b>12</b>	<b>30</b>	<b>9</b>
<b>Percentage</b>	<b>79%</b>	<b>35%</b>	<b>88%</b>	<b>26%</b>

As shown in Table 5.30, 34 out of 35 participants responded to Q1 in QS5. There are 79 references to the evaluation criteria in the experts' responses as shown in Table 5.28. The results in Table 5.28 can be interpreted as follows: the participants consider the IJPR architecture useful (88%), applicable (79%), understandable (35%), and general (26%). Hence, the results indicate that the IJPR architecture is applicable to represent components and context relevant to the domain, and it is useful in addressing the research gaps and research questions in hand (see Chapter 1). The results also show that the participants seem to consider the IJPR architecture clear and easy to understand and to be general enough to fit other smart contexts.

#### b) Suggested changes and responses

This section analyses the participants' responses to Q2 in QS6 regarding their suggestions about the IJPR architecture, which include changes (improvements, additions, and deletions). The evaluation process is as follow:

- Collect the suggestions on the IJPR architecture from the participants who responded to Q2 in QS5 as shown in Table 5.31, labelled ST 2.
- Group the experts' suggestions into five categories based on the IJPR architecture items mentioned in the suggestions, as shown in Table 5.31 (ST 2). The categories include information, actor, journey, PRA, and requirement (Table 5.30 (ST 2)).
- Respond to the suggestions, as shown in Table 5.31 (ST 2).

The experts' suggestions were used to refine and improve the beta version of the IJPR architecture and IJPR ontology, the two components of IJAPRA framework, which resulted in the gamma version of the IJAPRA framework. The gamma version of the IJAPRA is discussed in Chapter 4 in this thesis.

Table 5.31 Participants' suggestions, their categories, and the responses (ST2)

Category	Suggestion changes	Response
Information	“Passenger Identifiable Information (PII) is considered a limited scope definition which	The IJAPRA framework has been updated in the gamma version (discussed in Chapter 4). This update is reflected in the IJPR ontology

Category	Suggestion changes	Response
	<p>mainly refers to laws in USA et al. Consider aligning the IJAPRA framework with broader definition such as 'Personal Data' under laws like the GDPR. This captures not just 'identifiable' information but also pseudonymous information. This is important in the concept of smart airports, and the aviation industry. For example, a 'PNR' on the face of it may not fall into the definition of 'PII' since it consists of six characters of letter/numbers, but under the EU definition of 'Personal Data' it most certainly relates to living individuals (i.e., data subjects). This is because the ability to turn those letters into a person is achievable using a GDS system (i.e., Sabre/Amadeus). This is similar to other technologies where a unique identifier is used, such as phones, AdTech industry et al.”</p>	<p>(Figure 4.10, Chapter 4), where a new concept called “Ppersonal_Information, was added as a sub- concept under the existing “Passenger_Information” concept. The definition of the new concept is given in Table 4.3. Additionally, the exciting relationship “TYPE_OF” was updated to establish a connection between the new concept “Ppersonal_Information” and existing “Information_Type” concept. This newly added concept was added to the gamma version of the IJPRA architecture, as shown in Figure 4.11 in Chapter 4.</p>
	<p>“Include 'Sensitive Data' category in the Passenger Information section of the IJAPRA framework. The aviation industry collects and processing sensitive data (or referred to as Special Category Information) for providing additional services such as oxygen tank, disability support (i.e., wheelchair) or even through the identification of religion (i.e., Kosher, Halal, Hindu meal). This information may also be used in the context of a smart airport to support in either moving the passenger or providing food/vouchers in the event of a delay or disruption. This will bring additional privacy risks which'll need to be considered.”</p>	<p>The “Information_Classification” concept was added to the IJPRA ontology beta version, the first component of the IJAPRA framework, based on the results of illustrative scenario 1 in the second iteration method (see Section 5.3.2). This concept represents the classification of the handled information based on its sensitivity level, such as confidential, public, private, or restricted. However, in response to this suggestion, the added concept in the ontology beta version was incorporated into the gamma version of the architecture (as shown in Figure 4.11).</p>

Category	Suggestion changes	Response
	<p>“It would be better if the framework includes the types of personal information which are PII, SPI, PHI, and PFI, if possible, this would help the researchers, staff, experts, etc. to understand what type of data is stored or processed and categorization.”</p>	<p>The “Information_Type” concept was added to the IJPRA ontology beta version, the first component of the IJAPRA framework, based on the results of illustrative scenario 1 in the second iteration (see Section 5.3.2). This concept represents several types of passenger personal information that are handled in each stage of their interaction journey, such as PII, medical information, financial information, and biometric data. However, in response to this suggestion, the added concept in the ontology beta version was incorporated into the gamma version of the architecture (as shown in Figure 4.11, Chapter 4).</p>
Actor	<p>“I would recommend you include large GDS providers as key actors. The IJAPRA framework and/or any smart airport projects that aim to utilise passenger data must include the GDS providers (i.e., Sabre, Amadeus and Travelport) into their calculation as a key service provider as well. These two companies make up the crucial systems of the vast majority of global airlines operating. The success of any framework or smart airport relies upon the successful integration and support of these companies.”</p> <p>“It would also be important to consider the role and responsibilities of each actor in the supply chain of providing smart airport services from Airlines, GDS, security, CCTV operators, IT support, employees/contractors, and cloud providers”</p>	<p>The “Organisation/SP” concept was added to the IJPRA ontology beta version, the first component of the IJAPRA framework, based on the results of illustrative scenario 2 in the second iteration (see Section 5.3.3). This concept represents service providers who offer several services for passengers and airlines, and government in a smart airport.</p> <p>In the IJPRA ontology alpha version, the actor was identified as a concept and defined as an individual and Organisation which interact with each other as per their role in the smart airport (see Table 5.2), which highlights the diverse roles that actors play in the journey. However, the IJPRA architecture was updated to represent that the actor has roles within the journey. This update is reflected in the gamma version of the IJPRA architecture (Figure 4.11, Chapter 4).</p>
Journey	<p>“In the case of travel, we should break down the life cycle of</p>	<p>The scope of this research is limited to the in-airport journey on the departure side. Thus,</p>

Category	Suggestion changes	Response
	<p>passenger from beginning to end. This can help us to identify potential privacy issues and develop solutions for them. The life cycle of a passenger is a journey that includes many different phases, from booking to arrival. The privacy framework should be comprehensive enough to cover the entire process from beginning to end”</p>	<p>this suggestion will be considered as a future research direction</p>
PRA	<p>“I would suggest there should be a regulations component in privacy risk assessment. regulations are very important part and reflect on design of solution specially in terms of privacy”</p>	<p>Privacy regulations are included as influencing factors under the requirement component of the IJPRA architecture beta version (see Figure 5.18). This component includes all influencing factors, including privacy regulations and standards and privacy requirements that influence and guide the interaction journey, privacy risk assessment, and the use and handling of private information. This component will provide essential guidance for the design of privacy-aware solutions that adhere to the privacy requirements and imposed by relevant privacy laws. However, mitigating the risk and solution design is out of the scope of this research.</p>
	<p>“The only addition is in relation to the privacy risk assessment - it would be great to assess the "necessity" and "proportionality" of the process and the data being collected. Is the data collected necessary and proportional to the processing being carried out?”</p>	<p>These concepts are addressed in the gamma version of the IJPRA architecture under the development of the privacy risk identification (PRIdentification) tool (discussed in Section 4.3.2, Chapter 4)</p>
	<p>“In Privacy Risk Assessment, the privacy control shall come after analysing the risks, because the control should be specified based on the risk rating.”</p>	<p>Privacy control is identified under the risk identification in both the IJPRA ontology and architecture beta version as per the scope of this research. The analysis of the identified privacy control is conducted under the risk mitigation activity in the risk assessment process. The scope of this research is limited to risk identification and analysis, whereas</p>

Category	Suggestion changes	Response
		risk mitigation is out of the scope of this research. Thus, this suggestion will be considered as a future research direction.
Requirement	“Including privacy requirements in the framework would be beneficial.”	Privacy regulations are included as influencing factors under the requirement component of the IJPRA architecture beta version (see Figure 5.18). However, to avoid any confusion between the component name requirement and the privacy requirement as the influencing factor under this component in the IJPRA architecture beta version, the architecture has been updated to rename the component as factor instead of requirement. This update is reflected in the gamma version of the IJPRA architecture (Figure 4.11, Chapter 4).
	“The requirement section should be the very first of everything, we cannot do any process for no reasons, if there is a requirement to be enforced then it should be the first so we can have a reason to follow the requirements.”	The IJPRA architecture has been updated to reposition the requirement (renamed factor) to the beginning of the IJPRA architecture. This update is reflected in the gamma version of the IJPRA architecture (Figure 4.11, Chapter 4).
	“Also, regarding the requirements, I suggest elaborating more into it. As, shall you be using it as a checklist to ensure compliance with regulation (compliance assessment in this phase ?) or conduct a gap analysis? prioritise requirements?”	In the IJAPRA framework, both components, the IJPRA ontology and IJPRA architecture, have the requirement (renamed factor in the gamma version of the framework) as an influencing factor that represents privacy laws relevant to the aviation industry. This law plays a vital role in influencing and guiding the interaction journey, privacy risk assessment, and the use and handling of passenger information. However, the scope of this research is limited to identifying and recognising factor as an influencing factor. Compliance assessment, gap analysis, and prioritise requirements are out of the scope of this research and will be identified as future research directions.

## 5.6 Summary

This chapter presented the alpha, beta, and gamma iterations of the IJAPRA framework evaluation process. The result of each evaluation process led to an updated version of the IJAPRA framework. The explanation of the alpha and beta versions of the IJAPRA was covered in this chapter, while the illustration of the IJAPRA gamma version was covered in Chapter 4. This chapter discussed the analysis of IJPRA ontology based on five scenarios. The results of the illustrative scenarios indicated the applicability of the IJAPRA in representing the domain. Finally, the expert evaluation method via field survey was discussed in this research. The survey evaluation results indicate that IJAPRA was applicable to represent the domain in hand and is useful for addressing the gaps in this research area. On the other hand, the novelty of the framework is derived from our previously published SLR (Alabsi & Gill 2021). The results in this publication revealed that existing research-based studies lack a systematic understanding of privacy risks in smart airport. The proposed IJAPRA framework, the main contribution in this research, addresses this gap, indication its novelty in bringing a new knowledge in this domain. The output of this research, its limitations, contributions and future research directions are discussed in Chapter 6.

## 6 Chapter 6: Discussion and Conclusion

This thesis investigated the passenger interaction journey and associated privacy risks relevant to passenger information in smart airport. Comprehensive reviews of existing studies revealed a lack of understanding and assessment of privacy risks in smart airport from passenger perspective. This thesis aims to address this issue by answering the following research question **“How to design the passenger interaction journey architecture and assess the associated information privacy risks in the context of the smart airport?”**. This research introduces the IJAPRA framework as a practical solution to the aforementioned research question. The proposed framework was developed employing DSR methods and was evaluated through illustrative scenarios and expert evaluations via field surveys. This evaluation ensured that the framework meet the predetermined evaluation criteria and adequately address the research questions in hand. This research is significant, addressing the pressing issue of information privacy due to the rising interest in smart airports. The IJAPRA framework has implication for practitioner, assisting them in identifying and analysing privacy risks relevant to passenger information in smart airport. In addition, it has implication for researchers by bringing a new knowledge and understanding of privacy risks in smart airport contributing to the fields of information privacy, digital environments, and architecture. The component of this research has been presented and reported in reviewed conference and journals, facilitating iterative improvement based on external feedback.

This chapter outlines the research journey that started in July 2019, followed by a discussion of the research output and insights, including the research questions, the adopted methodology, and a summary of the evaluation process and its results in Section 6.1. It also presents the research implications in Section 6.2. The contributions and publications are listed in Section 6.3. The limitations of the IJAPRA framework and future research directions are discussed based on the expert evaluation feedback in section 6.4. Finally, this chapter discusses the research internal and external validity in Section 6.5 and provides an overall summary and conclusions in Section 6.6.

### 6.1 Research journey and main output

This section provides a detailed overview of the research journey, discusses the research output, presents DSR as the adopted methodology, and summarises the evaluation process and results.



### 6.1.1 The research journey

As shown in Figure 6.1, the research journey commenced in the spring of 2019 and spanned four years. The research thesis is expected to be submitted for review at the beginning of the spring of 2023. The research journey began by conducting an initial review (Chapters 1 and 2) to understand the research domain, followed by two systematic literature reviews (SLRs) (see Chapter 2), which helped identify the research gaps and problems. The following research question was identified "**How to design the passenger interaction journey architecture and assess the associated information privacy risks in the context of the smart airport?**". This was further divided into three sub-questions, as discussed in Chapter 1. An appropriate research methodology was identified (see Chapter 3), and the suggested solution, the IJAPRA framework, was proposed to address the research questions. In the second stage of the journey, the initial version of the IJAPRA framework was developed based on the results of both SLR 1 and SLR 2 and by adopting relevant theoretical and practical lenses to guide the development process (see Table 4.2, Chapter 4). The alpha version was evaluated using predetermined evaluation methods and criteria (see Chapters 3 and 5). The evaluation results were used to update the alpha version of the framework to the beta version. Then, the beta version was evaluated, and the results, along with expert suggestions, led to the development of the gamma version of the IJAPRA framework discussed in Chapter 4 and future research directions were proposed in Chapter 6.

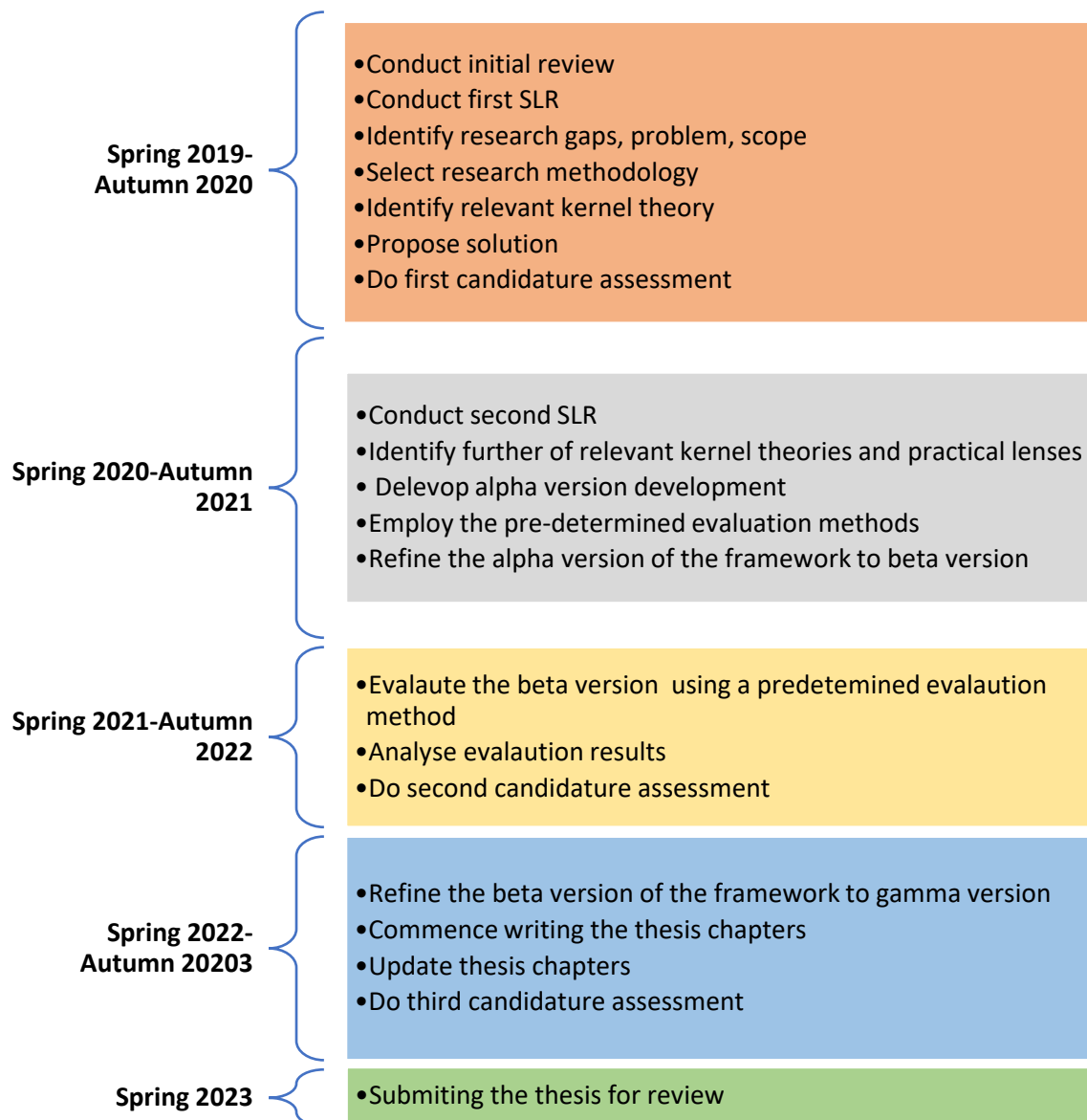
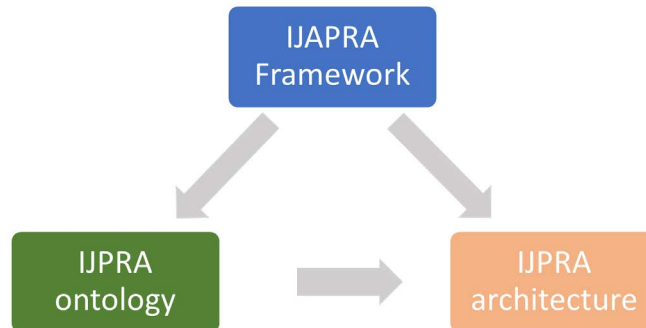


Figure 6.1 Research journey

### 6.1.2 Research output and insights

The main research output of this thesis is the IJAPRA framework, which assists in identifying and analysing the privacy risks associated with passenger information during their interaction journey in smart airports. The IJAPRA framework was constructed using the DSR method, as outlined in Chapter 3. The IJAPRA framework was incrementally developed and evaluated through three iterative processes using two predetermined DSR evaluation methods: illustrative scenario and expert evaluation via survey to measure the evaluation criteria identified in Chapter 3 (see Table 3.2). The results of each evaluation led to the development of the following framework versions: alpha, beta, and gamma. The gamma version of the IJAPRA framework was discussed in Chapter 4. The execution iteration processes, and evaluation

results are discussed in Chapter 5. The framework consists of two main components: the IJPRA ontology and the IJPRA architecture, as shown in Figure 4.1.



