IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received January 17, 2021, accepted February 5, 2021, date of publication February 23, 2021, date of current version March 4, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3061425

A Review of Passenger Digital Information Privacy Concerns in Smart Airports

MAHA IBRAHIM ALABSI AND ASIF QUMER GILL
Faculty of Engineering and Information Technology, School of Computer Science, University of Technology Sydney, Ultimo, NSW 2007, Australia
Corresponding author: Maha Ibrahim Alabsi (mahaibrahima.alabsi@student.uts.edu.au)

This work was supported by Taibah University, Saudi Arabia, which provided a PhD scholarship that covered funding for this work. This work was done at University of Technology Sydney, Australia.

ABSTRACT There is an increasing interest in the use of various digital technologies for interacting with passengers at smart airports. However, there is a need to identify and address the privacy issues that may threaten passenger's digital information during their interactions with smart airports applications. This study applies a systematic literature review method and reports the passenger's digital information privacy issues that arise during different stages of their travel journey in smart airports. This research identified a set of 324 studies, which were then reviewed to obtain a final set of 31 relevant studies to address the research questions in hand. The review results were organized into five major categories: passenger travel journey through smart airports applications; elements involved (people, process, information, and technology) in the journey; passenger's digital information privacy challenges; current solutions for identified challenges; passenger's information standards and privacy regulations. These results are further analyzed to report important insights and future research directions about the privacy of passenger's digital information in smart airports. This study will aid researchers and practitioners in obtaining a better understanding of the privacy concerns when dealing with the passenger's digital information at the digitally enabled smart airports.

INDEX TERMS Smart airport, digital information privacy, smart airport applications, enabling technology, automated system, privacy standards, privacy regulation.

I. INTRODUCTION

The continuous development in the airport industry is a result of the progressive growth in global passenger traffic. In 2018, passenger services demand rose 7.4%, exceeding the 5% long-run industry average rate [1]. Air travellers are projected to hit 8.2 billion by 2037 [2]. Accordingly, a massive pressure on existing airports facilities requires airport operators to rethink their traditional structures with a view to optimise their operations, increase capacity, expand revenues, and improve passenger experience while ensuring physical safety and digital security [3]. As such, digital technology enabled cooperation between airports facilities, data and applications to help personalising customer experiences. This leads to emergence of smart airport concept. The contemporary smart airports use a range of digital technologies such as self-service, flight information systems, baggage tracking, and smart parking.

A typical smart airport passenger journey comprises of five stages, which begins with the check-in. This stage involves capturing of identity and travel documents, which are used to create a single token for travel. Check-in is followed by bag drop, security control, border control, and boarding stages [4]. During this whole journey, different types of passenger's digital information elements are collected and handled. These include identity (biographic or biometric) and travel information.

Airports collect massive volumes of confidential and proprietary information about passengers. According to Leonard [5], dealing with the collection, storage, and use of such information may require addressing privacy concerns. Furthermore, such information would be an attractive target for cyber-attacks for various purposes such as fraud or sabotage that could cause disorder in airborne systems including aircrafts and airports [6].

Digital transformation of airports requires the need for understanding of passenger's information privacy concerns during their entire travel journey. To the best of our knowledge, no such recent academic studies are available that address this critical research need. Consequently, this study aims to fill this research gap by conducting a systematic literature review (SLR) to identify and synthesise the passenger's

The associate editor coordinating the review of this manuscript and approving it for publication was Zhe Xiao.

digital information privacy challenges. SLR is a type of study, which involves the identification, evaluation and analysis of systematically selected studies that relate to a specific research problem or field [7]. Hence, this study focuses on following research questions:

RQ1: What are the stages of passenger travel journey involving smart airport applications?

RQ2: What are the underpinning elements of the journey (people, process, information, and technology)?

RQ3: What are the passenger's digital information privacy challenges within each stage of their journey?

RQ4: What are the available current solutions for passenger's digital information privacy challenges?

RQ5: What are the relevant privacy standards, policies regulations in the aviation industry?

The main aspects and contributions of this paper are:

- We review and analyse various articles published in well-known academic databases during the last five years, including smart airports, information privacy, privacy regulations and standards.
- We use the Customer Journey Mapping framework (CJM) as a theoretical lens to identify the key elements of passenger's travel journey in smart airports.
- We use the Concerns for Information Privacy framework (CFIP) as a theoretical lens to identify and classify the privacy challenges of passenger's digital information in smart airports. Based on CFIP, we categorise privacy challenges into four types: collection, error, unauthorised use, and improper access.
- We identify the current proposed solutions and map them with the identified information privacy challenges.
- We cover the passenger's information standards and privacy regulations that relevant to aviation industry.
- We also provide future research directions about passenger's digital information challenges.

This paper is organised as follows. Firstly, it provides the research background. Secondly, it discusses the SLR research method. Thirdly, it describes the data extraction and synthesis. Fourthly, it presents SLR results. Finally, it discusses results, study limitations and future directions for further work in this important area of research.

II. BACKGROUND

There are several definitions of smart city, which can be distinguished based on their purpose and perspectives. Some of them focus on the importance of ICT infrastructure, while others emphasised on the social, economics, and the behavioural aspects of a smart city. For instance, IBM established a paradigm as a definition of smart cities. This paradigm calls "IN3" and consists of three dimensions: "instrumented, interconnected, and intelligent" [8], [9]. According to Giffinger, *et al.* [10], smart city is defined as a combination of six smart characteristics: economy, people, living, government, environment, and mobility. Kirimtat, *et al.* [11] focus on the importance of using information and communication technology (ICT) infrastructure to support smart city applications with a view to enhance the quality of life. The Office of the Government Chief Information Officer [12] discussed the integration of ICT, big data, and innovation for establishing smart cities.

Smart airport can be considered as a subsystem of smart city system or system of systems [13]. Thus, it is important to review important definitions related to smart airports within the context of smart city. According to the European Union Agency for Cybersecurity (ENISA), smart airport uses the capabilities of networked data-driven response and automated services in order to provide a better experience for passengers during their journey [14]. According to The Aviation Valuables Inside Information Technology [15], smart airport is defined as an ecosystem that implements efficient solutions for its components such as passengers, airlines, airport, and cargo [16].

The digital transformation of airport industry includes the use of emerging self-service, big data, and open data technologies [3]. Rajapaksha and Jayasuriya [17] discussed the evolution of airport industry in terms of four levels: Airport 1.0, 2.0, 3.0, and 4.0 (Figure 1). Firstly, Airport 1.0 (Basic airport operation) refers to the traditional airport that relies on manual operations and basic IT solutions. Secondly, Airport 2.0 (Agile airport) are the early adopters of digital technologies, mainly partial self-service facilities like Wi-Fi and check-in process. Thirdly, Airport 3.0 (Smart airport) involves the adoption of self-service at all levels of passenger services, including automated operations and mobility. Finally, Airport 4.0 (Smart airport) uses open and big data technologies to create value from real-time passenger information flow and profile analysis.

