Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 239 (2024) 1594–1603

Procedia Computer Science

www.elsevier.com/locate/procedia

CENTERIS – International Conference on ENTERprise Information Systems / ProjMAN – International Conference on Project MANagement / HCist – International Conference on Health and Social Care Information Systems and Technologies 2023

Integrated Interaction Journey and Privacy Risk Assessment: A Graph Model

Maha Alabsi[a,b,*], Asif Gill[a], Madhushi Bandara[a]

[a]*Faculty of Engineering and IT, School of Computer Science, University of Technology Sydney, Sydney, Australia*
[b]*Applied College, Taibah University, Al-Madinah Al-Munawarrah - Madina, Saudi Arabia*

Abstract

Smart airports involve several applications and stakeholders to facilitate passenger journey. Passengers interact with those stakeholders and share their personal information using the smart airport applications. While the use of smart airport applications offers several benefits, it also puts passengers' personal information at risk. This draws our attention to the need for identifying and understanding privacy risks with a view to protect passenger information at smart airports. Our earlier systematic literature review study revealed a gap in modelling passenger information privacy risks in the context of smart airports. This paper aims to address this gap by developing an ontology for interaction journey and privacy risk assessment modeling. The contribution of the proposed ontology is to bring new knowledge and understanding of privacy risks in the contemporary smart airport context. The development and evaluation of the proposed framework follows the Design Science Research (DSR) method along with the ontology development techniques. The proposed ontology aims to assist privacy experts in modelling and analyzing privacy risks relevant to passenger information in the smart airport context.

Keywords: smart airport, Passenger journey, information privacy, risk assessment, ontology.

* Corresponding author.
E-mail address: mahaibrahima.alabsi@student.uts.edu.au

10.1016/j.procs.2024.06.335

1. Introduction

Airport industry is rapidly evolving in response to changing travel requirements and digital technology landscape, such as cloud, IoT and mobile computing. This is also aimed to enhance the quality of provided airport services for improving passengers' experience during their journey [1]. One of the recent examples is utilizing digital technologies, which have enabled connectivity between airport facilities, data, and applications to help personalize customer experiences [2]. This has led to the emergence of the smart airport concept known as airport 4.0.

Smart airport 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 [3-5]. By using these technologies, passenger digital information embedded in their e-travel documents is collected, processed, and stored by airport and airlines systems. Such information can also be shared with various stakeholders, including airlines, customs, security and government agencies[6]. This clearly refers to the complexity around the handling of personal and sensitive information of passengers. This raises important concerns of personal privacy and data protection due to accidental or intentional threats, such as unauthorized access, misuse, and secondary uses [7] and lack of clear accountability among the involved stakeholders. For example, in 2018, British Airways faced a massive cyberattack that hacked their system, which led to the theft of credit card information by nearly 380,000 passengers. As a result, passengers suffered from significant financial loss, and the company faced adverse impacts on their reputation and customers' trust [8]. Thus, it is vital for passengers, airport authorities and related stakeholders to understand potential privacy risks associated with the passenger information. This can then lead to the identification and implementation of good practices to reduce the impact of the risks on individuals and related stakeholders.

Thus, this draws our attention to the need for an approach to help understand and address such concerns of information privacy in the context of smart airports. Therefore, as a first step, we conducted a systematic literature review to synthesize the literature published in this domain. This initial work revealed that studies lack a systematic and common understanding of privacy risks associated with passenger information in the smart airports context [anonymized for the purpose of peer review]. This paper builds on this earlier theoretical foundation and aims to address the knowledge gap of information privacy understanding and risk assessment by developing the Interaction Journey and Privacy Risk Assessment (IJPRA) Ontology.

This is a smart airport focused domain ontology that offers important concepts as well as the semantic relationships between them. The IJPRA ontology was developed and evaluated iteratively by using the DSR method and ontology modeling techniques. The main contribution of this paper is the development of the IJPRA ontology, a domain ontology which can be utilized as a tool to conceptualize, understand, assess and communicate privacy risks in smart airport context.

This paper is organized as follows: Section 2 presents the research background and related work. Section 3 outlines the methodology used in developing IJPRA ontology. Section 4 explains the ontology development process. Finally, section 5 presents the evaluation of the developed ontology before concluding.

2. Research background and related work

The meaning of privacy varies and is subject to interpretation within a given context. However, there are core components that are common to most definitions of privacy. A most simple and historical definition of privacy describes it as "the right to be let alone."[9]. Information specific privacy is defined as the relationship between an individual's right to privacy and the ability to access and control over their information, which is held by different organizations [10, 11].