*Figure 4.1 (recalled) IJAPRA framework conceptual view*

In this research, the main research question is “**How to design the passenger interaction journey architecture and assess the associated information privacy risks in the context of the smart airport?**” This research question was divided into the following sub-questions:

RQ1: How to model the knowledge of the domain of privacy risk associated with passenger information during their interaction journey in a smart airport?

RQ2: How to design the passenger interaction journey architecture in a smart airport?

RQ3: How to assist in the assessment of privacy risks associated with passengers’ information during their interaction journey in a smart airport?

To address the research question and sub-questions, this research investigated the passenger interaction journey and associated privacy risks relevant to passenger personal information by developing the IJAPRA framework which consists of two components: IJPRA ontology and IJPRA architecture. The development of the IJPRA was based on relevant existing studies and was guided by the adopted theoretical and practical lenses along with expert feedback. Each framework component was developed to answer the research sub-questions as discussed in the following.

### *IJPRA ontology*

The ontology development answered the first research sub-question “**How to model the knowledge of the domain of privacy risk associated with passenger information during their interaction journey in a smart airport?**” The development of the IJPRA ontology gamma version is discussed in Chapter 4. The IJPRA ontology resulted from the integration of the IJ and PR ontologies (see Figure 4.2) developed prior to the integration process. The IJPRA ontology represents the knowledge of the domain of passenger interaction and associated privacy risks in smart airports. The IJPRA ontology can be utilised as a tool to conceptualise, analyse, and communicate privacy risks in smart airports. Table 6.1 details the mapping of the ontology output, description, and its location in the thesis.

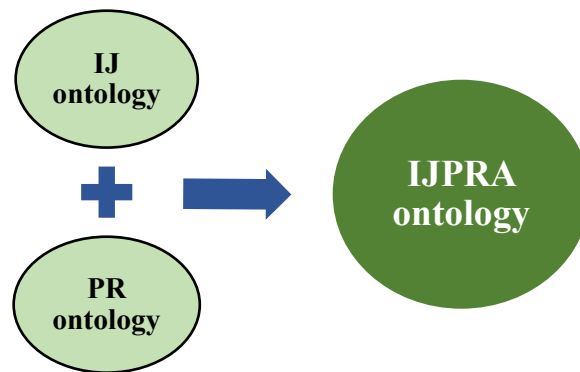


Figure 4.2 (recalled) IJPRA ontology conceptual view

Table 6.1 IJPRA ontology output

Ontology	Description	Source
IJ ontology	A total of 27 concepts and sub-concepts relevant to the passenger interaction journey in a smart airport are identified in the gamma version of the ontology. The IJ ontology captures the elements, primarily classified under actor, technology, process, information, and privacy-related legal factors, involved in the passenger interaction journey. The IJ ontology also identifies the relationships between these elements which provide insights into how these elements interact or relate to one another in the context of the passenger interaction journey. The IJ ontology is represented using a graph modelling approach implemented by the Neo4j graph database.	Chapter 4 Section 4.2.1 Table 4.3 Figures 4.3 and 4.4
PR ontology	The gamma version of the PR ontology identifies 16 concepts and their relevant relationships. The concepts capture the different types of privacy threats, which are classified based on the adopted theoretical lens, privacy requirements, and existing privacy controls. The primary focus of this ontology is the privacy risks that impact passenger personal information. The PR ontology offers a comprehensive coverage and structured understanding of the privacy risks associated with passenger	Chapter 4 Section 4.2.2 Table 4.5 Figures 4.5 and 5.6

Ontology	Description	Source
	information in a smart airport. Similar to the IJ ontology, PR is represented using a graph modelling approach implemented by the Neo4j graph database.	
IJPRA ontology	The gamma version of the IJPRA ontology includes the integration of the IJ and PR ontologies by identifying four concepts along with seven relationships produced to integrate PR and IJ ontologies. The structure of IJPRA includes concepts, relationships, and layers. The layer includes the organisation of the IJPRA concepts into (M0, M1, and M2) metamodel layers. The IJPRA ontology provides a comprehensive and systematic approach for identifying, communicating and analysing privacy risks, particularly those associated with passenger personal information in a smart airport. The IJPRA ontology is represented using a graph modeling approach implemented in the Neo4j graph database.	Chapter 4 Section 4.2.3 Tables 4.7 and 4.9 Figures 4.8, 4.9 and 4.10

### *IJPRA architecture*

The IJPRA architecture is the second component of the IJAPRA framework and comprises two main components: IJ and PR layers (see Figure 4.11). The IJPRA architecture was designed based on IJPRA concepts in the M2 and M1 metamodel layers. The gamma version of the architecture development is discussed in Chapter 4. The IJ layer answers the second research sub-question “**How to design the passenger interaction journey in a smart airport?**” by providing details of the assets involved in the interaction journey and the main journey stages and activities. The PR layer addresses the third research sub-question “**How to assist in the assessment of privacy risks associated with passengers’ information during their interaction journey in a smart airport?**” by providing tools to guide the risk assessment.

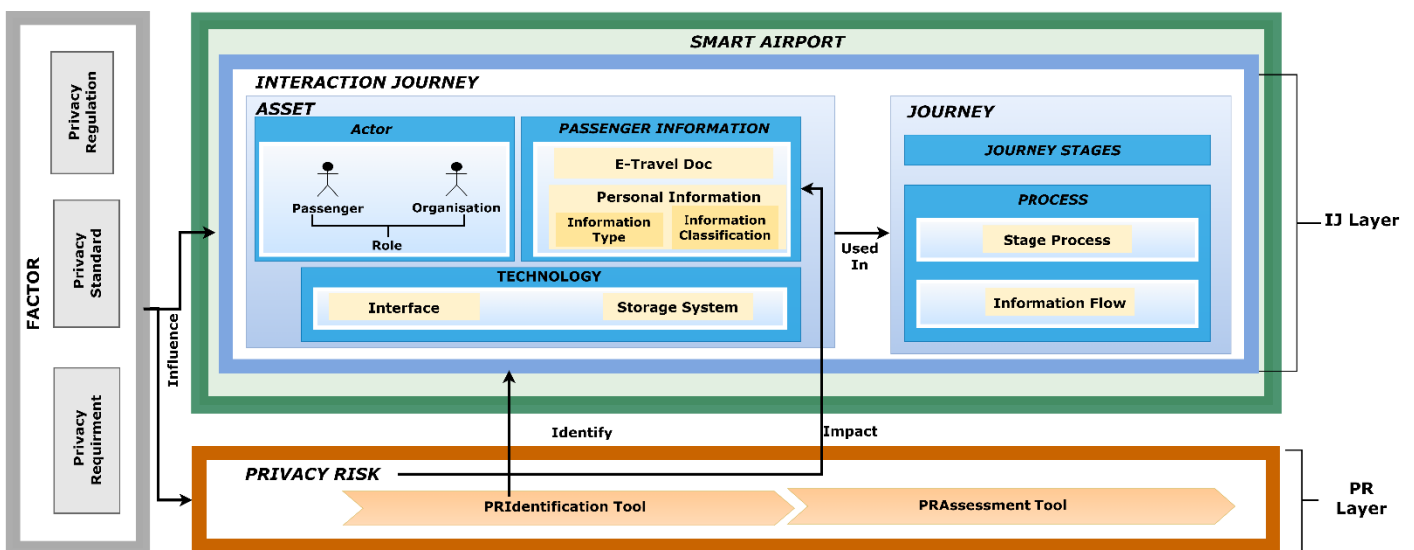


Figure 4.11 (recalled) IJPRA architecture conceptual view

Table 6.2 details the mapping of the architecture output, its description, and its location in the thesis.

*Table 6.2 IJPRA architecture output*

Architecture	Description	Source
IJ layer	This layer includes asset and journey components that are organised into the following views: IJ-actor, IJ-technology, IJ-process, IJ-information, and IJ-factor. These views provide details about the elements involved in the interaction journey to facilitate the identification of the associated privacy risks that arise during the interaction journey.	Chapter 4 Section 4.3.1 Figures 4.12-4.16
PR layer	This layer was introduced to guide in identifying and assessing the privacy risks associated with passenger information handled during the interaction journey. The layer includes two tools ( <b>PRIdentification</b> ) ( <b>PRAssessment</b> ). Each tool has specific inputs and outputs and provides a process that guide in privacy risk assessment.	Chapter 4 Section 4.3.2 Figures 4.17-4.20

By answering these research questions, this research seeks to guide the identification and analysis of privacy risks associated with passenger information in a smart airport which will help determine an appropriate decision for the risk. In addition, this research aims to provide new knowledge and an understanding of the privacy risks in smart airports.

This research adopted the DSR process derived from (Vaishnavi & Kuechler 2015) as presented in Figure 3.1. In addition, the DSR guidelines proposed by Hevner et al. (2004) were employed to assist in conducting and evaluating an effective DSR process, as discussed in Table 3.1. The steps of the adopted DSR research process applied in this research include awareness of the problem, suggestion, development, evaluation, and conclusion (see Section 3.5, Chapter 3). To obtain a solid background to the research topic and enable an understanding of the research context, a literature review was undertaken to cover the following topics: smart airport, personal information, privacy, ontology, and knowledge graph (Chapters 1 and 2). Following the review, two SLRs were conducted (Chapter 2), and their analysis and results helped identify the research gaps and develop the proposed framework. The IJPRA framework is the main contribution of this research, and DSR makes a verifiable contribution through its development and evaluation.

Two well-known DSR evaluation methods were used to evaluate the proposed IJPRA framework to determine whether it met the evaluation criteria (see Table 3.2). The evaluation methods were illustrative scenarios and expert evaluations through a field survey. To ensure

the validity of the research instruments, including the illustrative scenarios and field surveys, they were reviewed internally and externally with experts in the domain and updated based on the feedback received. These methods were implemented through three iterative processes, and each iteration was used to refine and develop a framework version: alpha, beta, and gamma.

In the first iteration, the alpha version of the framework was developed. This version was partially evaluated using an illustrative scenario to measure the applicability of IJ ontology in representing the domain. This evaluation iteration led to refining the IJ alpha version to the beta version, which included the three emerged concepts based on the evaluation results. Although this version of the framework was partially evaluated, it was still considered to be the alpha version. The beta version of the IJ ontology is able to capture the domain by including sufficient concepts and relationships that represent elements involved in the passenger interaction journey in a smart airport.

The second iteration involved the evaluation of the IJPRA ontology alpha version using five hypothetical scenarios representing different personas and privacy threats that might affect the information handled during the passenger interaction journey in a smart airport. The results of each scenario led to the refinement of the IJPRA ontology by including the emerged concepts based on the evaluation results. This assisted in improving the IJPRA ontology alpha version to the beta version. The IJPRA ontology beta version was able to provide sufficient concepts and relationships to represent and capture the information and risks in the evaluation scenarios relevant to privacy risk analysis and assessment.

The third iteration involved the evolution of the IJPRA architecture beta version, the second component of the framework, using expert evaluation via field survey. The survey was anonymous, as outlined in the online survey information sheet (Appendix D). The field survey used in this research employed a common survey design proposed by Hyndman (2008). The survey was distributed via LinkedIn and email to 230 experts in the field of information privacy/security and data protection, with a minimum of three years of experience (see Table 5.13). Of the 230 distributed surveys, 35 surveys were completed, and the responses were analysed. According to the existing research that utilised the expert evaluation method (Albladi & Weir 2018; Almaliki et al. 2014), it has been established that a sample size of 35 participants is appropriate for evaluating the proposed framework. Furthermore, this number ensures a diverse range of expert opinions, enhances the validity of the evaluation results, and provides comprehensive feedback for refinement. The survey included qualitative and quantitative data

collected from closed- and open-ended questions. The survey evaluation process consisted of two phases: quantitative and qualitative.

The quantitative evaluation process included the following sections: categorical and overall evaluations, which were used to collect rating data from closed-ended questions in the questionnaire sets QS1, QS2, QS3, QS4, and QS6 (see Section 5.5.2, Chapter 5). The collected ratings were mapped as numerical data to the results in Tables 5.21 -5.28 (see Chapter 5) based on the statistical values produced from calculating the PAA, FAA, and Chi2 p-value (see Equations 3.1–3.3, Chapter 3). The results were used to determine whether the IJPRA architecture satisfied the evaluation criteria (see Table 3.2). As shown in Table 5.21 and Table 5.22, PAA =97.86% and p-value < 0.01. These results indicate that the participants agree that the IJPRA is applicable for representing the key concepts related to the passenger interaction journey and risk assessment process in a smart airport. As shown in Tables 5.25 and 5.26, PAA=98.10% and p-value<0.01, which indicates that the participants considered IJPRA useful for privacy experts and researchers.

The qualitative evaluation process collected subjective feedback from participants and analysed it to evolve the IJAPRA framework to the gamma version and to identify the directions for future work. The qualitative evaluation process collected subjective data from open-ended questions in questionnaire set QS5 (see Chapter 5). The collected data were mapped and analysed in Tables 5.30 and Table 5.31. As shown in Table 5.30, there were 30 (88%) related references to the usefulness evaluation criteria in the participants' responses, indicating that the IJPRA is useful for addressing research gaps (see Section 1.2.1, Chapter 1).

In summary, based on the evaluation results from the illustrative scenarios and survey, it appears that the proposed IJAPRA framework is able to represent the domain in this research, it is useful for privacy experts and researchers, it is able to fill the research gaps, and privacy experts find it easy and clear to understand. Furthermore, based on our published SLR (Alabsi & Gill 2021), the existing studies lack a systematic and common understanding of the privacy risks associated with personal passenger information in the context of smart airports. Thus, the proposed IJAPRA framework demonstrates its novelty by addressing the aforementioned research gaps and creating new knowledge in this area. The ontology developed in this thesis has also been accepted in a highly ranked conference as a novel contribution (Alabsi, Gill, and Bandara, forthcoming).



## 6.2 Implications

The IJAPRA framework proposed in this research addresses the research questions outlined in Chapter 1 (see Section 1.3) and fills the research gaps identified in Chapter 1 (Section 1.2.1). In particular, IJAPRA focuses on understanding, identifying, and analysing the privacy risks which impact passengers' personal information which are handled during their interaction journey in a smart airport. In this section, the implications for the practice and research of IJAPRA are discussed.

### 6.2.1 Implications for practice

This research addresses information privacy concerns by developing a research-based practical IJAPRA framework. In this sense, the practical implications of this research are as follows.

- The IJAPRA framework can help address the current inadequate understanding of the elements involved in the passenger interaction journey. This includes actors, technologies, processes, and passenger information. The feedback from experts in the field survey supports this implication. For example, some experts' comments were "The interaction journey is really appealing," "Assets and journey seem to cover the domain well", and "The part of asset, you mostly cover all asset related to this framework".
- The IJAPRA framework can assist privacy experts in identifying the different types of privacy threats that cause the risk of information disclosure, which may affect passenger information in smart airports.
- The IJAPRA can be used as a tool to assist in analysing privacy risks and determining the level of overall risk to determine the appropriate response. Expert feedback from the survey support this, with one respondent noting, "I see this framework is in general useful for privacy experts or professionals, it would be helpful in terms of capturing the idea of privacy processes".
- The IJAPRA ontology component of the IJAPRA framework can be used as a tool to conceptualise and communicate the privacy risks, passenger information, and the elements involved in the passenger interaction journey in a smart airport.
- In accordance with the Saudi Vision 2030, this research can assist authorities and agencies in Saudi Arabia to better understand the privacy risks associated with passengers' personal information, which will contribute to the improvement of regulations and policies related to information privacy and governance in light of the digital transformation in several sectors, including airports. This contributes to achieving

the goals of Vision 2030, which seeks to deliver a better experience to individuals while ensuring the privacy of their information.