It has been indicated that enabling technologies are integral part of smart airports intending to enhance operational business efficiency and passenger services [18]. Examples of such enabling technologies in the context of smart airports are: Internet of Things (IoT), Artificial Intelligence (AI), Virtual Reality, Biometric, and Cloud Computing. These technologies can be used in many applications in order to enhance passenger's convenience during their travel journey. According to Rajapaksha and Jayasuriya [17] and Karakuş, *et al.* [19], smart airport application types include smart check-in; self- baggage services, biometric services, automated border control, and mobile applications for airports. Passengers can use the smart airports applications and services during both departure and arrival stages of their travel journey.

Passenger digital information is used during their travel journey in smart airports. This includes Passenger data comprises of Advance Passenger Information (API) and Passenger Name Records (PNR) [20]. Presently, besides this information, biometric data such as facial, and fingerprint recognition are also handled through smart airport applications [21]. Airlines and governments collect and share passenger digital information for identification purposes [22].

Privacy of information is defined as the individual's right about how their information is handled [23]–[25]. According

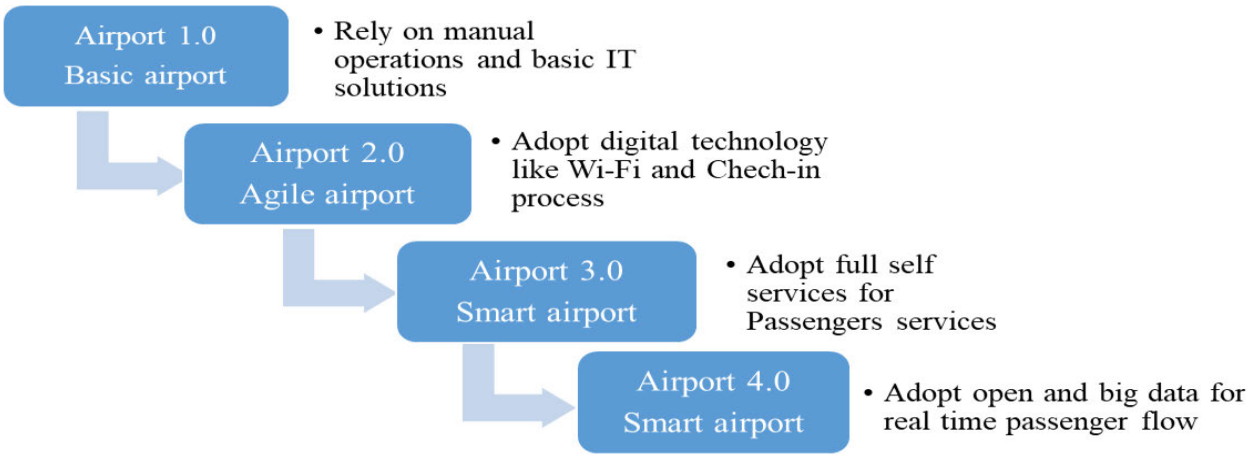

FIGURE 1. Airports digital transformation evolution levels.

to Solove [26], information privacy dimensions consists of: collect, process, publish, and violate the information. Further, it has been noted by Smith, *et al.* [27] that there is a need to identify the secondary usage and unauthorised access when dealing with privacy of information. Digital information privacy is a relevant concern, which can be linked to both smart airports and underpinning technology. In the context of information privacy, digital information privacy refers to an individual's right in deciding how their digital information is collected, shared and used. This draws our attention to the need for identifying the passenger's digital information privacy challenges in the context of smart cities and smart airports [28], [29].

In summary, passenger's digital information can be collected, processed, stored, and shared through smart airport applications during their travel journey. Such information is subject to privacy concerns. This study aims to address this vital need and reports the passenger information privacy concerns and challenges using the well-known SLR method, which is discussed in the following section.

III. RESEARCH METHOD

We followed a well-known SLR method guidelines to perform this study [7]. The structure of this SLR study is as follows: (1) study inclusion and exclusion criteria, (2) data source and search strategies, (3) study selection process, and (4) quality assessment.

A. INCLUSION AND EXCLUSION CRITERIA

Inclusion and exclusion are organised in two stages. The initial research stage included articles with following factors: (a) peer-reviewed; (b) English language; (c) search terms in Table 1 are included; (d) date between 2015 and 2020; (e) academic studies (journal articles, conference papers, book chapters). In this stage, duplicate results, non-academic documents such as magazines, reports, courses, tutorials, and notes, and grey literature were excluded. In the next search stage, the following inclusion criteria items were applied based on the research problem in hand.

TABLE 1. Search categories and keywords.

Search categories	Keywords
"Smart Airport"	Intelligent airport, digital airport, digital airfield, Aviation, airport, airfield, airport evolution level. smart airport applications
"Enabling technology"	Smart services, digital services, automated systems, smart system, digital system, IoT, AI, cloud computing, sensors, Self-services, E-gate, E-passport.
"Privacy of Passenger's information"	Individual's privacy, personal privacy, user privacy, passenger's privacy, data privacy threats, data privacy attacks, biometric privacy, data protection, privacy preservation, PNR, API, information, privacy standards and regulations, digital information.

- The article describes at least one stage of the passenger travel journey.
- The article discusses privacy challenges related to passenger digital information in the smart airport context. In addition, it discusses any existing solutions for the identified challenges as well as information privacy standards and regulations.

B. DATA SOURCE AND SEARCH STRING

Based on the identified research questions, we used the search string ''smart airport'', ''enabling technology'', and ''privacy of passenger's information'' to identify the relevant studies. Firstly, we searched the category ''smart airport'' in all selected databases. Then, we combined each item from first category ''smart airport'' with each item from second category ''enabling technology'' and then each item from third category ''privacy of passenger's data'' using the operator ''AND''. In each category, we combined similar terms using ''OR'' operator to achieve maximum coverage. Table 1 highlights search categories and terms used in performing the initial search.

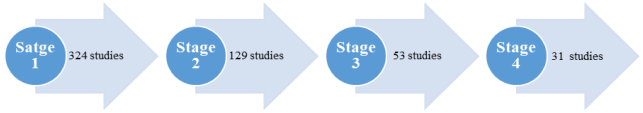

FIGURE 2. Study selection process.

TABLE 2. Summary of filtration stages.

Filtration stages	Method	Assessment criteria
1st stage	Based on the search string from the selected databases	All keywords
2nd stage	Exclude studies based on the title and keywords	"smart airport" and its terms
3rd stage	Exclude studies based on the abstract and conclusion	Additional criteria based on the research questions
4th stage	Obtained after critical evaluated of the full text	

The following electronic databases were used in this review. These well-known databases are expected to provide sufficient literature coverage for this SLR study.