The expected vulnerabilities, threats, losses and possible adverse impacts associated with the disclosure of personal information are referred to as privacy risks[12]. Pervasive literature attempts to identify the privacy risks of personal information. For example, Nissenbaum [13] proposed a privacy taxonomy based on the contextual integrity (CI) theory, which considers human factors, including their norms and attitudes, as part of privacy risk arising in public surveillance. In [14] a taxonomy using the same theoretical lens, IC, was proposed to address privacy risk in open data publishing. The privacy taxonomy developed by Solove [15] aimed to improve the understanding of information privacy in the legal system. This taxonomy classified privacy risk into four areas: collection, processing, dissemination, and invasion[15]. Further, there is another study [16], which provides a privacy taxonomy for classifying the privacy threats in the health domain e.g. identity, access, and disclosure threats in the health system. The framework designed in [17] provides key insights to help analysts with the addressing of key privacy issues when

designing software solutions. In [18] privacy risks relevant to IoT-enabled smart home system was discussed and a framework was proposed to help make appropriate privacy management decisions. The review conducted by [19] focused on security, privacy and risk in smart cities and how they impact the operational process of smart cities. In the smart airport, there is a few some mentioning of security challenges and the importance of privacy as a significant measure to secure and protect passenger information; however, they did not discuss privacy concerns in detail [20-22]. While there are several disjoint studies on this complex topic of privacy, however, according to our SLR [anonymized for the purpose of review], there is a lack of systematic research base studies that discuss the privacy risks and their impacts on passengers and their personal information in smart airports domain. Thus, the paper aims to address this gap by conceptualizing and developing IJPRA ontology to assist with the privacy risks assessment in smart airport context. The proposed ontology will provide a systematic and common understanding of the privacy risks in smart airport context. This can also be used as a tool in analyzing the risks.

3. Research Method

This research applied the design science research (DSR) method proposed by [23] to develop and evaluate the IJPRA ontology. In addition, we followed the specific ontology development guidelines proposed by Uschold and Grüninger [24] to develop the IJPRA ontology as a part of developing the IJPRA graph model. The guideline consists of 3 main steps: purpose, capture, and implementation. As a part of DSR, the proposed IJPRA ontology is evaluated by using illustrative scenarios to assess its applicability to capture knowledge for the domain in scope such as of the privacy risk in smart airport. It is important to mention here that several theoretical lenses, including Customer Journey Map (CJM) [25], Adaptive Enterprise Architecture (AEA) [26], Concerns for Information Privacy (CFIP) [27], and practical lens, such as NIST 800-30[28], were adopted to develop IJPRA ontology. Further, the Unified Foundational Ontology (UFO) [29] is used as a theoretical lens to develop IJPRA due to its significant roles in developing domain ontology conceptual modeling as a foundational ontology[30]. Figure 1 outlines the process of developing and evaluating the IJPRA. Ontology development is an iterative process, wherein each version is evaluated and improved using the scenarios intended to ensure the applicability of the ontology as a representation of knowledge relevant to the domain in scope (Figure 1).

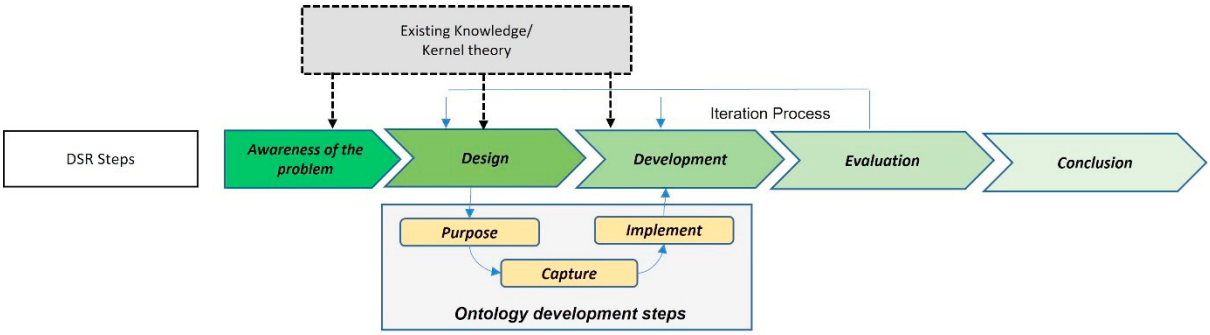

Fig. 1. IJPRA ontology development process.

As shown in Figure 1, the first step is: awareness of the problem. We conducted initial research to understand the research domain using the systematic literature review (SLR). This was done to identify the research gap and formalize the research problem. In the second step, design, Conceptual modeling was identified as an appropriate approach to address the research problem and develop the proposed solution. This will fill an important gap in understanding privacy risk in the context of smart airports. In the development step, The IJPRA was developed in two increments, which will be discussed in section 4. The design and development steps are conducted based on the following three sub-steps based on the adopted ontology development guidelines [24].