### 6.2.2 Implications for the research

This research applied several relevant theoretical lenses, including but not limited to Customer CJM , AEA, and CFIP (see Table 4.2), and a well-known DSR method developing for a theoretically sound framework, which was then evaluated using the illustrative scenarios and expert survey. The research resulted were also reported via a conference and journal paper with a view to get feedback from research community. These have contributed to the growing body of knowledge around information privacy and digital ecosystems or environment. The research implications are as follows.

- The IJAPRA provides a practical research-based framework for privacy risk assessment.
- This research provides new knowledge and an understanding of the privacy risks associated with passenger information in a smart airport. The conducted SLR in this research revealed a gap in understanding privacy risks in smart airport context in existing studies(Alabsi & Gill 2021).This understanding contributes to the body of knowledge in information privacy management, digital environments, and architecture fields.
- The evaluation of the IJAPRA framework underwent three iterations utilising two widely recognised DSR evaluation methods: illustrative scenarios and expert evaluation through a field survey. The development and documentation of the illustrative scenario evaluation method are discussed in Chapter 3. The methodology for developing and documenting scenarios in this research was proposed based on a review of the existing scenario development techniques in academic and industry fields. As there is currently a lack of research-based approaches for scenario development and documentation (do Prado Leite et al. 2000; Mahmoud et al. 2009) , researchers may employ the methodology proposed in this research to develop and document scenarios in various fields.

### 6.3 Key contributions and publications

The IJAPRA framework discussed in Chapter 4 was evaluated using two evaluation methods, as discussed in Chapter 5. The evaluation methods were used to determine whether the IJAPRA met the predetermined evaluation criteria outlined in Table 3.2 in Chapter 3. Publications in

conference and journal contributed to the development of the IJAPRA framework. Table 6.3 presents the key contributions of this research.

Table 6.3 Key contributions of this thesis

Contribution	Reference	Source
IJAPRA framework	The main contribution of this research is the construction of the IJAPRA framework to assist in identifying and analysing the privacy risks associated with passenger information in a smart airport.	Thesis output Chapter 4 Chapter 5 Section 6.1.2 in Chapter 6
Journal	ALABSI, M. I. & GILL, A. Q. 2021. A Review of Passenger Digital Information Privacy Concerns in Smart Airports. <i>IEEE Access</i> , 9, 33769-33781.	IEEE access
Journal (In review)	<b>Title: “A systematic review of personal information sharing in smart cities: risks, impacts, and controls”</b>  <b>Authors:</b> ALABSI & GILL <b>Journal homepage:</b> <a href="http://www.springer.com">Journal of the Knowledge Economy   Home (springer.com)</a>	Springer
Conference (Accepted)	<b>Title: Integrated Interaction Journey and Privacy Risk Assessment: A Graph Model</b>  <b>Authors:</b> ALABSI, GILL, and Bandara. <b>Conference homepage:</b> <a href="https://centeris.scika.org/">https://centeris.scika.org/</a>	CENTERIS

#### 6.4 Limitations and future work

The IJAPRA framework in this thesis has been evaluated using illustrative scenarios (see Chapter 5) and assessed by experts using survey questionnaires, as discussed in Chapter 5. The ontology component of the IJAPRA framework was peer-reviewed at a well-known conference (Alabsi, Gill, and Bandara, forthcoming). Although the aforementioned research contributions are noteworthy, there are still limitations in the current version of the IJAPRA framework that can guide future work, discussed as follows.

- The time constraint of the Ph.D. program limited the researcher's ability to spend more time investigating additional issues in the field. While significant progress was made in the understanding of information privacy concerns in smart airports, there are potential areas that might have been explored further with more time. This involves further investigation into the implication of utilising other technologies, such as mobile applications, in passenger journey within smart airports, on information privacy. This

will offer a comprehensive understanding of information privacy concerns. Nevertheless, the findings from this research lay a solid foundation for future studies and offer a starting point for researchers to explore more relevant concerns.

- The research may have potential methodological limitations due to the field survey recruitment method and sample size (see Section 3.7, Chapter 3). Participants, mainly recruited from LinkedIn, were limited to 35 due to time constraints. This number is adequate for evaluating the proposed framework as several studies utilised the same evaluation approach with a similar sample size (Albladi & Weir 2018; Almaliki et al. 2014). However, expanding the sample size by including additional experts to enhance the research robustness can be considered as future research directions. Another limitation is that the survey utilised closed-ended questions with predetermined choices, potentially limiting responses to current options. However, open-ended questions were included for subjective feedback, aiming to capture insights beyond predefined options. In addition, the survey employed a combination of qualitative and quantitative data analysis for a comprehensive understanding of the results.
- Five Illustrative scenarios were used as evaluation method along with field survey to further enhance the current research findings. In future research, more scenarios and case studies can be used for evaluation purposes to further strengthen the current findings.
- The scope of the study is limited to the passenger interaction journey on the departure side. This focused approach ensures depth in examining departure processes. However, more investigation is needed to understand the entire passenger experience, including the in-flight and arrival sides. This can be considered in future research, offering a more comprehensive understanding of passenger interactions across the entire air travel journey.
- The scope of this research is limited to identifying and analysing the privacy risks that impact passengers' personal information handled during their interaction journey. Risk mitigation, risk compliance, and gap analysis are beyond the scope of this research, limiting its ability to provide a comprehensive privacy management framework. These aspects could be explored in future research directions to establish a more holistic framework for privacy management in passenger interactions journey in smart airport.

## 6.5 Discussion of research validity

This section discusses the internal and external validity of this thesis, evaluating the robustness of the research design and the generalisability of the findings.

The main aim of this thesis is to develop the IJAPRA framework, addressing the main research question “How to design the passenger interaction journey architecture and assess the associated information privacy risks in the context of the smart airport?”, to fill the identified gap in existing studies that reveal a lack of understanding of privacy risks associated with passenger information in smart airports. The main research question was further divided into three sub-questions.

Concerning internal validity, the research questions were identified and evolved based on conducting two relevant SLRs to comprehensively explore the existing literature, both of which have undergone peer review and publication. As a result, the research questions are grounded in a solid foundation of peer-reviewed literature, contributing to the relevance of the proposed research objectives.

The IJAPRA framework was developed using the well-known DSR method, which served as an appropriate methodology providing a structured and systematic approach. This methodology assists and facilitates the development and evaluation of the construction of the IJAPRA framework in an iterative manner, relying on in kernel theories and existing knowledge (details of the validity of used methodology discussed in Chapter3, Section 3.7)

The proposed IJAPRA framework consists of two main components, including the IJPRA and the IJPRA architecture. The IJAPRA framework was developed to provide a practical solution to the research questions in hand. It is developed based on relevant existing studies, theoretical and practical lenses, and incorporates expert evaluation feedback to build and refine the IJAPRA.

In the process of developing and validating the research instruments, an iterative approach was employed. This involved continuous development and refinement of the instruments, with internal assessment by supervisors and external evaluation by domain experts and the feedback utilised to enhance the quality and relevance of the instruments, encompassing scenarios and a survey. Additionally, a pilot test involving three participants was conducted to assess the construction and relevance of the survey questionnaire. Based on the feedback received from the pilot study, the questionnaire was refined and improved.

The plausible external validity of the framework was examined by conducting five illustrative scenarios that represent various passenger persona types and the privacy risks that affect their information and privacy. In addition, a field survey involving experts in the field of information privacy/security and data protection was carried out to get their feedback and opinions on the proposed IJAPRA framework.

## 6.6 Conclusion and Summary

This thesis presented the IJAPRA framework that provides a practical solution to the privacy risks associated with passenger information in a smart airport. The IJAPRA was developed iteratively using the well-known DSR methodology. The IJAPRA framework is intended for use by privacy experts, including privacy architects, privacy solution designers, and researchers as a practical guide for identifying and assessing privacy risks in smart airports, which will help in designing the best privacy solutions relevant to passenger information in the smart airport. The IJAPRA framework consists of two components: IJPRA ontology and IJPRA architecture. IJAPRA provides new knowledge and an understanding of the privacy risks in smart airports. This thesis also presented research findings with significant implications for both the research community and practice. The IJAPRA framework will be extended in the future, based on further learning, research, and experience.

## Bibliography

- Abu-Salih, B. 2021, 'Domain-specific knowledge graphs: A survey', *Journal of Network and Computer Applications*, vol. 185, p. 103076.
- Agrawal, P.R. 2014, 'Digital Information Management: Preserving Tomorrow's Memory', *Cloud Computing and Virtualization Technologies in Libraries*, IGI Global, pp. 22-35.
- Agrawal, T.K., Kumar, V., Pal, R., Wang, L. & Chen, Y. 2021, 'Blockchain-based framework for supply chain traceability: A case example of textile and clothing industry', *Computers & industrial engineering*, vol. 154, p. 107130.
- Alabsi, M.I. & Gill, A.Q. 2021, 'A Review of Passenger Digital Information Privacy Concerns in Smart Airports', *IEEE Access*, vol. 9, pp. 33769-81.
- Alansari, Z., Soomro, S. & Belgaum, M.R. 2019, 'Smart Airports: Review and Open Research Issues', *Emerging Technologies in Computing*, Springer International Publishing, Cham, pp. 136-48.
- Albladi, S.M. & Weir, G.R. 2018, 'User characteristics that influence judgment of social engineering attacks in social networks', *Human-centric Computing and Information Sciences*, vol. 8, no. 1, pp. 1-24.
- Alghanim, A.A., Rahman, S.M.M. & Hossain, M.A. 2017, 'Privacy Analysis of Smart City Healthcare Services', *2017 IEEE International Symposium on Multimedia (ISM)*, pp. 394-8.
- Almaliki, M., Faniyi, F., Bahsoon, R., Phalp, K. & Ali, R. 2014, 'Requirements-driven social adaptation: Expert survey', *Requirements Engineering: Foundation for Software Quality: 20th International Working Conference, REFSQ 2014, Essen, Germany, April 7-10, 2014. Proceedings 20*, Springer, pp. 72-87.
- AlMashari, R., AlJurbua, G., AlHoshan, L., Al Saud, N.S., BinSaeed, O. & Nasser, N. 2018, 'IoT-based smart airport solution', *2018 International Conference on Smart Communications and Networking (SmartNets)*, IEEE, pp. 1-6.
- Alrumaih, H., Mirza, A. & Alsalamah, H. 2020, 'Domain ontology for requirements classification in requirements engineering context', *IEEE Access*, vol. 8, pp. 89899-908.
- Ambrose, M.L. 2012, 'It's about time: privacy, information life cycles, and the right to be forgotten', *Stan. Tech. L. Rev.*, vol. 16, p. 369.
- Ameller, D. & Franch, X. 2011, 'Ontology-based Architectural Knowledge representation: structural elements module', *Advanced Information Systems Engineering Workshops: CAISE 2011 International Workshops, London, UK, June 20-24, 2011. Proceedings 23*, Springer, pp. 296-301.
- Anand, A., Labati, R.D., Genovese, A., Munoz, E., Piuri, V., Scotti, F., Sforza, G. & Ieee 2017, 'Enhancing Fingerprint Biometrics in Automated Border Control with Adaptive Cohorts', paper presented to the Proceedings of 2016 Ieee Symposium Series on Computational Intelligence, Athens, Greece.
- Angles, R. 2018, 'The Property Graph Database Model', *AMW*.
- Angles, R., Arenas, M., Barceló, P., Hogan, A., Reutter, J. & Vrgoč, D. 2017, 'Foundations of modern query languages for graph databases', *ACM Computing Surveys (CSUR)*, vol. 50, no. 5, pp. 1-40.
- Anwar, M.J., Gill, A.Q. & Beydoun, G. 2019, 'Using adaptive enterprise architecture framework for defining the adaptable identity ecosystem architecture'.
- Anwar, M.J., Gill, A.Q., Hussain, F.K. & Imran, M. 2021, 'Secure big data ecosystem architecture: challenges and solutions', *EURASIP Journal on Wireless Communications and Networking*, vol. 2021, no. 1, p. 130.
- Australian Airport Association 2023
- PRIVACY POLICY, airports.asn.au, viewed 2 Jun 2020, <<https://airports.asn.au/wp-content/uploads/2023/05/May23-AAA-Privacy-Policy.pdf>>.

- Avanchar, S., Baxi, A. & Kotz, D. 2012, 'Privacy in mobile technology for personal healthcare', *ACM Computing Surveys (CSUR)*, vol. 45, no. 1, pp. 1-54.
- Ayoade, J. 2006, 'Security implications in RFID and authentication processing framework', *Computers & Security*, vol. 25, no. 3, pp. 207-12.
- Barev, T.J., Janson, A. & Leimeister, J.M. 2020, 'Designing Effective Privacy Nudges in Digital Environments: A Design Science Research Approach', *International Conference on Design Science Research in Information Systems and Technology*, Springer, pp. 388-93.
- Bart Willemsen, P.B. 2017, *The Four Do's and Don'ts of Implementing Your Privacy Program*, Gartner.
- Bebee, B.R., Choi, D., Gupta, A., Gutmans, A., Khandelwal, A., Kiran, Y., Mallidi, S., McGaughy, B., Personick, M. & Rajan, K. 2018, 'Amazon Neptune: Graph Data Management in the Cloud', *ISWC (P&D/Industry/BlueSky)*.
- Bélanger, F. & James, T.L. 2020, 'A theory of multilevel information privacy management for the digital era', *Information systems research*, vol. 31, no. 2, pp. 510-36.
- Bellomarini, L., Fakhoury, D., Gottlob, G. & Sallinger, E. 2019, 'Knowledge graphs and enterprise AI: the promise of an enabling technology', *2019 IEEE 35th international conference on data engineering (ICDE)*, IEEE, pp. 26-37.
- Benbasat, I., Goldstein, D.K. & Mead, M. 1987, 'The case research strategy in studies of information systems', *MIS quarterly*, pp. 369-86.
- Bogicevic, V., Bujisic, M., Bilgihan, A., Yang, W. & Cobanoglu, C. 2017, 'The impact of traveler-focused airport technology on traveler satisfaction', *Technological Forecasting and Social Change*, vol. 123, pp. 351-61.
- Bou Ghantous, G. & Gill, A.Q. 2021, 'Evaluating the DevOps Reference Architecture for Multi-cloud IoT-Applications', *SN Computer Science*, vol. 2, no. 2, p. 123.
- Bouyakoub, S., Belkhir, A., Guebli, W. & Bouyakoub, F.M. 2017, 'Smart airport: An IoT-based Airport Management System', paper presented to the ICFNDS '17 International Conference on Future Networks and Distributed Systems, New York, NY, USA.
- Boyce, S. & Pahl, C. 2007, 'Developing domain ontologies for course content', *Journal of Educational Technology & Society*, vol. 10, no. 3, pp. 275-88.
- Brian Lowans, B.W., Marc-Antoine Meunier 2019, *Use the Data Security Governance Framework to Balance Business Needs and Risks*, Gartner.
- Brooks, S., Lefkowitz, M.G.N. & Nadeau, S.L.E. 2017, *An Introduction to Privacy Engineering and Risk Management in Federal Systems*.
- Buchgeher, G., Gabauer, D., Martinez-Gil, J. & Ehrlinger, L. 2021, 'Knowledge graphs in manufacturing and production: A systematic literature review', *IEEE Access*, vol. 9, pp. 55537-54.
- Burdon, M. 2020, *Digital data collection and information privacy law*, vol. 54, Cambridge University Press.
- Burdon, M. & Telford, P. 2010, 'The conceptual basis of personal information in Australian privacy law', *eLaw J.*, vol. 17, p. 1.
- Cano, J., Pollini, A., Falciani, L. & Turhan, U. 2016, 'Modeling current and emerging threats in the airport domain through adversarial risk analysis', *Journal of Risk Research*, vol. 19, no. 7, pp. 894-912.
- Chang-Ryung, H., McGauran, R. & Nelen, H. 2017, 'API and PNR data in use for border control authorities', *Security Journal*, vol. 30, no. 4, pp. 1045-63.
- Charmaz, K. 2006, *Constructing grounded theory: A practical guide through qualitative analysis*, sage.
- Chen, J.K., Batchuluun, A. & Batnasan, J. 2015, 'Services innovation impact to customer satisfaction and customer value enhancement in airport', *Technology in Society*, vol. 43, pp. 219-30.
- Chenthara, S., Khandakar, A. & Whittaker, F. 2019, 'Privacy-Preserving Data Sharing using Multi-layer Access Control Model in Electronic Health Environment', *EAI Endorsed Transactions on Scalable Information Systems*, vol. 6, no. 22.