- Scopus(www.scopus.com/)
- IEEE Xplore (www.ieexplore.ieee.org/Xplore/)
- ACM (dl.acm.org/)
- ScienceDirect(www.sciencedirect.com)
- SpringerLink (www.springerlink.com/)
- ProQuest(www.proquest.com)

C. STUDY SELECTION PROCESS

EndNote was used to store the relevant references from each stage, and then they were exported to Excel sheet to analyse and record inclusion/exclusion decisions. In stage 1, we got 324 studies after applying the initial search strategy and the first phase inclusion and exclusion criteria (as discussed earlier). In stage 2, 129 studies were included based on the review of their title and keywords related to our search terms. In stage 3, studies were included if their abstract and conclusion met the second stage criteria, and the result was a set of 53 relevant studies. Finally, in stage 4, 31 studies were included based on their content review. Further, study quality was assessed using the pre-determined assessment criteria (Table 4). Summary of each filtration stage is shown in Table 2. Table 3 and Figure 2 include the number of selected studies from each database at each stage.

D. QUALITY ASSESSMENT

The final set of selected studies were evaluated by tailoring and using the quality assessment checklist [7]. This was done to ensure the relevance and quality of the final selected set of studies. The quality assessment criteria items are shown below:

1. Does the context of the study address the related research appropriately?
2. Is the aim of the study specified?
3. Was the research method suitable for the study aims?
4. Does the study provide the relevant findings?
5. Is the future direction provided in the study?

The score of each criterion was either "1" or "0". The selected studies were assigned a score (1 to 5) based on the number of assessment criteria, which is 5. The study quality has been rated based on its overall score, which means the study quality is acceptable when the overall score is 3 or above. All studies got score 1 in the research column, as all selected studies were from academic sources. Three of the selected studies did not have a clear statement of aim. For the context column, several selected studies did not include details about research methods. The majority number of studies mentioned the finding and future research direction. Overall, it shows that the quality of selected studies is acceptable (3 or more) as indicated in the total column of Table 4.

TABLE 3. Number of selected studies in each stage.

Database	First filtration	Second filtration	Third filtration	Fourth filtration
IEEE	61	26	17	11
ProQuest	60	18	5	2
Scopus	65	40	15	6
Science Direct	65	22	7	7
AMC	21	7	4	3
Springer Link	52	16	5	2
total	324(no duplication)	129	53	31

TABLE 4. Selected studies based on assessment quality criteria.

Study	Research	Aim	Context	Findings	Future	Total
S1	1	1	0	1	0	3
S2	1	1	0	1	1	4
S3	1	1	0	1	1	4
S4	1	1	0	1	1	4
S5	1	1	1	1	0	4
S6	1	1	1	1	1	5
S7	1	1	0	1	1	4
S8	1	1	0	1	1	4
S9	1	1	1	0	1	4
S10	1	1	0	1	1	4
S11	1	0	0	1	1	3
S12	1	1	1	1	1	5
S13	1	1	0	1	1	4
S14	1	1	1	1	1	5
S15	1	1	1	1	1	5
S16	1	1	1	0	1	4
S17	1	1	1	1	1	5
S18	1	0	1	1	0	3
S19	1	1	0	1	1	4
S20	1	1	1	0	1	4
S21	1	1	0	1	0	3
S22	1	1	0	1	1	4
S23	1	1	0	1	1	4
S24	1	0	0	1	1	3
S25	1	1	0	0	1	3
S26	1	1	0	0	1	3
S27	1	1	1	1	1	5
S28	1	1	1	1	1	5
S29	1	1	0	0	1	3
S30	1	1	1	1	1	5
S31	1	1	1	1	1	5

TABLE 5. Costumer journey map (CJM) for passenger travel journey in smart airports.

Stage	Check-in		Security control	Border control	Boarding	All stages
Application	Smart check-in	Smart baggage handling	Smart security	Smart border control	Smart boarding	Smart airport applications
Goals	Smartly check-in of passenger's documents and baggage to issue a boarding pass and bag tags.		Verification of documents Without personal assistance then screening passenger and carry-on bags	Verification of passenger's identity and crossing the restricted area by self-service	Self-boarding to the aircraft	Facilitate passenger journey
Process (Activity)	Enter surname and booking reference/PNR via a specific technology in order to issue the boarding pass.	Scan passport to Print out and affix the baggage tag, then put them in the automated bag drop area	Scan passenger's documents and capture their photo to confirm the match between their information in e-passport and the taken photo with stored information in government database. At the end security officer will proceed the security screen after receives passenger's information	Enter the e-gate; scan the e-document then the data are processing in order to verify the biometric identity; exit the e-gate	Scan the boarding pass in boarding card scanning machine. Then the e-gate opens after the verification of Verify the scanned document	Each application is differently processed based on its job
Information	Biographic/biometric		Biometric	Biometric	Travel information (boarding pass)	Different
Enabling technology	Kiosks, autonomous system (intelligent kiosks KATE), biometric tech (smart path), automated system	Automated system, RFID tech	Biometric tech	Biometric tech Automated system RFID tech	RFID tech Automated system	Mobile devices
	IoT, Cloud Servers					

IV. DATA EXTRACTION AND SYNTHESIS

We analysed and synthesised the results of this SLR using the Customer Journey Mapping framework (CJM) as a theoretical lens [30]. CJM is a visual representation of the sequence of activities and actions that are widely applied by organisations for understanding the customer interactions and experience [30]. We chose CJM to identify and understand the passenger travel journey stages, information and enabling technology as shown in Table 5. Further, we used the Concerns for Information Privacy framework (CFIP) [31] as a theatrical lens to identify and categorise the passenger digital information privacy challenges (Figure 3). CFIP is a framework, which can be used to address individual information privacy concerns. For example, in e-commerce, CFIP is used to measure consumer privacy concerns in order to improve the online shopping experience [31]. CFIP framework is a multidimensional structure that consists of four dimensions: collection, error, unauthorised use, improper access [31]. Each dimension covers individual concerns related to collecting, storing, accessing and protecting information. Thus, CFIP has been used in this research to capture and report results, which are presented in the following section.

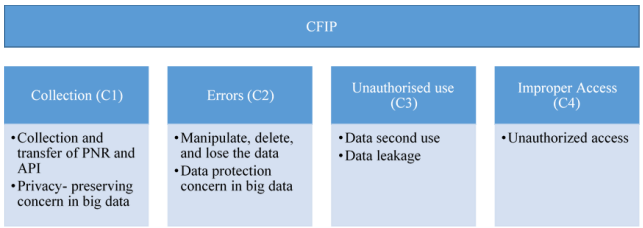

FIGURE 3. CFIP Framework- Identify and categorise information privacy challenges.

V. RESULT

In this section, we analysed the final selected studies (see Appendix A) in order to answer identified research questions. It is important to note here that 17 of the 31 selected studies were found in the conference sources, while the rest were from academic journals.

In order to address the research questions of this SLR, the results were analysed using CJM and CFIP frameworks, 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.