Purpose sub-step aims to identify the developed ontology's purpose and intended uses [24]. The purpose of developing IJPRA ontology is to fill the gap around the lack of a research-based understanding of privacy risk in the smart airport context. The developed ontology aims to assist privacy experts in academic and industry settings in understanding and analysing privacy risks associated with passenger information in the smart airport context e.g.

capturing and analysing privacy risk knowledge relevant to the identified domain of smart airports. Capture sub-step of ontology development involves identifying and defining relevant concepts and relationships within a domain This sub-step is executed through comprehensive reviews and the adoption of relevant practical and theoretical lenses to identify and categorize the identified concepts. Further, the identified concepts are mapped with the concepts in UFO that used as a theoretical lens. The definition of UFO concepts are founded in [29, 31, 32]. In Section 4, we will discuss how they were utilized in our study. Implementation sub step include representing the captured relevant knowledge (concepts and relationships) using a graph modelling approach [33]. To represent the IJPRA ontology using graph-modeling approach, the concepts in the ontology are representing as labelled node, whereas labelled edge representing the relationships in the IJPRA ontology [33]. Such approach is appropriate and provides a flexible structure for information-driven discipline, such as enterprise architecture, to model enterprise architecture with its privacy layer and underpinning elements, properties, and their connections [26]. We implemented the conceptual model and associated scenarios discussed in Section 5, using Neo4j graph database[34].

The DSR evaluation step helped to evaluate the applicability of the IJPRA using illustrative scenarios. This was done to evaluate the completeness, i.e. The proposed ontology is sufficient for capturing the domain knowledge in scope. In Section 5, we will discuss the evaluation process and the results. Finally, the Conclusion step provides the conclusion of the study including key contributions, limitations, and future work. It is important to mention that, due to the paper length constraints and the primary focus of this paper, we provided a condensed overview of the DSR method.

4. IJPRA Ontology

The development of the IJPRA ontology involved two increments: 1) the development of the interaction journey (IJ) ontology and privacy risk (PR)ontology, and 2) the development of the integrated Interaction Journey and Privacy Risk Assessment (IJPRA) ontology.

Increment 1 explains the development of IJ and PR ontologies. The CJM [25] and AEA [26] are the theoretical lenses that we adopted to assist in extracting and identifying entities relevant to passenger travel journeys in smart airports. The CJM was selected because it aids in the recognition and understanding of passenger travel stages, activities, and concerns during their travel, such as check-in, border control, and boarding stages. Adaptive EA was selected because it provides systematic layers for extracting and mapping the elements involved and interacting during passenger journeys, such as actor, process, information, and technology. This indicates the complex nature of the problem being addressed in this research. Further, the UFO was used to map the extracted concepts with UFO concepts as a foundational ontology to develop IJ ontology.

A systematic literature review [anonymized for purpose of review] was conducted to identify and extract key concepts and relationships relevant to passenger travel journey in smart airport context. The SLR results were analyzed and reported under the following categories: (1) passenger travel journey stages involving smart airport applications; (2) elements (people, process, information, technology) in the journey; (3) standards and regulations relevant to aviation industry to regulate passenger information during the journey. The definitions of concepts were inferred from the used theoretical lenses, including CJM, and Adaptive EA as well as existing studies. Following the identification and definition of the IJ concepts, these concepts are mapped with UFO concepts for consistency and compliance.

In parallel to IJ ontology, we developed the PR ontology by conducting an exhaustive review of existing studies in both academic and industrial fields on privacy models in several smart environments, such as smart health, smart homes, smart airports, smart cities, etc., to identify and extract key concepts and relationships relevant to privacy risks, requirements, and controls associated with personal information in several smart environments including the smart airport. This provided border coverage and a comprehensive view of privacy risks that impact passengers' information in their interaction journey in smart airports within the overall context of smart cities. The identified concepts were categorized using CFIP [27], besides the NIST 800-30 standard [28]. The CFIP helped to extract the privacy risk elements (threats and vulnerability) relevant to passenger information under four dimensions: collection, error, unauthorized use, and improper access. NIST SP 800-30 was used to identify and extract essential elements to assess the identified privacy risks, including privacy requirements and controls. The definitions of concepts were inferred from the used theoretical and practical lenses, CFIP and NIST, as well as existing studies. Then, the PR concepts are mapped with UFO concepts.