- Choi, H.S., Lee, W.S. & Sohn, S.Y. 2017, 'Analyzing research trends in personal information privacy using topic modeling', *Computers & Security*, vol. 67, pp. 244-53.
- Chua, H.N., Herbland, A., Wong, S.F. & Chang, Y. 2017, 'Compliance to personal data protection principles: A study of how organizations frame privacy policy notices', *Telematics and Informatics*, vol. 34, no. 4, pp. 157-70.
- Chua, H.N., Ooi, J.S. & Herbland, A. 2021, 'The effects of different personal data categories on information privacy concern and disclosure', *Computers & security*, vol. 110, p. 102453.
- Chuleeporn, C. 2008, 'Threat, Authentication, and Privacy', vol. 4, no 2, Taylor & Francis, pp. 1-2.
- Chun, S.-H. 2015, 'Privacy Enhancing Technologies (PETs) and Investment Strategies for a Data Market', *Procedia-Social and Behavioral Sciences*, vol. 185, pp. 271-5.
- CnSight 2021, *Top 5 Cyber Attacks in the Aviation Industry*, CnSight, cnsight.io, <<https://cnsight.io/2021/04/16/top-5-cyber-attacks-in-the-aviation-industry/>>.
- Coghlan, D. & Shani, A. 2005, 'Roles, politics, and ethics in action research design', *Systemic Practice and Action Research*, vol. 18, no. 6, pp. 533-46.
- Coleman, L. 2018, *IATA predicts 8.2 billion annual travellers in 20-year forecast*, DFNI FRNTIER, dfnionline.com, viewed 15 Oct 2020, <[221](https://www.dfnionline.com/lead-stories/iata-predicts-8-2-billion-travellers-20-year-forecast-25-10-2018/#:~:text=The%20International%20Air%20Transport%20Association%20%28IATA%29%20has%20forecast,meaning%20traffic%20will%20reach%208.2%20billion%20by%202037.>.</a>>.</p>
<p>Corbin, J.M. 1990, <i>Basics of qualitative research: Grounded theory procedures and techniques</i>, Sage.</p>
<p>Corcoran, P.M. 2017, 'A privacy framework for the Internet of Things', Institute of Electrical and Electronics Engineers Inc., pp. 13-8.</p>
<p>Coughlan, P. & Coughlan, D. 2002, 'Action research for operations management', <i>International journal of operations & production management</i>.</p>
<p>Creswell, J.W. & Miller, D.L. 2000, 'Determining validity in qualitative inquiry', <i>Theory into practice</i>, vol. 39, no. 3, pp. 124-30.</p>
<p>Crotty, M.J. 1998, <i>The foundations of social research: Meaning and perspective in the research process</i>.</p>
<p>Cui, L., Xie, G., Qu, Y., Gao, L. & Yang, Y. 2018, 'Security and Privacy in Smart Cities: Challenges and Opportunities', <i>IEEE Access</i>, vol. 6, pp. 46134-45.</p>
<p>Curzon, J., Almeahadi, A. & El-Khatib, K. 2019, 'A survey of privacy enhancing technologies for smart cities', <i>Pervasive and Mobile Computing</i>, vol. 55, pp. 76-95.</p>
<p>Custodio, E. 2021, 'The Construction and Internal Validation of a Model for the Effective Collaboration of Distributed Agile Teams', Nova Southeastern University.</p>
<p>Cygniak, R., Wood, D., Lanthaler, M., Klyne, G., Carroll, J.J. & McBride, B. 2014, 'RDF 1.1 concepts and abstract syntax', <i>W3C recommendation</i>, vol. 25, no. 02, pp. 1-22.</p>
<p>Das, A., Mitra, A., Bhagat, S.N. & Paul, S. 2020, 'Issues and Concepts of Graph Database and a Comparative Analysis on list of Graph Database tools', <i>2020 International Conference on Computer Communication and Informatics (ICCCI)</i>, IEEE, pp. 1-6.</p>
<p>Davis, G.B. & Olson, M.H. 1999, 'Management information systems', <i>PMI (1996). A Guide to the Project Management Body of Knowledge. Upper Darby, PA: Project Management Institute, McGraw-Hill</i>.</p>
<p>Deng, M., Wuyts, K., Scandariato, R., Preneel, B. & Joosen, W. 2011, 'A privacy threat analysis framework: supporting the elicitation and fulfillment of privacy requirements', <i>Requirements Engineering</i>, vol. 16, no. 1, pp. 3-32.</p>
<p>Deutsch, A., Xu, Y., Wu, M. & Lee, V. 2019, 'Tigergraph: A native MPP graph database', <i>arXiv preprint arXiv:1901.08248</i>.</p>
<p>do Prado Leite, J.C.S., Hadad, G.D., Doorn, J.H. & Kaplan, G.N. 2000, 'A scenario construction process', <i>Requirements Engineering</i>, vol. 5, pp. 38-61.</p>
<p>Dumitriu, D. & Popescu, M.A.-M. 2020, 'Enterprise architecture framework design in IT management', <i>Procedia Manufacturing</i>, vol. 46, pp. 932-40.</p>
</div>
<div data-bbox=)

- Duncan, R., Eden, R., Woods, L., Wong, I. & Sullivan, C. 2022, 'Synthesizing Dimensions of Digital Maturity in Hospitals: Systematic Review', *Journal of medical Internet research*, vol. 24, no. 3, pp. e32994-e.
- Eckhoff, D. & Wagner, I. 2018, 'Privacy in the Smart City—Applications, Technologies, Challenges, and Solutions', *IEEE Communications Surveys & Tutorials*, vol. 20, no. 1, pp. 489-516.
- Ehrlinger, L. & Wöß, W. 2016, 'Towards a definition of knowledge graphs', *SEMANTICS (Posters, Demos, SuCCCESS)*, vol. 48, no. 1-4, p. 2.
- Elmaghraby, A.S. & Losavio, M.M. 2014, 'Cyber security challenges in Smart Cities: Safety, security and privacy', *J Adv Res*, vol. 5, no. 4, pp. 491-7.
- European Network and Information Security Agency (ENISA) 2010, *Flying 2.0: Enabling automated air travel by identifying and addressing the challenges of IoT and RFID technology*.
- European Union Agency for Network and Information Security 2016, *SECURING SMART AIRPORTS*.
- Fattah, A., Lock, H., Buller, W. & Kirby, S. 2009, *Smart Airports: Transforming Passenger Experience To Thrive in the New Economy*.
- Fensel, D., Şimşek, U., Angele, K., Huaman, E., Kärle, E., Panasiuk, O., Toma, I., Umbrich, J., Wahler, A. & Fensel, D. 2020, *Knowledge graphs: Methodology, tools and selected use cases*, 1 st edn.
- Fernandez, W.D., Lehmann, H. & Underwood, A. 2002, 'Rigor and relevance in studies of IS innovation: A grounded theory methodology approach'.
- Ferrag, M.A., Maglaras, L.A., Janicke, H., Jiang, J. & Shu, L. 2018, 'A systematic review of data protection and privacy preservation schemes for smart grid communications', *Sustainable cities and society*, vol. 38, pp. 806-35.
- Finn, R.L., Wright, D. & Friedewald, M. 2012, 'Seven types of privacy', *European data protection: coming of age*, Springer, Dordrecht, pp. 3-32.
- Floridi, L. 2010, *Information : A Very Short Introduction*, Oxford University Press, Oxford, UNITED KINGDOM.
- Fried, C. 1970, *An anatomy of values: problems of personal and social choice*, Harvard University Press.
- Fung, K.W. & Bodenreider, O. 2023, 'Knowledge representation and ontologies', *Clinical research informatics*, Springer, pp. 367-88.
- Gailloux, M.A. & King, L.R.S.A. 2020, 'Private information disclosure consent management system', Google Patents.
- Gaire, R., Ghosh, R.K., Kim, J., Krumpholz, A., Ranjan, R., Shyamasundar, R. & Nepal, S. 2019, 'Crowdsensing and privacy in smart city applications', *Smart cities cybersecurity and privacy*, Elsevier, pp. 57-73.
- GDPR.ED 2023, *Art. 4 GDPR Definitions*, gdpr.eu, viewed 1 Jul 2023, <<https://gdpr.eu/article-4-definitions/>>.
- GDPR.EU 2023, *Art. 5 GDPR Principles relating to processing of personal data*, viewed 23 Sep 2023, <<https://gdpr.eu/article-5-how-to-process-personal-data/>>.
- Gellman, R. 2017, 'Fair information practices: A basic history', *Available at SSRN 2415020*.
- Gerber, T.C. 2015, 'The conceptual framework for financial reporting represented in a formal language', University of Pretoria.
- Gill, A. 2021a, 'Adaptive Information Architecture: Information Element Identification and Organisation Patterns for Digital Ecosystem', *Information and Knowledge Engineering*, CSCE.
- Gill, A.Q. 2015a, *Adaptive cloud enterprise architecture*, vol. 4, World Scientific.
- Gill, A.Q. 2015b, 'Adaptive enterprise architecture driven agile development', *International Conference on Information Systems Development, ISD 2015*.
- Gill, A.Q. 2018, 'Distributed Agile Development: Applying a Coverage Analysis Approach to the Evaluation of a Communication Technology Assessment Tool', *Information and Technology Literacy: Concepts, Methodologies, Tools, and Applications*, IGI Global, pp. 1633-55.
- Gill, A.Q. 2021b, 'A Theory of Information TrilogY: Digital Ecosystem Information Exchange Architecture', *Information*, vol. 12, no. 7, p. 283.

- Gill, A.Q. 2022, *Adaptive enterprise architecture as information*
- Golafshani, N. 2003, 'Understanding reliability and validity in qualitative research', *The qualitative report*, vol. 8, no. 4, pp. 597-607.
- Graham, A. 2000, 'Demand for leisure air travel and limits to growth', *Journal of Air Transport Management*, vol. 6, no. 2, pp. 109-18.
- Gray, D.E. 2014, *Doing research in the real world*, 3rd edition. edn, SAGE, Los Angeles, California.
- Gregor, S. & Hevner, A. 2013, 'Positioning and Presenting Design Science Research for Maximum Impact', *MIS Quarterly*, vol. 37, pp. 337-56.
- Gross, J., Sedlmeir, J., Babel, M., Bechtel, A. & Schellinger, B. 2021, 'Designing a central bank digital currency with support for cash-like privacy', *Available at SSRN 3891121*.
- Gruber, T.R. 1995, 'Toward principles for the design of ontologies used for knowledge sharing?', *International journal of human-computer studies*, vol. 43, no. 5-6, pp. 907-28.
- Guarino, N. 1995, 'Formal ontology, conceptual analysis and knowledge representation', *International journal of human-computer studies*, vol. 43, no. 5-6, pp. 625-40.
- Guarino, N. 1998, *Formal ontology in information systems: Proceedings of the first international conference (FOIS'98), June 6-8, Trento, Italy*, vol. 46, IOS press.
- Guba, E.G. & Lincoln, Y.S. 1994, 'Competing paradigms in qualitative research', *Handbook of qualitative research*, vol. 2, no. 163-194, p. 105.
- Guia, J., Soares, V.G. & Bernardino, J. 2017, 'Graph Databases: Neo4j Analysis', *ICEIS (1)*, pp. 351-6.
- Guizzardi, G. 2005, 'Ontological foundations for structural conceptual models'.
- Guizzardi, G. 2006, 'The role of foundational ontologies for conceptual modeling and domain ontology representation', *2006 7th International Baltic conference on databases and information systems*, IEEE, pp. 17-25.
- Guizzardi, G., Falbo, R. & Guizzardi, R. 2008, *Grounding Software Domain Ontologies in the Unified Foundational Ontology (UFO): The case of the ODE Software Process Ontology*.
- Hajmoosaei, A. & Abdul-Kareem, S. 2008, 'An approach for mapping of domain-based local ontologies', *2008 International Conference on Complex, Intelligent and Software Intensive Systems*, IEEE, pp. 865-70.
- Halpern, N., Budd, T., Suau-Sanchez, P., Bråthen, S. & Mwesiumo, D. 2021, 'Conceptualising airport digital maturity and dimensions of technological and organisational transformation', *Journal of Airport Management*, vol. 15, no. 2, pp. 182-203.
- Harteveldt, H. 2016, *The Future of Airline Distribution 2016-2021*, iata.org.
- Havlena, W.J. & DeSarbo, W.S. 1991, 'On the measurement of perceived consumer risk', *Decision Sciences*, vol. 22, no. 4, pp. 927-39.
- Henderson-Sellers, B. 2012, *On the Mathematics of Modelling, Metamodeling, Ontologies and Modelling Languages*, 1st 2012. edn, Springer Berlin Heidelberg, Berlin, Heidelberg.
- Henriksen-Bulmer, J., Faily, S. & Jeary, S. 2019, 'Privacy risk assessment in context: A meta-model based on contextual integrity', *computers & security*, vol. 82, pp. 270-83.
- Herrera, J.L., Berrocal, J., Garcia-Alonso, J., Murillo, J.M., Chen, H.-Y., Julien, C., Mäkitalo, N. & Mikkonen, T. 2021, 'Personal data gentrification', *arXiv preprint arXiv:2103.17109*.
- Heurix, J., Zimmermann, P., Neubauer, T. & Fenz, S. 2015, 'A taxonomy for privacy enhancing technologies', *Computers & Security*, vol. 53, pp. 1-17.
- Hevner, A.R. 2007, 'A three cycle view of design science research', *Scandinavian journal of information systems*, vol. 19, no. 2, p. 4.
- Hevner, A.R., March, S.T., Park, J. & Ram, S. 2004, 'Design science in information systems research', *MIS quarterly*, pp. 75-105.
- Hiller, J.S. & Blanke, J.M. 2016, 'Smart Cities, Big Data, and the Resilience of Privacy', *Hastings LJ*, vol. 68, p. 309.
- Hirsh, M. 2016, *Airport urbanism: infrastructure and mobility in Asia*, U of Minnesota Press.
- Hitzler, P. 2021, 'A review of the semantic web field', *Communications of the ACM*, vol. 64, no. 2, pp. 76-83.

- Hofer, M., Obraczka, D., Saeedi, A., Köpcke, H. & Rahm, E. 2023, 'Construction of knowledge graphs: State and challenges', *arXiv preprint arXiv:2302.11509*.
- Hoffman, L. 1973, 'Modern methods for computer security and privacy'.
- Hoffman, L.J. 1977, *Modern methods for computer security and privacy*, Prentice-Hall Englewood Cliffs, NJ.
- Hogan, A., Blomqvist, E., Cochez, M., d'Amato, C., Melo, G.d., Gutierrez, C., Kirrane, S., Gayo, J.E.L., Navigli, R. & Neumaier, S. 2021, 'Knowledge graphs', *ACM Computing Surveys (CSUR)*, vol. 54, no. 4, pp. 1-37.
- Holender, A., Sutton, S. & De Simoni, A. 2018, 'Opinions on the use of technology to improve tablet taking in > 65-year-old patients on cardiovascular medications', *Journal of International Medical Research*, vol. 46, no. 7, pp. 2754-68.
- Hou, Y., Gao, P. & Nicholson, B. 2018, 'Understanding organisational responses to regulative pressures in information security management: The case of a Chinese hospital', *Technological Forecasting and Social Change*, vol. 126, pp. 64-75.
- Hubauer, T., Lamparter, S., Haase, P. & Herzig, D.M. 2018, 'Use Cases of the Industrial Knowledge Graph at Siemens', *ISWC (P&D/Industry/BlueSky)*.
- Hyndman, R. 2008, 'Quantitative business research methods', *Department of econometrics and Business Statistics. Monash University (Clayton campus)*.
- Iguchi, M., Uematsu, T. & Fujii, T. 2018, 'The Anatomy of the HIPAA Privacy Rule: A Risk-Based Approach as a Remedy for Privacy-Preserving Data Sharing', *International Workshop on Security*, Springer, pp. 174-89.
- Imine, Y., Lounis, A. & Bouabdallah, A. 2020, 'An accountable privacy-preserving scheme for public information sharing systems', *Computers & Security*, vol. 93, p. 101786.
- International Air Transport Association 2014, *Smart Security getting smarter*, International Air Transport Association, viewed 13 Jul 2020, <<https://airlines.iata.org/analysis/smart-security-getting-smarter#:~:text=Smart%20Security%20is%20a%20blending,adopted%20the%20Smart%20Security%20name>>.
- International Air Transport Association 2018, *Future of the airline industry 2035.*, International Air Transport Association, viewed 30 June 2022, <<https://www.iata.org/contentassets/086e8361b2f4423e88166845afdd2f03/iata-future-airline-industry.pdf>>.
- International Air Transport Association 2022, *Strong Passenger Demand Continues in June*, iata.org, viewed 10 June 2022, <<https://www.iata.org/en/pressroom/2022-releases/2022-08-04-01>>.
- International Air Transport Association n.d, *Facilitation and Passenger Data*, iata.org, viewed 3 JUL 2020, <<https://www.iata.org/en/programs/passenger/passenger-data/>>.
- International Civil Aviation Organisation n.d., *Security and Facilitation*, icao.net, viewed 4 Jul 2020, <<https://www.icao.int/Security/FAL/PKD/Pages/ePassportBasics.aspx>>.
- INTERSOFT CONSULTING 2018, *GENERAL DATA PROTECTION REGULATION (GDPR)*, gdpr-info.eu, viewed 2 Jun 2020, <<https://gdpr-info.eu/>>.
- ISACA n.d., *CDPSE Review Manual*, Information Systems Audit and Control Association.
- Islam, M.B. 2009, 'PRIVACY BY DESIGN FOR SOCIAL NETWORKS', The Royal Institute of Technology.
- Iwaya, L.H., Fischer-Hübner, S., Åhlfeldt, R.-M. & Martucci, L.A. 2019, 'Mobile health systems for community-based primary care: Identifying controls and mitigating privacy threats', *JMIR mHealth and uHealth*, vol. 7, no. 3, p. e11642.
- Iyengar, V.S. 2002, 'Transforming data to satisfy privacy constraints', *Proceedings of the eighth ACM SIGKDD international conference on Knowledge discovery and data mining*, pp. 279-88.
- Kalakou, S., Psaraki-Kalouptsidi, V. & Moura, F. 2015, 'Future airport terminals: New technologies promise capacity gains', *Journal of Air Transport Management*, vol. 42, pp. 203-12.