A. PASSENGER TRAVEL JOURNEY THROUGH SMART AIRPORT APPLICATIONS

For RQ1, it has been found that only 48% of the selected studies discuss the stages of passenger travel journey (supported by smart airport applications), as shown in Table 6. Overall, passengers pass through several stages during their

FIGURE 4. The stages of passenger journey.

travel journey, which begins before arriving at the airport as outlined in Figure 4 [32].

After booking a flight, actual interaction between passenger and smart airport applications begins at the check-in stage. At this stage, passenger utilises smart check-in applications through self-service kiosk, website or mobile devices to obtain the boarding pass and bag tags. Most recently, it has been noted that biometric services are used for check-in such as at Brisbane and Hamad international airports [33]. This stage also includes the smart baggage handling applications that can be used to finalise the baggage check-in and drop-in through an automated system

Security control stage involves the verification of the travel documents and screening of the passengers and their carry-on bags. Since 2014, International Air Transport Association (IATA) and Airport Council International (ACI) have introduced the smart security control initiative, which aims to implement an end-to-end self-service by 2020. It is important to make security control checkpoint more secure and convenient for passengers [34]. In the meantime, airports still widely use the conventional process in this stage. However, it has been noted that biometric service has been adopted by Custom and Border Protection (CBP) at Hartsfield-Jackson Atlanta International (ATL) airport in USA [35].

It can be observed from Table 6, 29% of the selected studies discussed the Automated Border Control (ABC) at the border control stage. It has been found that smart border control applications (including self-service and biometric service) are mainly used at the departure and arrival to accelerate the identity verification at the border control stage. Finally, at the boarding stage, 6% of selected studies explained how smart boarding applications empower passengers to board on to the aircraft by using self-service.

Beside the above mentioned applications, the smart airport applications for mobile devices are widely used by passengers to assist and guide them during their travel journey [36]. For instance, they provide information about locations and status of counter numbers, flight update, boarding time, shops and other utilities. Further, they can be used for tracking luggage, checking the waiting queue, and finding of available parking spots.

B. ELEMENTS INVOLVED IN PASSENGER JOURNEY

RQ2 is related to the identification of elements that are involved in the journey (people, information, process, and technology). In order to address RQ2, we have identified some key stages of passenger journey through this SLR

TABLE 6. Passenger journey in smart airports.

Passenger travel journey	Smart airport applications	Papers	Percentage
Check-in stages	Smart check-in	S14, S26, S27,S28	13%
Bag drop stages	smart baggage handling	S14, 26,S28,S29	13%
Airport security control stage (Smart security)	Smart security	S11, S14	6%
Border control stages	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 airports Apps for mobile devices	S26, S2,S3,S1,S14	16%

TABLE 7. People involves in passenger's travel journey.

Elements	Who and what involved	Papers	Percentage
People	Airlines	S14, S21, S26	10%
	Airports	S14,S26	6%
	Government	S11,S26	6%
	Border control authorities	S21	3%

study. We further analysed the studies, and identified the underlying people (such as passengers, carriers, and governments), process (for explaining passenger's activity in each stage), information (e.g. passenger digital information) and technology (use to source and handle the passenger digital information through the applications) elements relevant to passenger travel journey in the context of smart airports. Here, we used CFIP framework as a theoretical lens to capture four dimensions of passenger digital information privacy concerns.

1) PEOPLE

In Table 7, 13% of reviewed studies discussed the handling of passenger's digital information during their travel journey. This information is collected and shared by various stakeholders: airlines, airports, and governments agencies (such as border controller authority) during departure and arrival. Further, 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 stages. Airports use passenger's information to improve their services and passenger experience.

2) PROCESS

In Table 8, 10% of selected studies describe how passengers can finalise their check-in process by using self-service

TABLE 8. Smart airports process for passengers.

Process	Description	Papers	Percentage
Passenger's check- in	The check-in process within smart check-in application relays on the kind of applied services either self-service or biometric one.	S14,S26,S27	10%
Baggage check-in	The process implements through smart baggage handling application by using self-services.	S14,S26	6%
Security control	The security checkpoint process where the passengers undergo the checking security through smart security control application.	S11	3%
Border control	It is the process within smart border control application where the passenger's identity is verifying without human assistance	S10,S11,S31,S30	13%
Boarding	The passenger on boards the aircraft after Appling some steps through smart boarding application.	S26	3%

kiosks (either common one or the intelligent one), or online systems (by using smart devices) to print the boarding pass. One of the studies (S27) discussed using the biometric technology for smart check-in. Confirmation of passenger's information including biometric data are key to check-in process. During smart baggage handling process, passenger scan their passport and boarding pass to print out and affix the baggage tag, then put them in the automated bag drop area.

Smart security control process includes the following items: (1) passenger scans the passport and boarding pass; (2) system verifies the passenger's name in both documents; (3) passenger's photo is captured to confirm the match between the taken photo and the one in the passport; (4) If the passenger's biometric identity is matched to the one stored in government database, passenger's details will be sent to the tablet of security officer to proceed with the security screening.

As shown in Table 8, 13% of selected studies outline the process of using smart border control application. This process starts and ends through automated gate (e-gate), and includes scanning passenger's e-passport, verifying their taken photo (biometric data) by camera, and finalising this stage after confirming the matching between e-passport and biometric data. Before entering the aircraft, passenger goes through smart boarding application to scan their boarding pass, then the automated gate will open to let them enter the aircraft.

TABLE 9. Passenger's digital information that is handled through their 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%

3) INFORMATION

Based on this review, the passenger information was mentioned in only 26% of selected studies as shown in Table 9. It has been found that passenger's information is classified into biographic and biometric data. Biographic data is usually located on the second page of the passport document. It includes passenger's name, nationality, place and date of birth, signature, photograph, passport number, date of issues, and expiry date. Biometric data refers to information about the biological characteristics of an individual that are captured using scanners or cameras [37]. Based on our review, the passenger's biometrics data such as fingerprint, facial, and iris are closely related to smart airports and collected in check-in, security control and border control stages. As indicated in Table 9, 16% of the selected studies described the e-passport as an example of e-travel document that is commonly used in smart airports. According to ICAO [38], an e-passport is a booklet that stores passenger's biographical information and biometric sample (such as fingerprint, face image) on an electronic chip. A unique digital signature protects this type of e-documents for each country.

Further, two types of passenger's information records are discussed in 6% of the selected studies as shown in Table 9. The first type is the advance passenger information (API), which contains 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 name record (PNR), which has passenger's contact number, address, credit card details. These information records are generated during booking and check-in stages by airlines and passengers themselves. In most cases, airlines are required to share such information records with the border control authority located in different destinations before the flight's arrival time [22].

4) TECHNOLOGY

In smart airport context, smart applications mainly rely on the use of underlying technologies that enable them. Based on our review, we classified the smart airport technologies items into five groups, as shown in Table 10: Internet of Things (IoT), radio frequency identification (RFID), mobile devices, autonomous system like intelligent check-in kiosk (KATE), kiosk, Artificial Intelligent (AI), machine learning, biometric technology, automated systems, and cloud computing. Sensor technology is an example of IoT, which is widely used in smart airport applications within each stage.