The second increment involves the development of IJPRA ontology by integrating IJ and PR ontologies. We used NIST 800-30 standard as a practical lens for integration as it offers a structured process to assess the privacy risks [28]. As a result, a list of concepts, shown in Table 2, emerged in this increment. The " PrivacyRiskAssess " concept represents the privacy risk assessment process and is the main concept for integration. The relationship "identify" was established to represent the connection between the privacy risk assessment concept and passenger information (main asset), privacy risk, requirements, and controls concept. Another relationship called "assess" was established to represent the connection between the Privacy risk assessment concept and "SeverityLvl" and "LikelihoodLvel," indicating that the severity and likelihood levels are assessed to determine the magnitude of the identified risk. Figure 2 presents the IJPRA graph model. Table 1 includes the identified concepts integrated IJPRA ontology, including IJ concepts, PR concepts, and emerged concepts for integration purpose in increment 2, their definitions, and their reference source and the mapping between the IJPRA concepts and UFO concepts.

Table 1. Integrated IJPRA concepts and their definition mapping with UFO concepts.

UFO Concepts	IJPRA Concept	Definition	Ref
Kind/Role	Actor	Individual and organization interact with each other as per their role in the smart airport. In smart airport individual role is passenger, while organisation roles are airline company, service providers, and government agency.	[3, 26]
Object	Passenger personal information	Represents information about an identified or identifiable passenger that is digitally handled during the journey in a smart airport.	[35]
Category	Information type	The category of the passenger personal information that is handled during their journey in smart airport, such as, PII, medical, or financial information, as well as passenger records.	[28]
Category	Information Classification	The way to classify passenger personal information based on its sensitivity level. For example, confidential, public, private, and restricted.	[36]
Kind	Technology	Represents interface that enables the interaction, via touchpoint and channel, to handle passenger information during the passenger journey, and data storage as devices used to store the handle passenger information.	[26]
Kind	Smart airport	The main building hosts elements involved in passenger journey.	[26]
Action	PasTraJourney	Passenger interaction with other actors, technology during their journey in smart airport.	[37]
Phase	Journey stage	The zone that divided passenger travel journey in smart airport.	[38]
Action	Process	A set of activities during the passenger journey. Including Stage process and data process.	[26]
Action	Stage Process	The activities to complete each stage of passenger journey.	[25, 26]
Action	Data Process	The handling process of passenger personal information during each stage of the journey.	[26]
Plan	Factor	Represents internal and external factors influence and guide the passenger journey, such as regulations, standards, and policies	[26]
Event	Privacy risk	A measure of the threats and vulnerabilities that impact passenger personal information in smart airport.	[28]
Event	Privacy Threat	Undesired and potential cause that harm passenger information in smart airport. such as unauthorized access, unauthorized use, non-compliance, and misuse.	[28]
Plan	Privacy requirement	Represent obligations arising from law and other sources to protect passenger information handled during their journey. Such as Confidentiality, Integrity, Availability, Anonymity, identification.	[28]
Action	Privacy Control	Process to mitigate the privacy risk that might impact passenger information in smart airport, such as technical and non-technical controls.	[28]

Category	Threat source	The source of the threat, internal or external, affecting the privacy of passenger personal information in smart airports.	[28]
Action	PrivacyRiskAssess	Represents the process of assessing risks associated with passenger personal information in smart airport context.	[28]
Phase	SeverityLvl	Represents the level of damage to passengers as a result of information disclosure, including Low, medium, High	[28]
Event	Impact	Represents the potential damage to passenger when passenger information is compromised.	[28]
Phase	LikelihoodLvl	Represents the level of probability of the threat source affecting passenger information, including Low, medium, High	[28]

As shown in Figures 2, passenger travel journey concept in IJPRA illustrates who and what is involved in the journey. The passenger travel journey is divided into several stages, as represented by the journey stage concept. The actor concept represents the people interacting during the passenger journey, including organizations and individuals. Organizations 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 concept of technology refers to the technologies used by actors to implement the processes. It includes underlying technologies that enable smart airport applications. Underlying technologies include IoT devices, biometrics, self-service, and automated systems, whereas smart airport applications support each stage of the passenger journey, from check-in to boarding. The process concept comprises three major processes: stage process, data process, and data flow process. These processes represent how passengers complete their journey stages including the handling of passenger information during their journey. The passenger information concept includes personal information with different types (represented by the information type concept), and classifications (described by the information classification concept). Various types of passenger personal information, such as Personal Identifiable Information (PII), biometric data, passenger records, medical information, and financial information, are handled in smart airports. These types of information are broadly classified into two main categories: private and sensitive. Additional classifications can also be used. It is important to mention that this paper focuses on passenger personal information, as non-personal information is beyond the scope of this research. The smart airport concept represents the facility that hosts actors, technology, process, and information. IJPRA ontology is designed to analyze and assess the risk of information disclosure. The risk assessment process starts by identifying privacy risks, controls, and requirements related to the passenger information asset. Thus, the privacy risk concept represents the privacy risk that consists of the privacy threat and vulnerability concepts. The privacy threat concept represents the various privacy threats that may exploit vulnerabilities in information handling. The privacy threat concept represents various privacy threats that exploit vulnerabilities in information handling. Privacy threats are mainly caused by internal or external threat sources. The privacy-control concept represents several technical and non-technical controls to mitigate risks and satisfy privacy requirements. The privacy requirements concept includes the requirements affected by risk. The identification process is followed by assessing the likelihood and severity levels to make an appropriate decision and choose the appropriate controls to mitigate the identified risk. The factor concept represents privacy regulations relevant to the aviation industry, influencing passenger journeys and risk assessment.