- Kalloniatīs, C., Kavakli, E. & Gritzalis, S. 2008, 'Addressing privacy requirements in system design: the PriS method', *Requirements Engineering*, vol. 13, no. 3, pp. 241-55.
- Kang, Y., Lee, H., Chun, K. & Song, J. 2007, 'Classification of privacy enhancing technologies on life-cycle of information', *The International Conference on Emerging Security Information, Systems, and Technologies (SECUREWARE 2007)*, IEEE, pp. 66-70.
- Karakuş, G., Karşıgil, E. & Polat, L. 2019, 'The Role of IoT on Production of Services: A Research on Aviation Industry', Springer International Publishing, pp. 503-11.
- Kenn Anthony Mendoza 2023, *Airport selfie poses risks when travelling, according to cybersecurity experts*, itwire, viewed 10 Aug 2023, <<https://itwire.com/business-it-news/security/airport-selfie-poses-risks-when-travelling,-according-to-cybersecurity-experts.html>>.
- Khi, I.A. 2020, 'Ready for take-off: how biometrics and blockchain can beat aviation's quality issues', *Biometric Technology Today*, vol. 2020, no. 1, pp. 8-10.
- Kılıç, S., Üçler, Ç. & Martin-Domingo, L. 2021, 'Innovation at airports: A systematic literature review (2000–2019)', *Aviation*.
- Kitchenham, B. & Charters, S. 2007, 'Guidelines for performing systematic literature reviews in software engineering'.
- Koenig, F., Found, P.A. & Kumar, M. 2019, 'Innovative airport 4.0 condition-based maintenance system for baggage handling DCV systems', *International Journal of Productivity and Performance Management*, vol. 68, no. 3, pp. 561-77.
- Konno, T., Huang, R., Ban, T. & Huang, C. 2017, 'Goods recommendation based on retail knowledge in a Neo4j graph database combined with an inference mechanism implemented in jess', *2017 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computed, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCOM/IOP/SCI)*, pp. 1-8.
- Koroniotis, N., Moustafa, N., Schiliro, F., Gauravaram, P. & Janicke, H. 2020, 'A holistic review of cybersecurity and reliability perspectives in smart airports', *IEEE Access*, vol. 8, pp. 209802-34.
- Kothari, C.R. 2004, *Research methodology: Methods and techniques*, New Age International.
- Kotzé, P., van der Merwe, A. & Gerber, A. 2015, 'Design science research as research approach in doctoral studies'.
- Krishnamurthy, B. & Wills, C.E. 2010, 'On the leakage of personally identifiable information via online social networks', *SIGCOMM Comput. Commun. Rev.*, vol. 40, no. 1, pp. 112-7.
- Labati, R.D., Genovese, A., Muñoz, E., Piuri, V., Scotti, F. & Sforza, G. 2016, 'Biometric Recognition in Automated Border Control: A Survey', *ACM Comput. Surv.*, vol. 49, no. 2, p. Article 24.
- Leonard, P. 2014, 'Customer data analytics: privacy settings for 'Big Data' business', *International Data Privacy Law*, vol. 4, no. 1, pp. 53-68.
- Li, C. & Palanisamy, B. 2018, 'Privacy in Internet of Things: from Principles to Technologies', *IEEE Internet of Things Journal*, vol. 6, no. 1, pp. 488-505.
- Li, F., Xie, W., Wang, X. & Fan, Z. 2020, 'Research on optimization of knowledge graph construction flow chart', *2020 IEEE 9th Joint International Information Technology and Artificial Intelligence Conference (ITAIC)*, vol. 9, IEEE, pp. 1386-90.
- Liew, A. 2013, 'DIKIW: Data, information, knowledge, intelligence, wisdom and their interrelationships', *Business Management Dynamics*, vol. 2, no. 10, p. 49.
- Lin, J.-S.C. & Hsieh, P.-L. 2007, 'The influence of technology readiness on satisfaction and behavioral intentions toward self-service technologies', *computers in Human Behavior*, vol. 23, no. 3, pp. 1597-615.
- Lincoln, Y.S. & Guba, E.G. 1985, *Naturalistic inquiry*, sage.
- Lykou, G., Anagnostopoulou, A. & Gritzalis, D. 2018, 'Implementing cyber-security measures in airports to improve cyber-resilience', paper presented to the Global Internet of Things Summit (GIoTS).



- Lykou, G., Anagnostopoulou, A. & Gritzalis, D. 2019, 'Smart airport cybersecurity: Threat mitigation and cyber resilience controls', *Sensors (Switzerland)*, vol. 19, no. 1.
- Mahmoud, M., Liu, Y., Hartmann, H., Stewart, S., Wagener, T., Semmens, D., Stewart, R., Gupta, H., Dominguez, D. & Dominguez, F. 2009, 'A formal framework for scenario development in support of environmental decision-making', *Environmental Modelling & Software*, vol. 24, no. 7, pp. 798-808.
- Makhdoom, I., Abolhasan, M., Lipman, J., Liu, R. & Ni, W. 2019, 'Anatomy of Threats to the Internet of Things', *IEEE Communications Surveys & Tutorials*, vol. 21, pp. 1636-75.
- Makhdoom, I., Zhou, I., Abolhasan, M., Lipman, J. & Ni, W. 2020, 'PrivySharing: A blockchain-based framework for privacy-preserving and secure data sharing in smart cities', *Computers & Security*, vol. 88, p. 101653.
- Malhotra, N., Kim, S. & Agarwal, J. 2004, 'Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model', *Information Systems Research*, vol. 15, pp. 336-55.
- Malik, H., Tahir, S., Tahir, H., Ihtasham, M. & Khan, F. 2023, 'A homomorphic approach for security and privacy preservation of Smart Airports', *Future Generation Computer Systems*, vol. 141, pp. 500-13.
- Martin, S., Szekely, B. & Allemang, D. 2021, *The Rise of the Knowledge Graph*, O'Reilly Media, Incorporated, <[https://info.cambridgesemantics.com/hubfs/The\\_Rise\\_of\\_the\\_Knowledge\\_Graph.pdf](https://info.cambridgesemantics.com/hubfs/The_Rise_of_the_Knowledge_Graph.pdf)>.
- Martinez-Balleste, A., Perez-Martinez, P.A. & Solanas, A. 2013, 'The pursuit of citizens' privacy: a privacy-aware smart city is possible', *IEEE Communications Magazine*, , no. 6, p. 136.
- Milne, G.R., Pettinico, G., Hajjat, F.M. & Markos, E. 2017, 'Information sensitivity typology: Mapping the degree and type of risk consumers perceive in personal data sharing', *Journal of Consumer Affairs*, vol. 51, no. 1, pp. 133-61.
- Morosan, C. 2018, 'Information Disclosure to Biometric E-gates: The Roles of Perceived Security, Benefits, and Emotions', *Journal of Travel Research*, vol. 57, no. 5, pp. 644-57.
- Mutanu, L., Gupta, K. & Gohil, J. 2022, 'Leveraging IoT solutions for enhanced health information exchange', *Technology in Society*, p. 101882.
- Mutumukwe, C., Twizeyimana, J.D. & Viberg, O. 2021, 'Students' information privacy concerns in learning analytics: Towards a model development', *arXiv preprint arXiv:2109.00068*.
- Nagy, E. & Csiszar, C. 2016, 'Airport Smartness Index – evaluation method of airport information services', *Osterreichische Zeitschrift Fur Verkehrswissenschaft* vol. 63, pp. 25-30.
- Nahar, K. & Gill, A.Q. 2020, 'A review towards the development of ontology based identity and access management metamodel', *Web, Artificial Intelligence and Network Applications: Proceedings of the Workshops of the 34th International Conference on Advanced Information Networking and Applications (WAINA-2020)*, Springer, pp. 223-32.
- Nahar, K., Gill, A.Q. & Roach, T. 2021, 'Developing an access control management metamodel for secure digital enterprise architecture modeling', *Security and Privacy*, vol. 4, no. 4, p. e160.
- National Institute of Standard and Technology 2013, *Guid for conducting risk assessments*.
- National Institute of Standard and Technology 2020, *NIST PRIVACY FRAMEWORK: A TOOL FOR IMPROVING PRIVACY THROUGH ENTERPRISE RISK MANAGEMENT, VERSION 1.0*.
- Nau, J.B. & Benoit, F. 2017, *SMART AIRPORT HOW TECHNOLOGY IS SHAPING THE FUTURE OF AIRPORTS*, Wavestone.
- Negri, N.A.R., Borille, G.M.R. & Falcão, V.A. 2019, 'Acceptance of biometric technology in airport check-in', *Journal of Air Transport Management*, vol. 81, p. 101720.
- Nissenbaum, H. 2004, 'Privacy as contextual integrity', *Wash. L. Rev.*, vol. 79, p. 119.
- Norberg, P., Horne, D. & Horne, D. 2007, 'The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors', *Journal of Consumer Affairs*, vol. 41, no. 1, pp. 100-26.
- Norta, A., Matulevičius, R. & Leiding, B. 2019, 'Safeguarding a formalized Blockchain-enabled identity-authentication protocol by applying security risk-oriented patterns', *Computers & Security*, vol. 86, pp. 253-69.

- Nosowsky, R. & Giordano, T.J. 2006, 'The Health Insurance Portability and Accountability Act of 1996 (HIPAA) privacy rule: implications for clinical research', *Annu. Rev. Med.*, vol. 57, pp. 575-90.
- Noy, N., Gao, Y., Jain, A., Narayanan, A., Patterson, A. & Taylor, J. 2019, 'Industry-scale Knowledge Graphs: Lessons and Challenges: Five diverse technology companies show how it's done', *Queue*, vol. 17, no. 2, pp. 48-75.
- Office of the Australian Information Commissioner n.d., *Your personal information*, oaic.gov.au, viewed 5 Jul 2020, <<https://www.oaic.gov.au/privacy/your-privacy-rights/your-personal-information>>.
- Office of the Australian Information Commissioner n.d., *AUSTRALIAN PRIVACY PRINCIPLES*, oaic.gov.au, viewed 2 Jun 2020, <<https://www.oaic.gov.au/privacy/australian-privacy-principles>>.
- Ohkubo, M., Suzuki, K. & Kinoshita, S. 2004, 'Efficient hash-chain based RFID privacy protection scheme', 01/01.
- Omerovic, S., Milutinovic, V. & Tomazic, S. 2001, *Concepts, Ontologies, and Knowledge Representation*, Springer: Berlin/Heidelberg, Germany.
- OntoUML 2018, *Class Stereotypes*, viewed 4 of JUL 2023, <<https://ontouml.readthedocs.io/en/latest/classes/index.html>>.
- Orlikowski, W.J. 1993, 'CASE tools as organizational change: Investigating incremental and radical changes in systems development', *MIS quarterly*, pp. 309-40.
- Orlikowski, W.J. & Barley, S.R. 2001, 'Technology and Institutions: What Can Research on Information Technology and Research on Organizations Learn from Each Other?', *MIS quarterly*, vol. 25, no. 2, pp. 145-65.
- Panahi Rizi, M.H. & Hosseini Seno, S.A. 2022, 'A systematic review of technologies and solutions to improve security and privacy protection of citizens in the smart city', *Internet of Things*, vol. 20, p. 100584.
- Papamartzivanos, D., Menesidou, S.A., Gouvas, P. & Giannetsos, T. 2021, 'A perfect match: Converging and automating privacy and security impact assessment on-the-fly', *Future Internet*, vol. 13, no. 2, p. 30.
- Patel, V. 2018, 'Airport passenger processing technology: a biometric airport journey', Embry-Riddle Aeronautical University, Daytona Beach, Florida.
- Pavlou, P.A. 2011, 'State of the Information Privacy Literature: Where are We Now And Where Should We Go?', *MIS Quarterly*, vol. 35, no. 4, pp. 977-88.
- Peacock, j. 2021, *What is NIST SP 800 30*, CyberSaintSecurity, viewed 90 sep 2021, <<https://www.cybersaint.io/blog/what-is-nist-sp-800-30>>.
- Peffers, K., Rothenberger, M., Tuunanen, T. & Vaezi, R. 2012, 'Design science research evaluation', *International Conference on Design Science Research in Information Systems*, Springer, pp. 398-410.
- Peffers, K., Tuunanen, T., Rothenberger, M. & Chatterjee, S. 2007, 'A design science research methodology for information systems research', *Journal of Management Information Systems*, vol. 24, pp. 45-77.
- Peppet, S.R. 2014, 'Regulating the internet of things: first steps toward managing discrimination, privacy, security and consent', *Tex. L. Rev.*, vol. 93, p. 85.
- Peter H.Gregory 2021, *CDPSE Certified Data Privacy Solutions Engineer All-in-One Exam Guide*, McGraw-Hill.
- Pfitzmann, A. & Hansen, M. 2010, 'A terminology for talking about privacy by data minimization: Anonymity, unlinkability, undetectability, unobservability, pseudonymity, and identity management', Dresden, Germany.
- Pingo, Z.B. 220, 'Privacy Literacy In the Era of the Internet of Things and Big Data', University of Technology Sydney Sydney.
- Pokorny, J. 2017, 'Modelling of graph databases', *Journal of Advanced Engineering and Computation*, vol. 1, no. 1, pp. 04-17.

- Pokorný, J. 2015, 'Graph databases: their power and limitations', *Computer Information Systems and Industrial Management: 14th IFIP TC 8 International Conference, CISIM 2015, Warsaw, Poland, September 24-26, 2015, Proceedings 14*, Springer, pp. 58-69.
- Pokorný, J. 2016, 'Conceptual and Database Modelling of Graph Databases', paper presented to the Proceedings of the 20th International Database Engineering & Applications Symposium, Montreal, QC, Canada, <<https://doi-org.ezproxy.lib.uts.edu.au/10.1145/2938503.2938547>>.
- Prat, N., Comyn-Wattiau, I. & Akoka, J. 2014, 'Artifact evaluation in information systems design-science research—a holistic view'.
- Psychoula, I. 2020, 'Privacy Modelling and Preservation for Assisted Living within Smart Homes', De Montfort University.
- Qi, Q. & Pan, Z. 2018, 'Internet of things, internet, big data and airport services make smart airport based on o2o and humanism', *2018 International Conference on Mechanical, Electronic, Control and Automation Engineering (MECAE 2018)*, Atlantis Press.
- Rajapaksha, A. & Jayasuriya, N. 2020, 'Smart Airport: A Review on Future of the Airport Operation', *Global Journal of Management and Business Research*, vol. 20.
- Rao, P.M. & Deebak, B. 2022, 'Security and privacy issues in smart cities/industries: technologies, applications, and challenges', *Journal of Ambient Intelligence and Humanized Computing*, pp. 1-37.
- Reason, P. & Bradbury, H. 2001, *Handbook of action research: Participative inquiry and practice*, sage.
- Robles-González, A., Parra-Arnau, J. & Forné, J. 2020, 'A LINDDUN-Based framework for privacy threat analysis on identification and authentication processes', *Computers & Security*, vol. 94, p. 101755.
- Robson, N. 2019, *How GDPR is Affecting Airports*, rezcomm.com, viewed 2 Jun 2020, <<https://www.rezcomm.com/blog/2019/07/16/gdpr-affecting-airports/>>.
- Romanou, A. 2018, 'The necessity of the implementation of Privacy by Design in sectors where data protection concerns arise', *Computer Law & Security Review*, vol. 34, no. 1, pp. 99-110.
- Romme, A.G.L. 2003, 'Making a difference: Organization as design', *Organization science*, vol. 14, no. 5, pp. 558-73.
- Rosenbaum, M.S., Otalora, M.L. & Ramírez, G.C. 2017, 'How to create a realistic customer journey map', *Business Horizons*, vol. 60, no. 1, pp. 143-50.
- Runeson, P. & Höst, M. 2009, 'Guidelines for conducting and reporting case study research in software engineering', *Empirical Software Engineering*, vol. 14, pp. 131-64.
- Runyon, B. 2020, *Healthcare CIOs: Prepare for Granular Patient Consent*, Gartner.
- Sadhukhan, D., Ray, S., Obaidat, M.S. & Dasgupta, M. 2021, 'A secure and privacy preserving lightweight authentication scheme for smart-grid communication using elliptic curve cryptography', *Journal of Systems Architecture*, vol. 114, p. 101938.
- Sakr, S., Bonifati, A., Voigt, H. & Iosup, A. 2021, 'Ensuring the success of big graph processing for the next decade and beyond', *COMMUNICATIONS OF THE ACM*, vol. 64, no. 9.
- Sandhu, R.S. & Samarati, P. 1994, 'Access control: principle and practice', *IEEE communications magazine*, vol. 32, no. 9, pp. 40-8.
- Sarraipa, J., Silva, J.P.M.A., Jardim-Goncalves, R. & Monteiro, A.A.C. 2008, 'MENTOR — A methodology for enterprise reference ontology development', *2008 4th International IEEE Conference Intelligent Systems*, vol. 1, pp. 6-32-6-40.
- Schneider, E.W. 1973, 'Course Modularization Applied: The Interface System and Its Implications For Sequence Control and Data Analysis'.
- Schwartz, P.M. & Solove, D.J. 2011, 'The PII problem: Privacy and a new concept of personally identifiable information', *NYUL rev.*, vol. 86, p. 1814.
- Schwartz, P.M. & Solove, D.J. 2014, 'Reconciling personal information in the United States and European Union', *Calif. L. Rev.*, vol. 102, p. 877.