TABLE 10. Enabling technology that used to enable smart airports 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,S26,25,S5	16%
Automated systems	S26,S14,S20,S10,S16	16%
Autonomous system (KATE intelligent kiosks)	S27	3%

It is observed that smart airport applications are implemented by a combination of two or more enabling technologies. For example, sensors and RFID, beside biometric technology, and automated systems, are utilised in smart boarder control and smart security control applications in order to increase the efficiency and security of the passenger identification process. The RFID and automated drop off machines are vital in smart baggage handling applications. They are used by passengers in printing baggage tags and self-drop-off their baggage. Mobile devices are commonly adopted by passengers for using smart airport mobile apps. About 6% of the selected studies discussed the importance of adopting artificial intelligence (IA) and machining learning technologies, beside biometric technology and automated system, in the security control application in order to improve the security level and passenger experience. On the other hand, 6% of the reviewed studies mentioned the importance of the integration between IoT and cloud technology in processing and analysing the collected information from passengers during their journey.

C. PASSENGER'S DIGITAL INFORMATION PRIVACY CHALLENGES

RQ3 is about the identification of passenger's digital information privacy challenges.

We used CFIP [31] framework to identify and categorise passenger's privacy challenges that may affect their digital information in smart airports. In Table 11, we identified 7 challenges, which are grouped into following categories: collection, error, unauthorised use, improper access. As shown in Table 11, 10% of the reviewed studies, highlighted the information privacy challenges within the collection category (C1). They include: (1) collection and transfer of PNR between airlines and countries, and also between countries as well, (2) collecting and storing big data without proper supervision may increase the privacy-preserving challenge.

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

TABLE 11. Privacy challenges of passenger's information.

Ref	Categories	Concerns	Papers	Percentage
C1	Collection	Collection and transfer of PNR and API	S21,S22	10%
		Privacy- preserving concern in big data	S7	
C2	Error	Data manipulation, deleting and losing	S22	10%
		Data-protection concern in big data.	S7	
		Data integrity concern in (FMEC)	S22	
C3	Unauthorized use	The second usage of stored data	S10,S24,S11,S22	16%
		Data leakage	S22,S5	
C4	Improper access	Unauthorized access	S22	3%

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

Improper access (C4) is the last category and includes unauthorised access challenge. Based on our review, 3% of the selected studies pointed-out the unauthorised access to the stored information in cloud servers by the cloud service provider.

D. CURRENT SOLUTION

RQ4 is about the identification of current solutions for passenger's information privacy challenges.

In addition to information privacy challenges, we carefully reviewed the selected studies in order to identify the possible privacy solutions. Based on our review, we identified 6 solutions, which are extracted from 23% of the selected studies (Table 12 maps the challenges with relevant solutions).

In Table 12, 3 types of the identified solutions were related to cryptography. For instance, Public key infrastructure (PKI) cryptographic method is proposed in order to prevent unauthorised access (C4) and securing the sharing (C1) of the information stored in e-passport, while AES algorithm is proposed to encrypt the information and biometric data in QR code in order to address the current data leakage challenge (C3) when using FRID chip in e-passports. The multi-dimensional encryption algorithm is proposed for challenge (C1) to ensure the security of shared information within the System Wide Information Management (SWIM).

TABLE 12. 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 in order to sole privacy-protection challenge 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 in order to solve the data-protection challenge in big data	S7	6%
	Fog and multi-access edge paradigm (FMEC)	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 paradigm (FMEC) to prevent the secondary use of information in cloud server	S22	
C4	Public key infrastructure (PKI) cryptographic method to secure the access to e-passport information.	S10	6%
	Fog and multi-access edge paradigm (FMEC) to prevent the unauthorised access to the information in cloud server	S22	

In order to address the challenges (C1, C2) related to big data technology, security as a service framework is proposed to monitor the data, and protect it from errors with a view to guarantee the correctness of the data and analysis result. The main idea of this framework is focused on OpenSSL authentication and attributes authorisation.

Fog and multi-access edge paradigm (FMEC) is proposed as a solution for information privacy challenges in cloud servers, which are: the secondary use of stored information (C3), unauthorised access to the stored information (C4), and modifying the stored information (C2).

As shown in Table 12, 6% of the reviewed studies discussed the European Union (EU) agreements that outline the role of PNR transfer between EU and other countries. The EU agreements considered as a solution for sharing passenger's information (C1). Since 2011, the EU agreements were signed in September between EU and Australia, and in December between EU and USA [39]. However, a new agreement between EU and Canada was launched in 2018, and it was under negotiation as mentioned in [39].

E. PASSENGER'S INFORMATION STANDARDS AND PRIVACY REGULATIONS

Privacy administrative and constitutional laws, besides polices, play a vital role to address the privacy concerns [40].

TABLE 13. Standards for passenger's information in the aviation industry.

Governing body	Description	Papers	Percentage
ICAO	Introduced standards for biometric data, biographic/passport data.	S10,S16,S5 ,S20,S12,S 30	19%
ISO/IEC	Standards ISO/IEC 29794 & ISO/IEC 19794 to address the quality of biometric data.	S10	3%
Frontex, NIST	Contributing in formulating standards and for biometric information.	S30	3%
EN, ISA/IEC, ENISA	List of standards for the aviation industry	S12,S15,S1 8	10%

We identified and extracted the standards and policies relevant to passenger's information in aviation industry from 26% of the selected studies. In Table 13, the biometric data needs to be adhered to standards (ISO/IEC 29794 & ISO/IEC 19794) to ensure the quality of the collected biometric data. Based on our review, 19% of the selected studies mentioned the role of International Civil Aviation Organization (ICAO) in developing standards for biometric/biographic information, and e-passport, while 3% mentioned that the European Border and Coast Guard Agency (Frontex), and National Institute of Standards and Technology (NIST) also contribute to formulating standards for biometric information in the e-gate context. A list of relevant standards to the aviation industry is stated in 10% of the reviewed studies.

We also performed a manual search to identify and include the recent relevant known information privacy regulations to complement this academic SLR study. We focused on the most recent general Data Protection Regulation (GDPR), which was adopted by the EU in 2018 and included its principle for processing personal information [41]. Also, Australian privacy principle (APPs), which are set out in the Privacy Act 1988(Act) to govern the use of PII [42]. Table 14 includes details about these two important regulations in the context of smart airports. It is worth noting here that the manual research results were used to cover information privacy regulations in smart airports and were not critically analysed. Thus, those results are not included in the total number of the selected studies.

VI. DISCUSSION

This study discussed a number of important aspects relevant to the passenger's digital information privacy in smart airports. It used SLR method to capture the passenger's travel journey and the underpinning elements of people, process, information and technology. It also identified privacy challenges of passenger's digital information and relevant possible solutions. To provide a broader coverage, this study also included privacy regulations and standards related to passenger's information in the context of aviation industry.