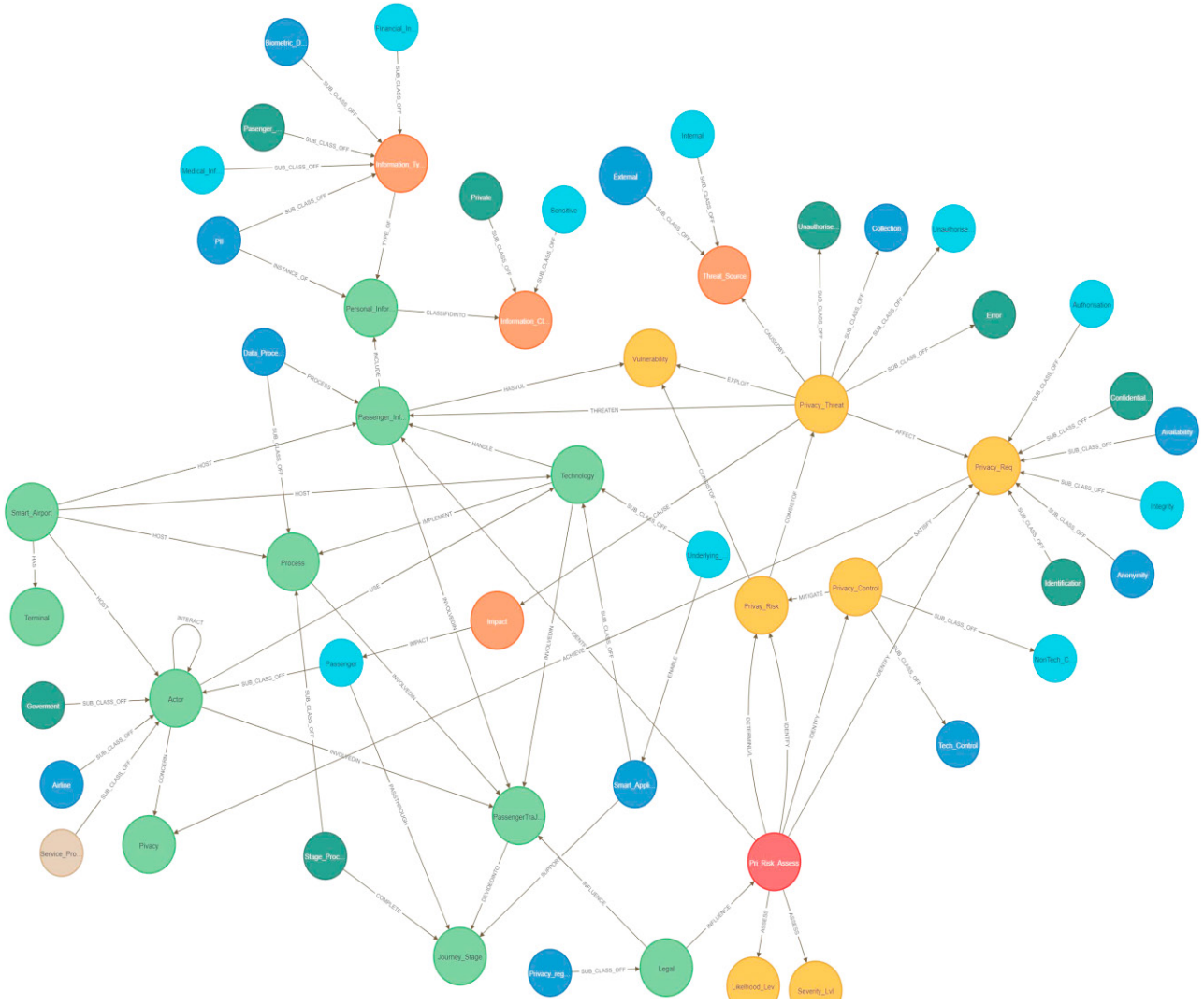

Fig. 2. IJPRA graph model.