- Shamshad, S., Mahmood, K., Kumari, S. & Chen, C.-M. 2020, 'A secure blockchain-based e-health records storage and sharing scheme', *Journal of Information Security and Applications*, vol. 55, p. 102590.
- Sharma, S., Singh, G., Sharma, R., Jones, P., Kraus, S. & Dwivedi, Y.K. 2020, 'Digital Health Innovation: Exploring Adoption of COVID-19 Digital Contact Tracing Apps', *IEEE transactions on engineering management*, pp. 1-17.
- Shehieb, W., Al Sayed, H., Akil, M.M., Turkman, M., Sarraj, M.A. & Mir, M. 2016, 'A smart system to minimize mishandled luggage at airports', *2016 International Conference on Progress in Informatics and Computing (PIC)*, IEEE, pp. 154-8.
- Shehieb, W., Al Sayed, H., Akil, M.M., Turkman, M., Sarraj, M.A. & Mir, M. 2017, 'A smart system to minimize mishandled luggage at airports', paper presented to the PIC 2016 - Proceedings of the 2016 IEEE International Conference on Progress in Informatics and Computing
- Shanghai, China.
- Siddiqui, F.M. & Ieee 2019, 'DIGITAL TRANSFORMATION OF MODERN AIRPORTS BY EXPLOITING FOG AS A SERVICE MODEL', *2019 Integrated Communications, Navigation and Surveillance Conference*.
- Silva, P., Monteiro, E. & Simões, P. 2021, 'Privacy in the Cloud: A Survey of Existing Solutions and Research Challenges', *IEEE Access*, vol. 9, pp. 10473-97.
- Smith, H., Milberg, S. & Burke, S.J. 1996, 'Information Privacy: Measuring Individuals' Concerns About Organizational Practices', *MIS Q.*, vol. 20, pp. 167-96.
- Solove, D.J. 2006, 'A TAXONOMY OF PRIVACY', *University of Pennsylvania Law Review*, vol. 154, no. 3, pp. 477-564.
- Solove, D.J. 2008, 'Understanding privacy'.
- Sowa, J.F. 1999, *Knowledge representation: logical, philosophical and computational foundations*, Brooks/Cole Publishing Co.
- Steenkamp, A.L. & McCord, S.A. 2007, 'Approach to teaching research methodology for information technology', *Journal of Information Systems Education*, vol. 18, no. 2, p. 255.
- Stoneburner, G., Goguen, A. & Feringa, A. 2002, *Risk Management Guide for Information Technology Systems, Special Publication (NIST SP)*, National Institute of Standard and Technology.
- Straker, K. & Wrigley, C. 2018, 'Engaging passengers across digital channels: An international study of 100 airports', *Journal of Hospitality and Tourism Management*, vol. 34, pp. 82-92.
- Studer, R., Benjamins, V.R. & Fensel, D. 1998, 'Knowledge engineering: principles and methods', *Data & knowledge engineering*, vol. 25, no. 1-2, pp. 161-97.
- Szekeres, A. 2020, 'Human Motivation as the Basis of Information Security Risk Analysis', Norwegian University of Science and Technology.
- Tamašauskaitė, G. & Groth, P. 2023, 'Defining a knowledge graph development process through a systematic review', *ACM Transactions on Software Engineering and Methodology*, vol. 32, no. 1, pp. 1-40.
- Taplin, K. 2021, 'South Africa's PNR regime: Privacy and data protection', *Computer Law & Security Review*, vol. 40, p. 105524.
- Terence Blevins and Mike Lambert 2022, *Business Scenarios*, The Open Group, <https://pubs.opengroup.org/>, viewed 10 Feb 2023, <[https://pubs.opengroup.org/togaf-standard/business-architecture/business-scenarios.html#\\_Toc68617078](https://pubs.opengroup.org/togaf-standard/business-architecture/business-scenarios.html#_Toc68617078)>.
- Thapa, C. & Camtepe, S. 2020, 'Precision health data: Requirements, challenges and existing techniques for data security and privacy', *Computers in biology and medicine*, p. 104130.
- Tlacuilo Fuentes, I. 2020, 'Legal Recognition of the Digital Trade in Personal Data', *Mexican law review*, vol. 12, no. 2, pp. 87-117.
- Urquhart, C. & Fernandez, W. 2006, 'Grounded theory method: The researcher as blank slate and other myths', *ICIS 2006 proceedings*, p. 31.

- Urquhart, C., Lehmann, H. & Myers, M.D. 2010, 'Putting the 'theory' back into grounded theory: guidelines for grounded theory studies in information systems', *Information systems journal*, vol. 20, no. 4, pp. 357-81.
- Uschold, M. & Grüninger, M. 1996, 'Ontologies: Principles, methods and applications', *The Knowledge Engineering Review*, vol. 11.
- Vaishnavi, V.K. & Kuechler, W. 2015, *Design science research methods and patterns: innovating information and communication technology*, Crc Press.
- Van Aken, J.E. 2005, 'Management research as a design science: Articulating the research products of mode 2 knowledge production in management', *British journal of management*, vol. 16, no. 1, pp. 19-36.
- Van Blarkom, G., Borking, J.J. & Olk, J.E. 2003, 'Handbook of privacy and privacy-enhancing technologies', *Privacy Incorporated Software Agent (PISA) Consortium, The Hague*, vol. 198.
- Van Bruggen, R. 2014, *Learning Neo4j*, Packt Publishing Ltd.
- Van Slyke, C., Shim, J., Johnson, R. & Jiang, J. 2006, 'Concern for Information Privacy and Online Consumer Purchasing', *J. AIS*, vol. 7.
- Vedaschi, A. 2018, 'Privacy and data protection versus national security in transnational flights: the EU–Canada PNR agreement', *International Data Privacy Law*, vol. 8, no. 2, pp. 124-39.
- Veghes, C., Orzan, M., Acatrinei, C. & Dugulan, D. 2012, 'Privacy literacy: what is and how it can be measured?', *Annales Universitatis Apulensis: Series Oeconomica*, vol. 14, no. 2, p. 704.
- Velliari, D.M. & Coleman-George, D. 2016, *Handbook of Research on Study Abroad Programs and Outbound Mobility*, IGI Global, Hershey, UNITED STATES.
- Venable, J., Pries-Heje, J. & Baskerville, R. 2012, *A Comprehensive Framework for Evaluation in Design Science Research*, vol. 7286.
- Vivek Kumar 2019, *Why Do Airports Need to Leverage Smart Cybersecurity?*, Analytica Insight, 2023, <<https://www.analyticsinsight.net/why-do-airports-need-to-leverage-smart-cybersecurity/>>.
- Wall, J., Lowry, P.B. & Barlow, J.B. 2015, 'Organizational violations of externally governed privacy and security rules: Explaining and predicting selective violations under conditions of strain and excess', *Journal of the Association for Information Systems*, vol. 17, no. 1, pp. 39-76.
- Wang, Y., Zhang, A., Zhang, P. & Wang, H. 2019, 'Cloud-assisted EHR sharing with security and privacy preservation via consortium blockchain', *IEEE Access*, vol. 7, pp. 136704-19.
- Warren, S.D. & Brandeis, L.D. 1890, 'Right to privacy', *Harv. L. Rev.*, vol. 4, p. 193.
- Webber, J. 2012, 'A programmatic introduction to neo4j', *Proceedings of the 3rd annual conference on Systems, programming, and applications: software for humanity*, pp. 217-8.
- Weber, R.H. 2010, 'Internet of Things–New security and privacy challenges', *Computer law & security review*, vol. 26, no. 1, pp. 23-30.
- Westin, A.F. 1968, 'Privacy and freedom', *Washington and Lee Law Review*, vol. 25, no. 1, p. 166.
- Willemsen, B. & Cadee, M. 2018, 'Extending the airport boundary: Connecting physical security and cybersecurity', *Journal of Airport Management*, vol. 12, no. 3, pp. 236-47.
- Williams, M., Axon, L., Nurse, J.R.C. & Creese, S. 2016, 'Future scenarios and challenges for security and privacy', *2016 IEEE 2nd International Forum on Research and Technologies for Society and Industry Leveraging a better tomorrow (RTSI)*, pp. 1-6.
- Wolford, B. 2020, *What is GDPR, the EU's new data protection law?*, gdpr.eu, viewed 2 Feb 2020, <<https://gdpr.eu/what-is-gdpr/>>.
- Wuyts, K., Scandariato, R. & Joosen, W. 2014, 'LIND (D) UN privacy threat tree catalog', *Department of Computer Science, KU Leuven*.
- Wuyts, K., Sion, L. & Joosen, W. 2020, 'Linddun go: A lightweight approach to privacy threat modeling', *2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, IEEE, pp. 302-9.
- Xiong, W. & Lagerström, R. 2019, 'Threat modeling – A systematic literature review', *Computers & Security*, vol. 84, pp. 53-69.

- Xu, H., Dinev, T., Smith, J. & Hart, P. 2011, 'Information privacy concerns: Linking individual perceptions with institutional privacy assurances', *Journal of the Association for Information Systems*, vol. 12, no. 12, p. 1.
- Yan, J., Wang, C., Cheng, W., Gao, M. & Zhou, A. 2018, 'A retrospective of knowledge graphs', *Frontiers of Computer Science*, vol. 12, pp. 55-74.
- Yang, L., Xue, H. & Li, F. 2014, 'Privacy-preserving data sharing in smart grid systems', *2014 IEEE International Conference on Smart Grid Communications (SmartGridComm)*, IEEE, pp. 878-83.
- Yang, Y., Zheng, X., Guo, W., Liu, X. & Chang, V. 2018, 'Privacy-preserving fusion of IoT and big data for e-health', *Future Generation Computer Systems*, vol. 86, pp. 1437-55.
- Yi, X., Miao, Y., Bertino, E. & Willemsen, J. 2013, 'Multiparty privacy protection for electronic health records', *2013 IEEE Global Communications Conference (GLOBECOM)*, IEEE, pp. 2730-5.
- Zhang, K., Ni, J., Yang, K., Liang, X., Ren, J. & Shen, X.S. 2017, 'Security and Privacy in Smart City Applications: Challenges and Solutions', *IEEE Communications Magazine*, vol. 55, no. 1, pp. 122-9.
- Zhang, Z. 2020, 'Technologies Raise the Effectiveness of Airport Security Control', paper presented to the 2019 IEEE 1st International Conference on Civil Aviation Safety and Information Technology (ICCASIT), Kunming, China, China.
- Zins, C. 2007, 'Conceptual approaches for defining data, information, and knowledge', *Journal of the American society for information science and technology*, vol. 58, no. 4, pp. 479-93.

## Appendices

### Appendix A- Second SLR selected studies

S1	A. Daly, "The introduction of data breach notification legislation in Australia: A comparative view," <i>Computer Law &amp; Security Review</i> , vol. 34, no. 3, pp. 477-495, 2018.
S2	B. Greaves and M. Coetzee, "Access control for secure information sharing in smart content spaces," <i>Journal of information security and applications</i> , vol. 34, pp. 63-75, 2017
S3	A. A. Alghanim, S. M. M. Rahman, and M. A. Hossain, "Privacy Analysis of Smart City Healthcare Services," in <i>2017 IEEE International Symposium on Multimedia (ISM)</i> , 11-13 Dec. 2017 2017, pp. 394-398, doi: 10.1109/ISM.2017.79
S4	J. Huang, Y. W. Qi, M. R. Asghar, A. Meads, and Y.-C. Tu, "MedBloc: A blockchain-based secure EHR system for sharing and accessing medical data," in <i>2019 18th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/13th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)</i> , 2019: IEEE, pp. 594-601.
S5	J. J. Hathaliya and S. Tanwar, "An exhaustive survey on security and privacy issues in Healthcare 4.0," <i>Computer Communications</i> , vol. 153, pp. 311-335, 2020.
S6	S. Chenthara, K. Ahmed, H. Wang, F. Whittaker, and Z. Chen, "Healthchain: A novel framework on privacy preservation of electronic health records using blockchain technology," (in English), <i>PloS one</i> , vol. 15, no. 12, p. 1, 2020
S7	Y. Yang, X. Zheng, W. Guo, X. Liu, and V. Chang, "Privacy-preserving fusion of IoT and big data for e-health," <i>Future Generation Computer Systems</i> , vol. 86, pp. 1437-1455, 2018/09/01/ 2018.
S8	S. Jiang, H. Wu, and L. Wang, "Patients-Controlled Secure and Privacy-Preserving EHRs Sharing Scheme Based on Consortium Blockchain," in <i>2019 IEEE Global Communications Conference (GLOBECOM)</i> , 9-13 Dec. 2019 2019, pp. 1-6.
S9	K. Li, Y. Yang, S. Wang, R. Shi, and J. Li, "A lightweight privacy-preserving and sharing scheme with dual-blockchain for intelligent pricing system of smart grid," <i>Computers &amp; Security</i> , vol. 103, p. 102189, 2021.
S10	E. Noe, L. Yang, F. Chao, and Y. Cao, "A framework of blockchain-based secure and privacy-preserving E-government system," (in English), <i>Wireless Networks</i> , pp. 1-11, Dec 2018
S11	P. Kumar, G. P. Gupta, and R. Tripathi, "TP2SF: A Trustworthy Privacy-Preserving Secured Framework for sustainable smart cities by leveraging blockchain and machine learning," <i>Journal of Systems Architecture</i> , vol. 115, p. 101954, 2021.
S12	A. Romanou, "The necessity of the implementation of Privacy by Design in sectors where data protection concerns arise," <i>Computer Law &amp; Security Review</i> , vol. 34, no. 1, pp. 99-110, 2018
S13	T. Braun, B. C. M. Fung, F. Iqbal, and B. Shah, "Security and privacy challenges in smart cities," <i>Sustainable Cities and Society</i> , vol. 39, pp. 499-507, 2018.
S14	Y. Wang, A. Zhang, P. Zhang, and H. Wang, "Cloud-assisted EHR sharing with security and privacy preservation via consortium blockchain," <i>IEEE Access</i> , vol. 7, pp. 136704-136719, 2019.
S15	C. Thapa and S. Camtepe, "Precision health data: Requirements, challenges and existing techniques for data security and privacy," <i>Computers in biology and medicine</i> , p. 104130, 2020.
S16	A. Agarkar and H. Agrawal, "A review and vision on authentication and privacy preservation schemes in smart grid network," <i>Security and Privacy</i> , vol. 2, no. 2, p. e62, 2019.
S17	T. Kanwal, A. Anjum, A. Khan, A. Asheralieva, and G. Jeon, "A formal adversarial perspective: Secure and efficient electronic health records collection scheme for multi-records datasets," <i>Transactions on Emerging Telecommunications Technologies</i> , p. e4180, 2020.