The results of this SLR indicate that there is an increasing interest in the topics related to smart airports and the

TABLE 14. GDPR And APPs privacy regulation in Australian and European airports.

	Description
GDPR	GDPR allows airport of all sizes to ensure that passenger data are kept safe and protected for collection, storage and dissemination [43].
	GDPR Article 5 includes the principle of personal data processing. While Article 44 and Article 50 covers the transfers of personal data to third countries or between international organisations[44].
(APPs)	The Australian Airport Association (AAA) applies the Australian Privacy Principles (APPs) to guarantee the privacy of the passenger's information held by it[45].
	The Australian Privacy Principles consists of 13 principles to govern standards, rights for the following[42]: -Collect, utilize and reveal the personal data. - The responsibility and governance of organizations. - Correct the personal data - Access personal data by individuals.

privacy challenges of passenger's digital information. About 324 studies were selected from well-known selected database in the initial stage of this study, then final 31 relevant studies were reviewed and evaluated in order to address the research questions in hand.

A. FINDINGS AND FUTURE DIRECTION

The privacy and security issues of using several technologies such as RFID, IoT, and cloud and fog computing has been investigated in the literature. According to Ohkubo, *et al.* [46], Ayoade [47], using FRID could affect personal privacy as the collected information can be leaked without users knowledge and can also be used for other purposes. Furthermore, the use of IoT devices in handling personal information may cause a number of security and privacy issues [48], [49]. Imine, *et al.* [50] mentioned that privacy is becoming one of the major concerns when personal information is shared through cloud and fog computing. This is because that there is a possibility of personal information leakage and activity tracking such as travel journey. Based on Table 10, our findings reveal that the majority of the reviewed studies (62%) focused on enabling technologies, which are used to support smart airport applications without considering the privacy issues that may arise when using those technologies. However, only one study proposed a framework to encrypt passenger's information, which is stored in e-passport using QR code as a countermeasure of the current security issues when using RFID chip. Since the protection of passenger's digital information is essential, future research is needed to address the implications of enabling technologies in terms of privacy of passenger information in smart airports.

Passenger's digital information is collected and shared among several stakeholders (airlines, airports and government agencies) Agrawal [51] defined the digital information as an invisible piece of information that needs to be visible by using hardware and software technologies. The characteristics of digital information are also described as follows: ''dependency, multipliable, dynamic, economic, modular, and delicate''. Our notable findings in Table 7, to the best of our knowledge, the reviewed selected studies have not outlined how the stakeholders handle passenger's information that is collected during their travel journey. As a result, there are concerns of using the collected information for other purposes without passengers' consent. On the other hand, there is no standardised system to verify the mechanism of sharing passenger's digital information between airlines and governments (border control authorities). Considering the above, there is a need for developing a trusted framework for sharing passenger information among multiple stakeholders. This should consider passenger's consent and control over the access of their information. This draws our attention to another important future research direction.

There is an increasing interest among academic community in information privacy concerns. According to Choi, *et al.* [52], the majority of literature discussed information privacy concerns based on the Concerns for Information Privacy framework (CFIP) – provided by Van Slyke, *et al.* [31], or the Internet Users' Information Privacy Concerns (IUIPC) - provided by Malhotra, *et al.* [53]. In this study, we used CFIP framework in order to identify and categorise the passenger's digital information privacy in the selected studies in the specific context of smart airports. As noted in Table 11, a number of information privacy challenges were identified. However, the reviewed studies did not provide any concrete or explicit guidance on linking the privacy challenges to the stages of passenger travel journey. It appears to be still an area of further research.

In Table 12, although, we identified current solutions for the mentioned privacy concerns in Table 11. However, 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 mentioned privacy challenges in this study have remained unsolved. Those challenges are secondary use of information stored in government's database, the data leakage and data modification challenges in fog computing. Based on Table 12, most proposed solutions are about encryption methods. Encryption, biometrics, anonymity, and access control solutions have been proposed (be implemented) to preserve the individual privacy in smart city [8], [49], [54]. However, Cui, *et al.* [55] stated that such encryption methods are not sufficient for the current context of smart environment. Similarly, Labati, *et al.* [56] mentioned that conventional cryptographic methods are not suitable for biometric data. The authors proposed ad-hoc methods (to be used) for protecting diametric data. It is thus necessary to investigate and develop more relevant solutions involving privacy enhancing technologies (PETs) and methods (e.g. Blockchain) to ensure passenger's digital information privacy in smart airports.

There is also a lack 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, based on Table 13, only

TABLE 15. Final selected studies.