5. IJPRA Evaluation

The passing sections discussed the development of the proposed IJPRA. This section demonstrates the applicability of the IJPRA ontology. The applicability of the IJPRA was evaluated from the perspective of its potential to describe and represent the selected domain in scope. We developed a set of privacy risk analysis and assessment scenarios based on the existing research to test the IJPRA [3, 39, 40]. Further, walkthrough review session was conducted among the research team to ensure the quality and relevance of the developed scenarios. The developed scenarios simulate smart airport situation. In this paper, we identify the fictitious airport as PMAS airport and develop a hypothetical scenario.

Case study: PMAS is a vital international airport that supports a large number of domestic and international flights to several destinations. PMAS smart airport terminals, domestic and international, are equipped with the underlying digital technologies that enable several smart applications to support and facilitate passenger-journey. It provides passengers with self-services, biometric and automated services to move through the process without human assistance. During the journey, a vast amount of 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). While the

intent of passenger information sharing is to enhance passenger experience. However, such information might be impacted by the disclosure of their information privacy to undesired systems and people. Therefore, it is important to assess potential passenger information privacy risks with a view to reduce the risks and their impacts on individuals. This case study example is further augmented with a test scenario that discusses an example type of passenger persona (Merchant) and privacy threat that affect their information. This scenario is further discussed below.

5.1. Scenario 1: Merchant passenger

Overview: Jon is merchant and has booked a domestic flight for their journey from point M to D. On the flight day, he arrived at Terminal 1 at PMAS smart airport, and went through the smart check-in self-service, and used a kiosk that helped him to move through the check-in process. He entered his e-ticket and phone numbers, inserted his credit card for flight upgrading, and obtained the e-boarding pass after the verification process. Jon's personal 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. His credit card information is intentionally shared with an unauthorized person by an airline staff member, revealing his financial information. This is likely to impact Jon, who could suffer from both information privacy and financial loss.

This situation draws our attention to the need for a mitigation of this the 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 identity and access mechanisms, privacy policies, and data encryption. General Data Protection regulation (GDPR) is used as a privacy regulation to influence or guide the protection, use and disclosure of financial information.