S18	M. A. Ferrag, L. A. Maglaras, H. Janicke, J. Jiang, and L. Shu, "A systematic review of data protection and privacy preservation schemes for smart grid communications," <i>Sustainable cities and society</i> , vol. 38, pp. 806-835, 2018
S19	J. Liu, J. Hou, X. Huang, Y. Xiang, and T. Zhu, "Secure and efficient sharing of authenticated energy usage data with privacy preservation," <i>Computers &amp; Security</i> , vol. 92, p. 101756, 2020.
S20	I. Makhdoom, I. Zhou, M. Abolhasan, J. Lipman, and W. Ni, "PrivySharing: A blockchain-based framework for privacy-preserving and secure data sharing in smart cities," <i>Computers &amp; Security</i> , vol. 88, p. 101653, 2020.
S21	Y. Zhang, D. He, and K.-K. R. Choo, "BaDS: Blockchain-based architecture for data sharing with ABS and CP-ABE in IoT," <i>Wireless Communications and Mobile Computing</i> , vol. 2018, 2018.
S22	Q. Zhang, Y. Li, R. Wang, L. Liu, Y. a. Tan, and J. Hu, "Data security sharing model based on privacy protection for blockchain-enabled industrial Internet of Things," <i>International Journal of Intelligent Systems</i> , vol. 36, no. 1, pp. 94-111, 2021.
S23	R. Khatoun and S. Zeadally, "Cybersecurity and Privacy Solutions in Smart Cities," <i>IEEE Communications Magazine</i> , vol. 55, no. 3, pp. 51-59, 2017.
S24	Y. Hou, P. Gao, and B. Nicholson, "Understanding organizational responses to regulative pressures in information security management: The case of a Chinese hospital," <i>Technological Forecasting and Social Change</i> , vol. 126, pp. 64-75, 2018.
S25	H. N. Chua, A. Herbland, S. F. Wong, and Y. Chang, "Compliance to personal data protection principles: A study of how organizations frame privacy policy notices," <i>Telematics and Informatics</i> , vol. 34, no. 4, pp. 157-170, 2017.
S26	P. Brous, M. Janssen, and P. Herder, "The dual effects of the Internet of Things (IoT): A systematic review of the benefits and risks of IoT adoption by organizations," <i>International Journal of Information Management</i> , vol. 51, p. 101952, 2020.
S27	S. Cao, J. Wang, X. Du, X. Zhang, and X. Qin, "CEPS: A Cross-Blockchain based Electronic Health Records Privacy-Preserving Scheme," in <i>ICC 2020 - 2020 IEEE International Conference on Communications (ICC)</i> , 7-11 June 2020 2020, pp. 1-6.
S28	H. Djigal, F. Jun, and J. Lu, "Secure Framework for Future Smart City," in <i>2017 IEEE 4th International Conference on Cyber Security and Cloud Computing (CSCloud)</i> , 26-28 June 2017 2017, pp. 76-83.
S29	N. Andola, Raghav, S. Prakash, S. Venkatesan, and S. Verma, "SHEMB:A secure approach for healthcare management system using blockchain," in <i>2019 IEEE Conference on Information and Communication Technology</i> , 6-8 Dec. 2019 2019, pp. 1-6.
S30	I. A. Khi, "Ready for take-off: how biometrics and blockchain can beat aviation's quality issues," <i>Biometric Technology Today</i> , vol. 2020, no. 1, pp. 8-10, 2020.
S31	D. Han, J. Chen, L. Zhang, Y. Shen, X. Wang, and Y. Gao, "Access control of blockchain based on dual-policy attribute-based encryption," in <i>2020 IEEE 22nd International Conference on High Performance Computing and Communications; IEEE 18th International Conference on Smart City; IEEE 6th International Conference on Data Science and Systems</i> . 2020
S32	T. K. Agrawal, V. Kumar, R. Pal, L. Wang, and Y. Chen, "Blockchain-based framework for supply chain traceability: A case example of textile and clothing industry," <i>Computers &amp; industrial engineering</i> , vol. 154, p. 107130, 2021
S33	G. Magyar, "Blockchain: Solving the privacy and research availability tradeoff for EHR data: A new disruptive technology in health data management," in <i>2017 IEEE 30th Neumann Colloquium (NC)</i> , 24-25 Nov. 2017 2017, pp. 000135-000140.
S34	M. M. Mahdy, "Semi-Centralized Blockchain Based Distributed System for Secure and Private Sharing of Electronic Health Records," in <i>2020 International Conference on Computer, Control, Electrical, and Electronics Engineering (ICCCEEE)</i> , 26 Feb.-1 March 2021 2021, pp. 1-4.
S35	M. T. Quasim, A. A. E. Radwan, G. M. M. Alshmrani, and M. Meraj, "A Blockchain Framework for Secure Electronic Health Records in Healthcare Industry," in <i>2020</i>

	<i>International Conference on Smart Technologies in Computing, Electrical and Electronics (ICSTCEE)</i> , 9-10 Oct. 2020 2020, pp. 605-609.
S36	D. Sadhukhan, S. Ray, M. S. Obaidat, and M. Dasgupta, "A secure and privacy preserving lightweight authentication scheme for smart-grid communication using elliptic curve cryptography," <i>Journal of Systems Architecture</i> , vol. 114, p. 101938, 2021
S37	S. Shamshad, K. Mahmood, S. Kumari, and C.-M. Chen, "A secure blockchain-based e-health records storage and sharing scheme," <i>Journal of Information Security and Applications</i> , vol. 55, p. 102590, 2020.
S38	S. Chenthara, A. Khandakar, and F. Whittaker, "Privacy-Preserving Data Sharing using Multi-layer Access Control Model in Electronic Health Environment," (in English), <i>EAI Endorsed Transactions on Scalable Information Systems</i> , vol. 6, no. 22, 2019.
S39	H. Huang, P. Zhu, F. Xiao, X. Sun, and Q. Huang, "A blockchain-based scheme for privacy-preserving and secure sharing of medical data," <i>Computers &amp; Security</i> , vol. 99, p. 102010, 2020
S40	B. Shen, J. Guo, and Y. Yang, "MedChain: Efficient Healthcare Data Sharing via Blockchain," (in English), <i>Applied Sciences</i> , vol. 9, no. 6, 2019
S41	E. Zaghoul, T. Li, and J. Ren, "Security and privacy of electronic health records: decentralized and hierarchical data sharing using smart contracts," in <i>2019 International Conference on Computing, Networking and Communications (ICNC)</i> , 2019: IEEE, pp. 375-379.
S42	J. den Hartog and N. Zannone, "Security and privacy for innovative automotive applications: A survey," <i>Computer Communications</i> , vol. 132, pp. 17-41, 2018.
S43	Z. Xiao, X. Fu, and R. S. M. Goh, "Data Privacy-Preserving Automation Architecture for Industrial Data Exchange in Smart Cities," <i>IEEE Transactions on Industrial Informatics</i> , vol. 14, no. 6, pp. 2780-2791, 2018.
S44	Z. Li, M. Alazab, S. Garg, and M. S. Hossain, "PriParkRec: Privacy-Preserving Decentralized Parking Recommendation Service," <i>IEEE Transactions on Vehicular Technology</i> , pp. 1-1, 2021.
S45	X. Yang, T. Li, W. Xi, A. Chen, and C. Wang, "A Blockchain-Assisted Verifiable Outsourced Attribute-Based Signcryption Scheme for EHRs Sharing in the Cloud," <i>IEEE Access</i> , vol. 8, pp. 170713-170731, 2020.
S46	S. Zhang, J. Rong, and B. Wang, "A privacy protection scheme of smart meter for decentralized smart home environment based on consortium blockchain," <i>International Journal of Electrical Power &amp; Energy Systems</i> , vol. 121, p. 106140, 2020.
S47	J. Cha, S. K. Singh, T. W. Kim, and J. H. Park, "Blockchain-empowered cloud architecture based on secret sharing for smart city," <i>Journal of Information Security and Applications</i> , vol. 57, p. 102686, 2021.
S48	D. C. Nguyen, P. N. Pathirana, M. Ding, and A. Seneviratne, "Blockchain for Secure EHRs Sharing of Mobile Cloud Based E-Health Systems," <i>IEEE Access</i> , vol. 7, pp. 66792-66806, 2019.
S49	M. Han, S. Liu, S. Ma, and A. Wan, "Anonymous-authentication scheme based on fog computing for VANET," <i>PLoS one</i> , vol. 15, no. 2, p. e0228319, 2020.
S50	J. Sun, L. Ren, S. Wang, and X. Yao, "A blockchain-based framework for electronic medical records sharing with fine-grained access control," (in English), <i>PLoS One</i> , vol. 15, no. 10, Oct 2020
S51	G. S. Reen, M. Mohandas, and S. Venkatesan, "Decentralized Patient Centric e- Health Record Management System using Blockchain and IPFS," in <i>2019 IEEE Conference on Information and Communication Technology</i> , 2019, pp. 1-7.
S52	M. S. Swetha, S. K. Pushpa, M. S. Muneshwara, and T. N. Manjunath, "Blockchain enabled secure healthcare Systems," in <i>2020 IEEE International Conference on Machine Learning and Applied Network Technologies (ICMLANT)</i> , 2020, pp. 1-6.

S53	M. T. Quasim, F. Algarni, A. A. E. Radwan, and G. M. M. Alshmrani, "A Blockchain based Secured Healthcare Framework," in <i>2020 International Conference on Computational Performance Evaluation (ComPE)</i> , 2020, pp. 386-391.
S54	B. Y. He and J. Y. J. Chow, "Optimal privacy control for transport network data sharing," presented at the <i>Transportation Research Procedia</i> , 2019/01/01/, 2019. [Online].
S55	Y. Li, D. Yang, and X. Hu, "A differential privacy-based privacy-preserving data publishing algorithm for transit smart card data," <i>Transportation Research Part C: Emerging Technologies</i> , vol. 115, p. 102634, 2020.
S56	F. Liu and T. Li, "A clustering-anonymity privacy-preserving method for wearable iot devices," <i>Security and Communication Networks</i> , vol. 2018, 2018
S57	Q. Huang, L. Wang, and Y. Yang, "Secure and Privacy-Preserving Data Sharing and Collaboration in Mobile Healthcare Social Networks of Smart Cities," (in English), <i>Security and Communication Networks</i> , vol. 2017, p. 12, 2017
S58	W. Cheng, W. Ou, X. Yin, W. Yan, D. Liu, and C. Liu, "A privacy-protection model for patients," <i>Security and Communication Networks</i> , vol. 2020, 2020.
S59	P. S. W. Shieng, J. Jansen, and S. Pemberton, "Fine-grained access control framework for igror, a unified access solution to the internet of things," presented at the <i>Procedia Computer Science</i> , 2018.
S60	O. Olakanmi and K. Odeyemi, "FEACS: A fog enhanced expressible access control scheme with secure services delegation among carers in E-health systems," <i>Internet of Things</i> , vol. 12, p. 100278, 2020.
S61	S. Amofa <i>et al.</i> , "A Blockchain-based Architecture Framework for Secure Sharing of Personal Health Data," in <i>2018 IEEE 20th International Conference on e-Health Networking, Applications and Services (Healthcom)</i> , 17-20 Sept. 2018.
S62	Q. Xia, S. Emmanuel Boateng, A. Smahi, S. Amofa, and X. Zhang, "BBDS: Blockchain-Based Data Sharing for Electronic Medical Records in Cloud Environments," (in English), <i>information</i> , vol. 8, no. 2, p. 44, 2017
S63	T. T. Thwin and S. Vasupongayya, "Blockchain-Based Access Control Model to Preserve Privacy for Personal Health Record Systems," (in English), <i>Security and Communication Networks</i> , vol. 2019, p. 15, 2019
S64	X. Liang, S. Shetty, D. Tosh, D. Bowden, L. Njilla, and C. Kamhoua, "Towards blockchain empowered trusted and accountable data sharing and collaboration in mobile healthcare applications," <i>EAI Endorsed Transactions on Pervasive Health and Technology</i> , Article 2018.
S65	Y. Nakamura, K. Harada, and H. Nishi, "A privacy-preserving sharing method of electricity usage using self-organizing map," <i>ICT Express</i> , vol. 4, no. 1, pp. 24-29, 2018/03/01/ 2018.
S66	Q. H. Cao, M. Giyyarpuram, R. Farahbakhsh, and N. Crespi, "Policy-based usage control for a trustworthy data sharing platform in smart cities," <i>Future Generation Computer Systems</i> , vol. 107, pp. 998-1010, 2020/06/01/ 2020.
S67	T. A. Butt, R. Iqbal, K. Salah, M. Aloqaily, and Y. Jararweh, "Privacy management in social internet of vehicles: review, challenges and blockchain based solutions," <i>IEEE Access</i> , vol. 7, pp. 79694-79713, 2019
S68	D. Eckhoff and I. Wagner, "Privacy in the Smart City—Applications, Technologies, Challenges, and Solutions," <i>IEEE Communications Surveys &amp; Tutorials</i> , vol. 20, no. 1, pp. 489-516, 2018, doi: 10.1109/COMST.2017.2748998
S69	M. Du, Q. Chen, J. Chen, and X. Ma, "An Optimized Consortium Blockchain for Medical Information Sharing," <i>IEEE transactions on engineering management</i> , vol. 68, no. 6, pp. 1677-1689, 2021
S70	L.-Y. Yeh, P. J. Lu, S.-H. Huang, and J.-L. Huang, "SOChain: A Privacy-Preserving DDoS Data Exchange Service Over SOC Consortium Blockchain," <i>IEEE transactions on engineering management</i> , vol. 67, no. 4, pp. 1487-1500, 2020

S71	O. Ajayi, M. Abouali, and T. Saadawi, "Secure Architecture for Inter-Healthcare Electronic Health Records Exchange," in 2020 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS), 9-12 Sept. 2020 2020, pp. 1-6.
N1	B. Willemsen, "Use a Privacy Impact Assessment to Ensure Baseline Privacy Criteria", Gartner, 20.
N2	R. C. Patrick Long, "5 Tips to Protect Data for Midsize Enterprise Remote Workers," Gartner, 2020.
N3	B. Runyon, "Healthcare CIOs: Prepare for Granular Patient Consent," Gartner, 2020
N4	S. J. Guido De Simoni, "Implement Your Data and Analytics Governance Through 5 Pragmatic Steps," Gartner, 2020.
N5	R. G. Richard Hunter, Neil MacDonald, Bart Willemsen, Jay Heiser, "Address Digital Business Risk by Using Adaptive Governance," Gartner, 2020.
N6	J. A. Wheeler, "Hype Cycle for Risk Management, 2018," Gartner, 2018
N7	B. W. Nader Henein, "The State of Privacy and Personal Data Protection, 2019-2020," Gartner, 2019.
N8	M. H. Nader Henein, "5 Steps to Managing Privacy in the Blockchain," Gartner, 2018.
N9	M. R. Avivah Litan, "Managing the Risks of Enterprise Blockchain Smart Contracts," Gartner, 2020.
N10	B. W. Brian Lowans, Marc-Antoine Meunier, "Use the Data Security Governance Framework to Balance Business Needs and Risks," Gartner, 2019
N11	A. M. Samantha Searle, "How to Develop the Right Technical and Human Architectures for Digital Business," Gartner, 2019.
N12	P. B. Bart Willemsen, "The Four Do's and Don'ts of Implementing Your Privacy Program," Gartner, 2017.



## Appendix B- Ethical approval

**From:** Research.Ethics@uts.edu.au <Research.Ethics@uts.edu.au>

**Sent:** Friday, May 28, 2021 10:34 AM

**To:** Research Ethics <research.ethics@uts.edu.au>; Asif Gill <Asif.Gill@uts.edu.au>; Maha Ibrahim A ALABSI <MahaIbrahimA.ALABSI@student.uts.edu.au>

**Subject:** HREC Approval Granted - ETH20-5093

Dear Applicant

**Re: ETH20-5093 - " A Framework of Privacy Assessment for Smart Airport Passenger Interaction Architecture**

."

Thank you for your response to the Committee's comments for your project. The Committee agreed that this application now meets the requirements of the National Statement on Ethical Conduct in Human Research (2007) and has been approved on that basis. You are therefore authorised to commence activities as outlined in your application.

You are reminded that this letter constitutes ethics approval only. This research project must also be undertaken in accordance with all [UTS policies and guidelines](#) including the Research Management Policy.

Your approval number is UTS HREC REF NO. ETH20-5093.

Approval will be for a period of five (5) years from the date of this correspondence subject to the submission of annual progress reports.

The following standard conditions apply to your approval:

- Your approval number must be included in all participant material and advertisements. Any advertisements on Staff Connect without an approval number will be removed.
- The Principal Investigator will immediately report anything that might warrant review of ethical approval of the project to the [Ethics Secretariat](#).
- The Principal Investigator will notify the Committee of any event that requires a modification to the protocol or other project documents, and submit any required amendments prior to implementation. Instructions on how to submit an amendment application can be found [here](#).
- The Principal Investigator will promptly report adverse events to the Ethics Secretariat. An adverse event is any event (anticipated or otherwise) that has a negative impact on participants, researchers or the reputation of the University. Adverse events can also include privacy breaches, loss of data and damage to property.
- The Principal Investigator will report to the UTS HREC or UTS MREC annually and notify the Committee when the project is completed at all sites. The Principal Investigator will notify the Committee of any plan to extend the duration of the project past the approval period listed above.
- The Principal Investigator will obtain any additional approvals or authorisations as required (e.g. from other ethics committees, collaborating institutions, supporting organisations).
- The Principal Investigator will notify the Committee of his or her inability to continue as Principal Investigator including the name of and contact information for a replacement. This research must be undertaken in compliance with the [Australian Code for the Responsible Conduct of Research](#) and [National Statement on Ethical Conduct in Human Research](#).

You should consider this your official letter of approval. If you require a hardcopy please contact the Ethics Secretariat.

If you have any queries about your ethics approval, or require any amendments to your research in the future, please don't hesitate to contact the Ethics Secretariat and quote the ethics application number (e.g. ETH20-xxxx) in all correspondence.

Yours sincerely,

The Research Ethics Secretariat

On behalf of the UTS Human Research Ethics Committees

**C/- Research Office**

University of Technology Sydney

E: [Research.Ethics@uts.edu.au](mailto:Research.Ethics@uts.edu.au)

*Ref: E38*

## Appendix C- Invitation letter

### **A Framework of Privacy Assessment for Smart Airport Passenger Interaction Architecture**

Dear .....,

My name is Maha Ibrahim Alabsi and I am a PhD student at the University of Technology Sydney.

I am conducting research in the area of privacy for digital information sharing in smart airport and would welcome your assistance. To evaluate the developed framework, I would like to request you to take part in this research, review the developed framework and provide your feedback via online survey. The online survey should take no more than 60-90 minutes of your time. I have asked you to participate because of your expertise in the field of information privacy/ security and smart cities.

This research is supported by Taibah University/ Kingdom of Saudi Arabia as a part of academic career requirements to pursue a PhD in Information technology.