S1	R. AlMashari, G. AlJurbua, L. AlHoshan, N. S. A. Saud, O. BinSaeed, and N. Nasser, "IoT-based Smart Airport Solution," presented at the 2018 International Conference on Smart Communications and Networking (SmartNets), Yasmine Hammamet, Tunisia, Tunisia, 2018.
S2	A. Rajapaksha and N. Jayasuriya, "Smart Airport: A Review on Future of the Airport Operation," Global Journal of Management and Business Research, vol. 20, 03/09 2020, doi: 10.34257/GJMBRAVOL20IS3PG25.
S3	W. Shehieb, H. Al Sayed, M. M. Akil, M. Turkman, M. A. Sarraj, and M. Mir, "A smart system to minimise mishandled luggage at airports," presented at the PIC 2016 - Proceedings of the 2016 IEEE International Conference on Progress in Informatics and Computing
S4	R. D. Labati, A. Genovese, E. Muñoz, V. Piuri, F. Scotti, and G. Sforza, "Advanced design of Automated Border Control gates: Biometric system techniques and research trends," presented at the 2015 IEEE International Symposium on Systems Engineering (ISSE), Rome, Italy, 2015
S5	Z. H. Choudhury and M. M. A. Rabbani, "Biometric Passport for National Security Using Multibiometrics and Encrypted Biometric Data Encoded in the QR Code," Journal of Applied Security Research, Article vol. 15, pp. 1-31, 2019, doi: 10.1080/19361610.2019.1630226.
S6	C. Morosan, "An empirical examination of U.S. travelers' intentions to use biometric e-gates in airports," Journal of Air Transport Management, vol. 55, pp. 120-128, 2016/08/01/ 2016, doi: https://doi.org/10.1016/j.jairtraman.2016.05.005.
S7	W. Zhijun and W. Caiyun, "Security-as-a-service in big data of civil aviation," presented at the 2015 IEEE International Conference on Computer and Communications (ICCC), Chengdu, China, 2016.
S8	A. Vedaschi, "Privacy and data protection versus national security in transnational flights: the EU–Canada PNR agreement," (in English), International Data Privacy Law, vol. 8, no. 2, pp. 124-139, 2018, doi: doi.org/10.1093/idpl/ipy004.
S9	J. Cano, A. Pollini, L. Falciani, and U. Turhan, "Modeling current and emerging threats in the airport domain through adversarial risk analysis," Journal of Risk Research, Article vol. 19, no. 7, pp. 894-912, 2016, doi: 10.1080/13669877.2015.1057201.
S10	R. D. Labati, A. Genovese, E. Muñoz, V. Piuri, F. Scotti, and G. Sforza, "Biometric Recognition in Automated Border Control: A Survey," ACM Comput. Surv., vol. 49, no. 2, p. Article 24, 2016, doi: 10.1145/2933241.
S11	Z. Zhang, "Technologies Raise the Effectiveness of Airport Security Control," presented at the 2019 IEEE 1st International Conference on Civil Aviation Safety and Information Technology (ICCASIT), Kunming, China, China, 2020.
S12	G. Lykou, A. Anagnostopoulou, and D. Gritzalis, "Smart airport cybersecurity: Threat mitigation and cyber resilience controls," Sensors (Switzerland), Article vol. 19, no. 1, 2019, doi: 10.3390/s19010019.
S13	S. Bouyakoub, A. Belkhir, W. Guebli, and F. M. Bouyakoub, "Smart airport: An IoT-based Airport Management System," presented at the ICFNDS '17 International Conference on Future Networks and Distributed Systems, New York, NY, USA, 2017.
S14	S. Kalakou, V. Psaraki-Kalouptsidi, and F. Moura, "Future airport terminals: New technologies promise capacity gains," Journal of Air Transport Management, vol. 42, pp. 203-212, 2015.
S15	G. Lykou, A. Anagnostopoulou, and D. Gritzalis, "Implementing cyber-security measures in airports to improve cyber-resilience," presented at the 2018 Global Internet of Things Summit GIoTS Bilbao, Spain, 2018, Conference Paper.
S16	A. Anand et al., "Enhancing Fingerprint Biometrics in Automated Border Control with Adaptive Cohorts," presented at the Proceedings of 2016 Ieee Symposium Series on Computational Intelligence, Athens, Greece, 2017.
S17	Z. Wu, L. Liu, C. Yan, J. Xu, and J. Lei, "The approach of SWIM data sharing based on multi-dimensional data encryption," presented at the 2017 25th International Conference on Software, Telecommunications and Computer Networks (SoftCOM), Split, Croatia, 2017.
S18	F. M. Siddiqui, "Digital Transformation of Modern Airports by Exploiting Fog as a Service Model," presented at the 2019 Integrated Communications, Navigation and Surveillance Conference (ICNS), Herndon, VA, USA, USA, 2019.
S19	N. Le, Y. Zheng, Q. Huang, and Y. Pei, "Prospect of 5g application in civil airport," presented at the Proceedings of 2019 IEEE 1st International Conference on Civil Aviation Safety and Information Technology, ICCASIT 2019, Kunming, China, China, 2020, Conference Paper.
S20	J. S. d. Río, C. Conde, A. Tsitiridis, J. R. Gómez, I. M. d. Diego, and E. Cabello, "Face-based recognition systems in the ABC e-gates," presented at the 2015 Annual IEEE Systems Conference (SysCon) Proceedings, 10.1109/SYSCON.2015.7116774, 2015.
S21	H. Chang-Ryung, R. McGauran, and H. Nelen, "API and PNR data in use for border control authorities," (in English), Security Journal, vol. 30, no. 4, pp. 1045-1063, 2017, doi: 10.1057/sj.2016.4.
S22	P. Tedeschi and S. Sciancalepore, "Edge and Fog Computing in Critical Infrastructures: Analysis, Security Threats, and Research Challenges," presented at the 2019 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), Stockholm, Sweden, Sweden, 2019.
S23	M. Han, L. Li, X. Peng, Z. Hong, and M. Li, "Information Privacy of Cyber Transportation System: Opportunities and Challenges," presented at the Proceedings of the 6th Annual Conference on Research in Information Technology, Rochester, New York, USA, 2017.
S24	I. A. Khi, "Ready for take-off: how biometrics and blockchain can beat aviation's quality issues," Biometric Technology Today, vol. 2020, no. 1, pp. 8-10, 2020, doi: 10.1016/S0969-4765(20)30010-2.
S25	G. Karakuş, E. Karşıgil, and L. Polat, "The Role of IoT on Production of Services: A Research on Aviation Industry," in Proceedings of the International Symposium for Production Research 2018, N. M. Durakbasa and M. G. Gencyilmaz, Eds. Cham: Springer International Publishing, 2019, pp. 503-511.
S26	V. Bogicevic, M. Bujisic, A. Bilgihan, W. Yang, and C. Cobanoglu, "The impact of traveler-focused airport technology on traveler satisfaction," Technological Forecasting and Social Change, vol. 123, pp. 351-361, 2017/10/01/ 2017, doi: 10.1016/j.techfore.2017.03.038.
S27	S. E. Zaharia and C. V. Pietreanu, "Challenges in airport digital transformation," Transportation Research Procedia, vol. 35, pp. 90-99, 2018/01/01/ 2018, doi: https://doi.org/10.1016/j.trpro.2018.12.016.
S28	N. A. R. Negri, G. M. R. Borille, and V. A. Falcão, "Acceptance of biometric technology in airport check-in," Journal of Air Transport Management, vol. 81, p. 101720, 2019/10/01/ 2019, doi: https://doi.org/10.1016/j.jairtraman.2019.101720.
S29	Z. Alansari, S. Soomro, and M. R. Belgaum, "Smart Airports: Review and Open Research Issues," in Emerging Technologies in Computing. Cham: Springer International Publishing, 2019, pp. 136-148.
S30	J. Sanchez del Rio, D. Moctezuma, C. Conde, I. Martin de Diego, and E. Cabello, "Automated border control e-gates and facial recognition systems," Computers & Security, vol. 62, pp. 49-72, 2016/09/01/ 2016, doi: https://doi.org/10.1016/j.cose.2016.07.001.
S31	D. Ortega, A. Fernández-Isabel, I. Martín de Diego, C. Conde, and E. Cabello, "Dynamic facial presentation attack detection for automated border control systems," Computers & Security, vol. 92, p. 101744, 2020/05/01/ 2020, doi: https://doi.org/10.1016/j.cose.2020.101744

19% of the selected studies briefly mentioned the ICAO standards, policies and recommendations for biometric and biographic/passport information. Thus, there is clearly an increasing need and scope for academic research in this important area of privacy regulation and standards for ensuring passenger's information privacy in smart airports.

B. LIMITATION

Like any other SLR, this work has some limitations. Firstly, it is important to mention that we selected six well-known databased in conducting this SLR. This was done to ensure that the research topic is sufficiently addressed; however, the selected studies are limited to only these databases. Secondly, the keywords and search terms were generated based on the research questions and tested across several databases. Also, the multistage process was reviewed to ensure the coverage of the research topic before the documentation stage. The quality assessment criteria were reviewed and revised many times to avoid the researcher bias and ensure the relevance and quality of final selected studies. Nevertheless, research is an ongoing process, and we did our best to ensure that our search methodology has not caused any omission of relevant studies on purpose. Furthermore, in order to minimise the possibility of human error, when conducting and applying research method, fortnightly review meetings were held with the senior researcher and author of this study to ensure that the selected studies and results are of a good quality.