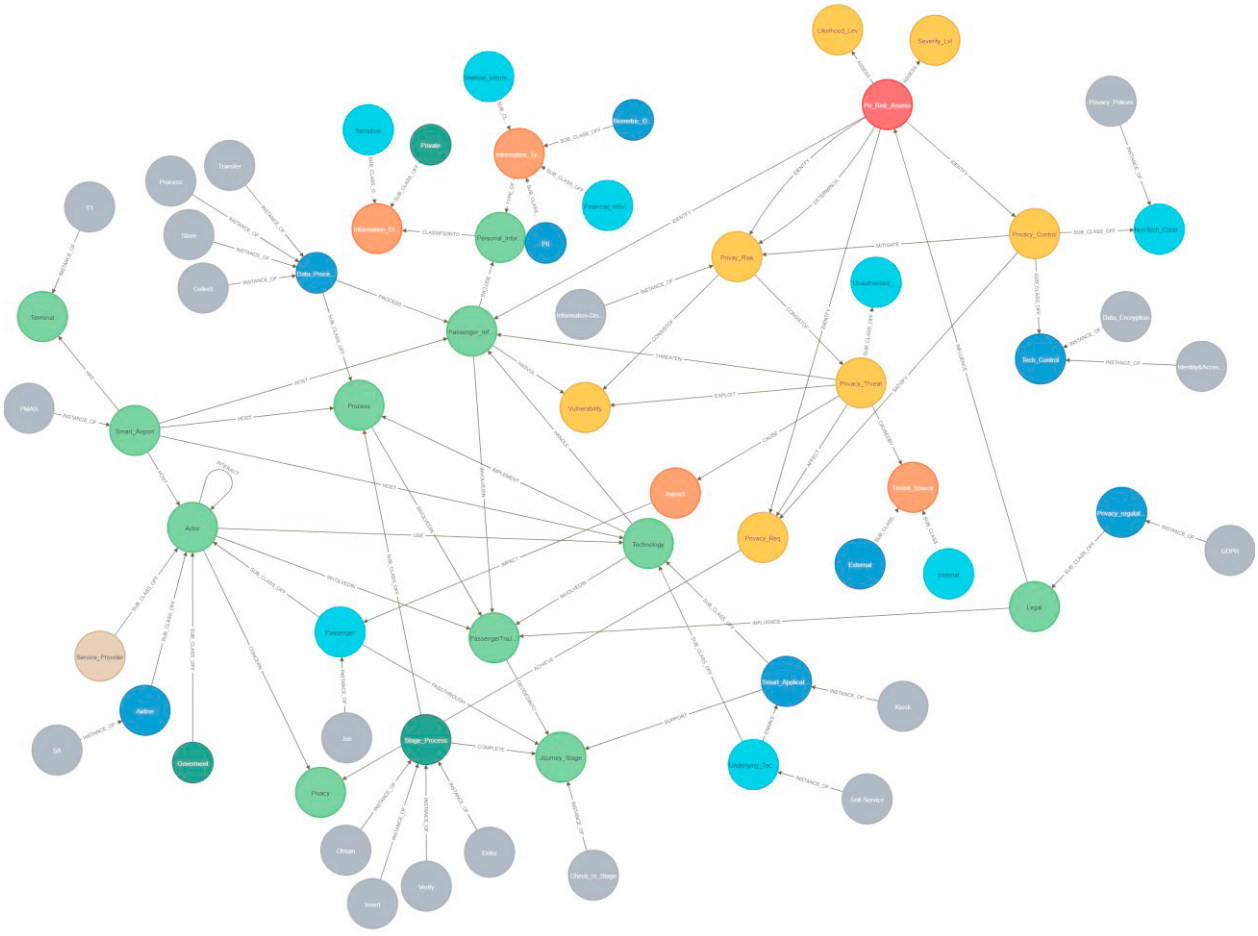

Fig. 3. Implementing the scenario to IJPRA graph-model.

Implementation: The scenario is implemented and represented using a graph modeling approach as noted by the IJPRA. For this purpose, No4j graph database was used to represent the instances, presented in gray color, based on the scenario, as shown in Figure 3.

Results and discussion: The IJPRA is applied to the described scenario as noted in Figure 3 to support the understanding of the information an relevant risks. It can be seen from this scenario that IJPRA ontology provided sufficient concepts and relationships to support the capturing information and risks for the evaluation scenario.

6. Conclusion and Future Work

This paper presents the Interaction Journey and Privacy Risk Assessment (IJPRA) ontology, which is designed to capture knowledge around privacy risks associated with passengers' information in the smart airport context. The developed ontology and its initial applicability evaluation is a first step towards further developing the Interaction Journey and Privacy Risk Assessment (IJPRA) framework and related privacy solutions. The development of ontology went through two main increments that were conducted based on DSR method and specific ontology development guidelines, as shown in Figure 1. The adopted guidelines involve three main steps that assist in identifying the purpose of the developed ontology, capture key concepts and relationships and finally representing the IJPRA using a graph modeling approach to offer a more flexible and contemporary approach to connecting concepts and their relationships. The process of ontology development is iterative, and each version was refined and evaluated using an illustrative scenario to ensure its applicability in representing the relevant domain knowledge. The proposed ontology aims to support privacy experts in academic and industrial fields to understand, analyze and conceptualize privacy risks in smart airport and design better privacy solutions. Future work includes evaluating the ontology for more scenarios and case studies and extending it further.

Reference

[1]Siddiqui FM, Ieee. DIGITAL TRANSFORMATION OF MODERN AIRPORTS BY EXPLOITING FOG AS A SERVICE MODEL. 2019 Integrated Communications, Navigation and Surveillance Conference. Integrated Communications Navigation and Surveillance Conference2019.

[2]Halpern N, Budd T, Suau-Sanchez P, Bråthen S, Mwesiumo D. Conceptualising airport digital maturity and dimensions of technological and organisational transformation. Journal of Airport Management. 2021;15(2):182-203.

[3]European Union Agency for Network and Information Security SECURING SMART AIRPORTS. 2016.

[4]The Aviation Valuables inside. Smart Airport. The Aviation Valuables Inside Information Technology n.d.

[5]Gill AQ, editor Adaptive enterprise architecture driven agile development. International Conference on Information Systems Development, ISD 2015; 2015.

[6]Labati RD, Genovese A, Muñoz E, Piuri V, Scotti F, Sforza G. Biometric Recognition in Automated Border Control: A Survey. ACM Comput Surv. 2016;49(2):Article 24.

[7]Chang-Ryung H, McGauran R, Nelen H. API and PNR data in use for border control authorities. Security Journal. 2017;30(4):1045-63.

[8]Vivek Kumar. Why Do Airports Need to Leverage Smart Cybersecurity? : Analytica Insight; 2019 [Available from: https://www.analyticsinsight.net/why-do-airports-need-to-leverage-smart-cybersecurity/.

[9]Warren SD, Brandeis LD. Right to privacy. Harv L Rev. 1890;4:193.

[10]Hoffman L, editor Modern methods for computer security and privacy1973.

[11]Martinez-Balleste A, Perez-Martinez PA, Solanas A. The pursuit of citizens' privacy: a privacy-aware smart city is possible. IEEE Communications Magazine, . 2013(6):136.