If you are interested in participating, you will find the survey link in the online survey information sheet.

You are under no obligation to participate in this research.

Yours sincerely,

Maha Ibrahim Alabsi  
School of Computer Science  
University of Technology Sydney  
Ultimo NSW 2007, Australia  
E-mail:MahalbrahimA.ALABSI@student.uts.edu.au

#### **NOTE:**

This study has been approved by the University of Technology, Sydney Human Research Ethics Committee. If you have any complaints or reservations about any aspect of your participation in this research which you cannot resolve with the researcher, you may contact the Ethics Committee through the Research Ethics Officer (ph: +61 2 9514 2478 Research.Ethics@uts.edu.au), and quote the UTS HREC reference number. Any complaint you make will be treated in confidence and investigated fully and you will be informed of the outcome.

## ONLINE SURVEY INFORMATION SHEET

### **ETH20-5093 - A Framework of Privacy Assessment for Smart Airport Passenger Interaction Architecture**

#### WHO IS CONDUCTING THIS RESEARCH?

My name is Maha Ibrahim Alabsi and I am a student at school of Computer science/ FEIT at UTS. My supervisor is Dr.Asif Q. Gill

#### WHAT IS THE RESEARCH ABOUT?

The purpose of this research/online survey is to design privacy-preserving framework for sharing passengers' digital information in smart airport (PDIS). The framework aims to preserve the privacy of passengers' digital information that is shared among stakeholders in smart airport context.

You have been invited to participate because of your distinguished experience in Information Privacy/Security relevant to passengers in the aviation industry and smart airports, privacy-preserving technologies, and privacy regulations and standards.

Your contact details were obtained from the LinkedIn professional network for the supervisor, industry and academic conference of information privacy/security, and white paper and journal articles of information privacy/security.

#### FUNDING

This research is supported by Taibah University/ Kingdom of Saudi Arabia as a part of academic career requirements to pursue a PhD in Information technology.

#### WHAT DOES MY PARTICIPATION INVOLVE?

Participation in this study is voluntary. It is completely up to you whether or not you decide to take part.

If you decide to participate, I will invite you to kindly participate in the evaluation of my research outcome using the method of online survey. The survey includes a set of questionnaires designed to evaluate and the developed framework (PDIS Framework).

Further information:

- The survey questionnaire may require 60 to 90 mints.
- No travelling or payments are required.
- The surveys will be conducted online. Upon completion the data will be sent back to me.
- The data will not include any information that may identify you in any way. No personal data will be collected; the data collected via survey is technical and completely anonymous.
- The data will be stored in UTS systems. Only my supervisor and I have access to the stored data.
- The collected technical/anonymous data will be used for publications of conference papers, journal papers and the research thesis.

You can change your mind at any time and stop completing the survey/s without consequences.

#### ARE THERE ANY RISKS/INCONVENIENCE?

Yes, there are some risks/inconvenience. You may encounter potential inconvenience of contributing 1-1.5 hours to the study. However, you can save the survey and complete it later. Furthermore, your participation is voluntary and you can withdraw your participation anytime.

#### WHAT WILL HAPPEN TO INFORMATION ABOUT ME?

Access to the online questionnaire is via [https://utsau.au1.qualtrics.com/jfe/form/SV\\_bNP89k22nmVN4WO](https://utsau.au1.qualtrics.com/jfe/form/SV_bNP89k22nmVN4WO).

Submission of the online questionnaire/s is an indication of your consent.

It is anticipated that the results of this research project will be published and/or presented in a variety of forums. In any publication and/or presentation, information will be provided in such a way that you cannot be identified, except with your permission. The responses will be treated confidentially. The data will be stored in UTS systems as per UTS research data management policy. Only my supervisor and I have access to data via UTS secure login. The collected anonymous data from your response to the online survey form will not identify you in any way and will only be used for the purpose of this research project (thesis) and papers publications (conference and journal).

In accordance with relevant Australian and/or NSW Privacy laws, you have the right to request access to the information about you that is collected and stored by the research team. You also have the right to request that any information with which you disagree be corrected. Please inform the research team member named at the end of this document if you would like to access your information.

The results of this research may also be shared through open access (public) scientific databases, including internet databases. This will enable other researchers to use the data to investigate other important research questions. Results shared in this way will always be de-identified by removing all personal information (e.g. your name, address, date of birth etc.).

#### WHAT IF I HAVE CONCERNS OR A COMPLAINT?

If you have concerns about the research that you think I or my supervisor can help you with, please feel free to contact us on (Maha Ibrahim Alabsi (researcher):

[MahalbrahimA.ALABSI@student.uts.edu.au](mailto:MahalbrahimA.ALABSI@student.uts.edu.au), Dr.Asif Q. Gill (supervisor):

[Asif.Gill@uts.edu.au](mailto:Asif.Gill@uts.edu.au)).

If you would like to talk to someone who is not connected with the research, you may contact the Research Ethics Officer on 02 9514 9772 or [Research.ethics@uts.edu.au](mailto:Research.ethics@uts.edu.au) and quote this number ETH20-5093

## Appendix E- Online field survey Questionnaire

### Introduction

Smart airports aim to improve passengers' experience and deliver qualified services that rely on ICT in effective and affordable ways in order to enhance passenger convenience during their journey. Passengers need to share their information with respective stakeholders using several smart applications to get these services. IJAPRA (Interaction Journey Architecture and Privacy risk Assessment) is an ontology-based framework that integrates passenger interaction travel journey with privacy risks associated with passengers' information in the smart airport context. The vital part of the IJAPRA framework is the integrated ontology that defines the domain's concepts as well as the semantic relationships between them. The integrated ontology was developed in iterative processes where each version was evaluated over illustrative scenarios to ensure that relevant concepts were sufficiently covered. The developed IJAPRA framework will assist privacy experts, in both academic and industrial fields, in analysing privacy risk and designing privacy solutions relevant to personal information in smart airports context.

This survey questionnaire is intended to get valuable participants' ratings and experts' feedback about this framework. Please refer to the IJAPRA description section for further details about the framework.

### Scope

The scope of IJAPRA is limited to privacy risks for passengers' personal information during their journey on the departure side of domestic and international travel at smart airport. Arrival and In-flight information handling is beyond the scope of this project.

### Assessment Criteria

IJAPRA framework is assessed against the following criteria.

Criteria	Description
Applicability	The framework represents components and concepts relevant to the context
Understandability	The framework is clear and understandable
Usefulness	The framework is useful for privacy experts.
Generalisability	The framework is general and can fit different smart environments or contexts.

### Terms Glossary

ICT- Information and Communication Technology

IJAPRA-Interaction Journey Architecture and Privacy Risk Assessment Framework

IJ - Interaction Journey

PRA- Privacy Risk Assessment

PII- Personally Identifiable Information.

### Demographic Questions

Q1: Field of Experience (you can choose multiple answers)

Information privacy       Information security       Data protection

Q2: Duration of Experience

Less than 5 years       between 5 and 10 years       More than 10 years

## Framework Description:

Ontology-based IJAPRA framework comprises three main components: 1. Interaction journey (IJ), 2. Privacy risk assessment (PRA), and 3. Requirement. An overview of the framework is provided in Fig. 1. Descriptions of the framework's components are detailed below.

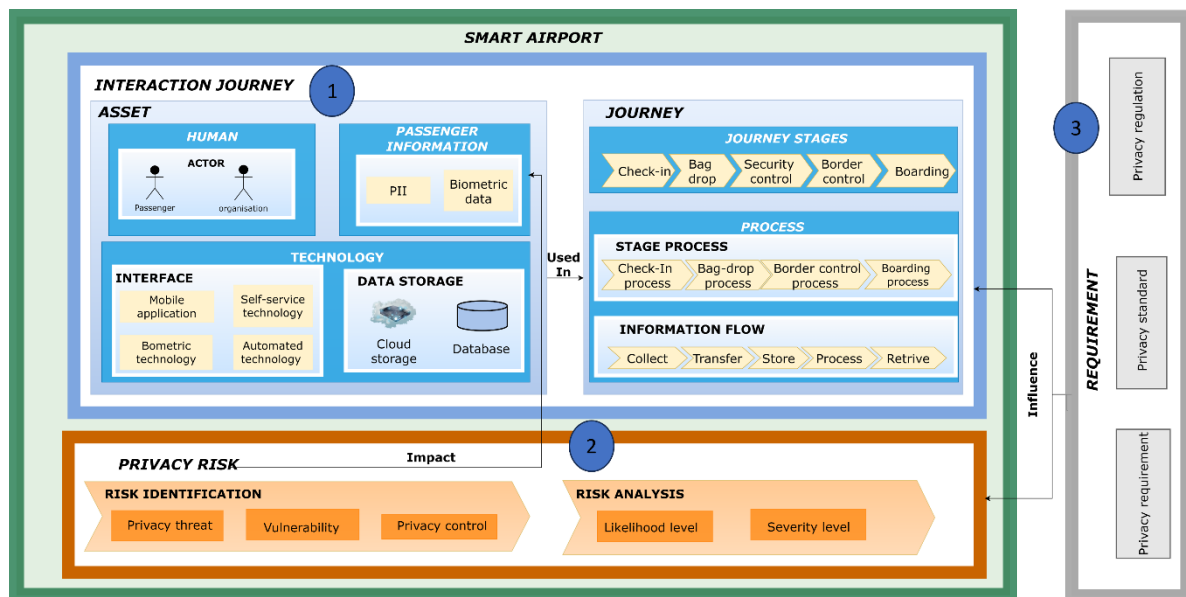


Figure 1: IJAPRA framework components: 1. Interaction journey, 2. Privacy risk, and 3. Requirement

### 1. Interaction journey (IJ)

This component includes assets used in the journey. It helps to cover key concepts of passenger travel journey in smart airport, including actors, information, process, technology, and journey stages. The concepts in IJ are grouped under two sub-components: Asset and Journey.

#### 1.1. Asset

The assets fall under three main categories: actors, such as individuals and organisation (carriers and governments), who interact during the journey. The information category presents the passenger's personally identifiable information (PII), and biometric information, that is handled during the journey. Technology category covers technological interface and data storage involved in passenger interaction journey. The interfaces such self-service technology, automated technology, biometric technology, mobile application, are enabled by several data storage, such as database, and cloud-based storage. Actors use these technological interfaces to handle passenger information at each journey stage.

#### 1.2. Journey

This sub-component presents concepts relevant to the journey, such as journey travel stages, which consists of stages on the departure side of the passenger travel journey. Process is another concept under the journey sub-component. It includes two types of process, stages process to represent passenger activity in each stage, and information flow that show the flow of passenger information during the journey stages.

### 2. Privacy risk assessment

This component includes the risk assessment process used to assess the privacy risks associated with passenger information during the journey. The process consists of two main steps: risk identification and risk analysis. The risk identification step involves the identification of (a) privacy threats and vulnerability associated with passenger

information (Table 1), and **(b)** existing privacy controls, technical and non-technical, to mitigate the identified risks (Table 2). Following the identification, the risk analysis step is conducted to evaluate severity and likelihood levels in order to determine the overall risk level.

a) **Privacy risks**

Table 1 Privacy risks associated with passenger personal information in smart airport

Category	Privacy Risks	
	Threats	Vulnerability
Improper Access	<ul style="list-style-type: none"> <li>• Unauthorised access (T1)</li> </ul>	<ul style="list-style-type: none"> <li>• Lack of policies and regulations or their un-transparency (V1)</li> <li>• Unprotected/ insecure storage systems (V2)</li> <li>• Insecure /unprotected sharing mechanism (V3)</li> </ul>
Unauthorised use	<ul style="list-style-type: none"> <li>• Secondary use (T2)</li> <li>• Modification(T3)</li> <li>• Information leakage(T4)</li> <li>• ID theft (T5)</li> </ul>	<ul style="list-style-type: none"> <li>• Lack of policies and regulations or their un-transparency (V1)</li> <li>• Unprotected/ insecure storage systems (V2)</li> <li>• Insecure /unprotected sharing mechanism(V3)</li> </ul>
Error	<ul style="list-style-type: none"> <li>• Misuse (T6)</li> </ul>	<ul style="list-style-type: none"> <li>• Lack of policies and regulations or their un-transparency (V1)</li> </ul>
Collection	<ul style="list-style-type: none"> <li>• Policy and consent non-compliance (T7)</li> </ul>	<ul style="list-style-type: none"> <li>• Lack of policies and regulations or their un-transparency (V1)</li> </ul>

b) **Privacy control**

Table 2 Existing privacy control relevant to the identified risks

Associated threats	Privacy control Type	Control classification
T2, T4, T5	Anonymisation (C1)	Technical solutions
T1,T2, T4, T5,	Cryptographic techniques (C2)	Technical solutions
T1, T4,	Access control mechanism (C3)	Technical solutions
T1, T2, T3, T4, T6	Blockchain (C4)	Technical solutions
T5	Machine learning (C5)	Technical solutions
T1, T2, T3, T4, T5, T7	Policies and regulation (C6)	Non-Technical solutions
T1, T2, T5,T7	Privacy risk management (C7)	Non-Technical solutions

3. **Requirement**

This component includes regulations, standards, and privacy requirements relevant to passenger information and its privacy in the aviation industry. This component is an



influencing factor that influences the handling of passengers' information and the risk assessment process. Examples of privacy regulations are General Data Protection Regulation (GDPR) adopted in Saudi Arabia and European airports, and the Australian Privacy Principle (APPs) in Australian airports. Standards and policies relevant to biographic/biometric passengers' information are developed by several governing bodies, such as the International Civil Aviation Organisation (ICAO), the European Border and Coast Guard Agency (Frontex), and the NIST. In addition, privacy requirements capture the passengers' privacy needs such as confidentiality, integrity, availability, authentication, authorisation, identification, anonymity, and unlinkability. The requirements definition is shown in Table 3.

Table 3 Privacy requirements

Privacy Requirements	Definition
Confidentiality	Restricting access to the information to authorised.
Integrity	Preventing unauthorised change and ensuring the authenticity of the information.
Availability	Providing timely and dependable access to and utilisation of information.
Authentication	Verification of user's identification before accessing information system resources.
Authorisation	Permitting access to a system resource, e.g., information.
Identification	Allowing only authorised people to access the stored information.
Anonymity	Subject's identity is not identified by others.
Unlinkability	It cannot determine whether the set of information is related.

Considering the description of the IJAPRA framework, please check the appropriate rating for the following statements:

**Survey Rating factors**

Qualitative rating	Quantitative rating
Strongly disagree	1
Disagree	2
Average	3
Agree	4
Strongly agree	5

**Applicability:**

1. The "Asset" defined in the Interaction journey component (IJ), (component 1), includes necessary assets used in passenger journey in smart airport.

Strongly Disagree	Disagree	Average	Agree	Strongly Agree

2. The "Journey" defined in the Interaction journey (IJ) component, component 1, includes key concepts needed to represent the stages and processes of passenger journey in smart airport.

Strongly Disagree	Disagree	Average	Agree	Strongly Agree

3. The Privacy risk assessment (PRA) component, component 2, represent an appropriate process to assess privacy risks associated with passenger information in smart airport.

Strongly Disagree	Disagree	Average	Agree	Strongly Agree

4. The "Requirement" component, component 3, includes concepts needed to influence the handling of passenger information during the journey and risk assessment process.

Strongly Disagree	Disagree	Average	Agree	Strongly Agree

**Understandability:**

1. IJAPRA framework and its components are clear and easy to understand.

Strongly Disagree	Disagree	Average	Agree	Strongly Agree

**Usefulness:**

1. IJPRFA framework is useful for privacy architects.

Strongly Disagree	Disagree	Average	Agree	Strongly Agree

2. IJPRFA framework is useful for privacy solution designers

Strongly Disagree	Disagree	Average	Agree	Strongly Agree

3. IJPRFA framework is useful for researchers.

Strongly Disagree	Disagree	Average	Agree	Strongly Agree

**Generalisability:**

1. IJAPRA Framework can be used in another smart context.

Strongly Disagree	Disagree	Average	Agree	Strongly Agree

**Overall feedback and rating**

What aspects are useful or valuable about IJAPRA framework?

.....

What improvements, including modifications, additions, deletions, or any additional feedback, would you suggest to IJAPRA framework?

.....

On a scale of 1 to 5 (5 being the highest), Please provide an overall rating for the IJAPRA framework.

IJAPRA Ratings

1	2	3	4	5

Comment

.....

Thank you for completing the survey.

## Appendix F- Research data

The following links provide the source of the data utilised in this thesis. This include the link of online field survey, and the survey processed data. The survey collected raw data have been stored in UTS systems as per UTS research data management policy. Access to these stored data files is restricted to the researcher and the principal supervisor (Dr. Asif Gill). The research data files are arranged as follow:

- Online field survey

[https://utsau.au1.qualtrics.com/jfe/form/SV\\_bNP89k22nnVN4WO](https://utsau.au1.qualtrics.com/jfe/form/SV_bNP89k22nnVN4WO)

- Field survey files- processed quantitative data

[Quantitative analysis- Applicability](#)

[Quantitative analysis- Generalisability](#)

[Quantitative analysis- Overall](#)

[Quantitative analysis- Understandability](#)

[Quantitative analysis- Usefulness](#)