[12]Xu H, Dinev T, Smith J, Hart P. Information privacy concerns: Linking individual perceptions with institutional privacy assurances. Journal of the Association for Information Systems. 2011;12(12):1.

[13]Nissenbaum H. Privacy as contextual integrity. Wash L Rev. 2004;79:119.

[14]Henriksen-Bulmer J, Faily S, Jeary S. Privacy risk assessment in context: A meta-model based on contextual integrity. computers & security. 2019;82:270-83.

[15]Solove DJ. A TAXONOMY OF PRIVACY. University of Pennsylvania Law Review. 2006;154(3):477-564.

[16]Avancha S, Baxi A, Kotz D. Privacy in mobile technology for personal healthcare. ACM Computing Surveys (CSUR). 2012;45(1):1-54.

[17]Deng M, Wuyts K, Scandariato R, Preneel B, Joosen W. A privacy threat analysis framework: supporting the elicitation and fulfillment of privacy requirements. Requirements Engineering. 2011;16(1):3-32.

[18]Dasgupta A, Gill AQ, Hussain F. Privacy of IoT-enabled smart home systems. Internet of Things (IoT) for automated and smart applications. 2019:9.

[19]Ismagilova E, Hughes L, Rana NP, Dwivedi YK. Security, Privacy and Risks Within Smart Cities: Literature Review and Development of a Smart City Interaction Framework. Information Systems Frontiers. 2020.

[20]Choudhury ZH, Rabbani MMA. Biometric Passport for National Security Using Multibiometrics and Encrypted Biometric Data Encoded in the QR Code. Journal of Applied Security Research. 2019;15:1-31.

[21]Khi IA. Ready for take-off: how biometrics and blockchain can beat aviation's quality issues. Biometric Technology Today. 2020;2020(1):8-10.

[22]Tedeschi P, Sciancalepore S, editors. Edge and Fog Computing in Critical Infrastructures: Analysis, Security Threats, and Research Challenges. 2019 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW); 2019 17-19 June 2019.

[23]Vaishnavi VK, Kuechler W. Design science research methods and patterns: innovating information and communication technology: Crc Press; 2015.

[24]Uschold M, Grüninger M. Ontologies: Principles, methods and applications. The Knowledge Engineering Review. 1996;11.

[25]Rosenbaum MS, Otalora ML, Ramírez GC. How to create a realistic customer journey map. Business Horizons. 2017;60(1):143-50.

[26]Gill AQ. Adaptive enterprise architecture as information 2022.

[27]Smith H, Milberg S, Burke SJ. Information Privacy: Measuring Individuals' Concerns About Organizational Practices. MIS Q. 1996;20:167-96.

[28]National Institute of Standard and Technology Guid for conducting risk assessments. 2013.

[29]Guizzardi G. Ontological foundations for structural conceptual models. 2005.

[30]Guizzardi G, editor The role of foundational ontologies for conceptual modeling and domain ontology representation. 2006 7th International Baltic conference on databases and information systems; 2006: IEEE.

[31]Guizzardi G, Falbo R, Guizzardi R. Grounding Software Domain Ontologies in the Unified Foundational Ontology (UFO): The case of the ODE Software Process Ontology2008. 127-40 p.

[32]OntoUML. Class Stereotypes 2018 [Available from: https://ontouml.readthedocs.io/en/latest/classes/index.html.

[33]Pokorný J. Conceptual and Database Modelling of Graph Databases. Proceedings of the 20th International Database Engineering & Applications Symposium; Montreal, QC, Canada: Association for Computing Machinery; 2016. p. 370–7.

[34]Van Bruggen R. Learning Neo4j: Packt Publishing Ltd; 2014.

[35]GDPR.ED Art. 4 GDPR Definitions: gdpr.eu; 2023 [Available from: https://gdpr.eu/article-4-definitions/.

[36]Peter H.Gregory. CDPSE Certified Data Privacy Solutions Engineer All-in-One Exam Guide: McGraw-Hill; 2021.

[37]Law Insider. Passenger Journeys Definition | Law Insider [Available from: https://www.lawinsider.com/dictionary/passenger-journeys.

[38]Willemsen B, Cadee M. Extending the airport boundary: Connecting physical security and cybersecurity. Journal of Airport Management. 2018;12(3):236-47.

[39]Kalakou S, Psaraki-Kalouptsidi V, Moura F. Future airport terminals: New technologies promise capacity gains. Journal of Air Transport Management. 2015;42:203-12.

[40]Lykou G, Anagnostopoulou A, Gritzalis D. Smart airport cybersecurity: Threat mitigation and cyber resilience controls. Sensors (Switzerland). 2019;19(1).