VII. CONCLUSION

Smart airport is undoubtedly a key part of the smart city concept that will not only help personalise passenger experiences but also help airport operators in managing their operations more efficiently while ensuring cost-effectiveness. However, several passenger's digital information privacy concerns need to be addressed as highlighted in this SLR study. This study synthesised and analysed the results using customer journey map (CJM) and concerns for privacy information (CFIP) as theoretical lens. Based on CFIP framework, 7 types of passenger's digital information privacy challenges were identified and categorised into collection, error, unauthorised use, and improper access. Furthermore, we mapped the identified challenges to the current solutions, which were extracted from selected studies. Finally, we identified the relevant standards and policies related to passenger's information, and investigated the information privacy regulations from Europe and Australia. Based on our findings, it can be suggested that contemporary solutions for digital information privacy challenges are needed to improve the privacy level of passenger's digital information in smart airports. This SLR can benefit researchers to get a better understanding of passenger's information privacy in smart airports and provides foundations for further work in this important area of research. This research provided a foundation and rationale for the development of a trusted and privacy-preserving passenger digital information sharing framework for the specific context of smart airports.

APPENDIX A

See Table 15.

REFERENCES

[1] IATA. (2019). *Annual Review 2019*. Accessed: Feb. 10, 2021. [Online]. Available: https://www.iata.org/contentassets/c81222d96c9a4e0bb4ff6ced0126f0bb/iata-annual-review-2019.pdf
[2] IATA. *IATA Forecast Predicts 8.2 Billion Air Travelers in 2037*. Accessed: Feb. 11, 2021. [Online]. Available: https://www.iata.org/EN/PRESSROOM/PR/2018-10-24-02/
[3] J. B. Nau and F. Benoit. (2017). Smart airport how technology is shaping the future of airports. Wavestone. [Online]. Available: https://www.wavestone.com/app/uploads/2017/12/Smart-Airport-2017.pdf
[4] *SITA Launches its Single Biometric Solution*. Accessed: Feb. 16, 2021. [Online]. Available: https://www.passengerselfservice.com/2016/03/sita-launches-its-single-biometric-solution/
[5] P. Leonard, "Customer data analytics: Privacy settings for 'big data' business," *Int. Data Privacy Law*, vol. 4, no. 1, pp. 53–68, Feb. 2014, doi: 10.1093/IDPL/IPT032.
[6] R. Zhang, G. Liu, J. Liu, and J. P. Nees, "Analysis of message attacks in aviation data-link communication," *IEEE Access*, vol. 6, pp. 455–463, 2018, doi: 10.1109/access.2017.2767059.
[7] S. Keele, "Guidelines for performing systematic literature reviews in software engineering," EBSE, Goyang-si, South Korea, EBSE Tech. Rep., Version 2.3, 2007, vol. 5.
[8] A. S. Elmaghraby and M. M. Losavio, "Cyber security challenges in smart cities: Safety, security and privacy," *J. Adv. Res.*, vol. 5, no. 4, pp. 491–497, 2014, doi: 10.1016/j.jare.2014.02.006.
[9] T. Braun, B. C. M. Fung, F. Iqbal, and B. Shah, "Security and privacy challenges in smart cities," *Sustain. Cities Soc.*, vol. 39, pp. 499–507, May 2018, doi: 10.1016/j.scs.2018.02.039.
[10] R. Giffinger, C. Fertner, H. Kramar, R. Kalasek, N. Milanović, and E. Meijers, "Smart cities—Ranking of European medium-sized cities," Centre Regional Sci., Vienna Univ. Technol., Vienna, Austria, 2007.
[11] A. Kirimtat, O. Krejcar, A. Kertesz, and M. F. Tasgetiren, "Future trends and current state of smart city concepts: A survey," *IEEE Access*, vol. 8, pp. 86448–86467, 2020, doi: 10.1109/ACCESS.2020.2992441.
[12] Office of the Government Chief Information Officer, "Smart city development in Hong Kong," *IET Smart Cities*, vol. 1, no. 1, pp. 23–27, Jun. 2019, doi: 10.1049/iet-smc.2019.0036.
[13] E. Nagy and C. Csiszar, "Airport smartness index—Evaluation method of airport information services," *Osterreichische Zeitschrift Fur Verkehrswissenschaft*, vol. 63, no. 4, pp. 25–30, 2016.
[14] ENISA. (2016). *Securing Smart Airports*. Accessed: Feb. 9, 2021. [Online]. Available: https://www.enisa.europa.eu/publications/securing-smart-airports
[15] The Aviation Valuables Inside Information Technology. *Smart Airport*. Accessed: Feb. 9, 2021. [Online]. Available: http://www.tavtechnews.com/pdf/SMART-AIRPORT.pdf
[16] V. Narula. *Smart Airports*. Accessed: Jul. 1, 2020. [Online]. Available: https://www.icao.int/safety/iStars/Documents/IUG%20Meeting%201/Presentations/Smart%20Airports%20-%20Vijay%20Narula.pdf
[17] A. Rajapaksha and D. N. Jayasuriya, "Smart airport: A review on future of the airport operation," *Global J. Manage. Bus. Res.*, vol. 12, pp. 25–34, Feb. 2020, doi: 10.34257/GJMBRAVOL20IS3PG25.
[18] G. Lykou, A. Anagnostopoulou, and D. Gritzalis, "Implementing cyber-security measures in airports to improve cyber-resilience," presented at the Global Internet Things Summit (GIoTS), 2018.
[19] G. Karakuş, E. Karşıgil, and L. Polat, "The role of IoT on production of services: A Research on aviation industry," presented at the Int. Symp. Prod. Res. (ISPR). Cham, Switzerland: Springer, 2019.
[20] IATA. *API-PNR Toolkit*. Accessed: Jul. 3, 2020. [Online]. Available: https://www.iata.org/en/publications/api-pnr-toolkit/
[21] I. A. Khi, "Ready for take-off: How biometrics and blockchain can beat aviation's quality issues," *Biometric Technol. Today*, vol. 2020, no. 1, pp. 8–10, 2020, doi: 10.1016/S0969-4765(20)30010-2.
[22] IATA. *Facilitation and Passenger Data*. Accessed: Jul. 3, 2020. [Online]. Available: https://www.iata.org/en/programs/passenger/passenger-data/
[23] L. J. Hoffman, *Modern Methods for Computer Security and Privacy*. Englewood Cliffs, NJ, USA: Prentice-Hall, 1977.
[24] Lexico. *Privacy*. Accessed: Sep. 11, 2019. [Online]. Available: https://www.lexico.com/en/definition/privacy

[25] A. Martinez-Balleste, P. A. Perez-Martinez, and A. Solanas, "The pursuit of citizens' privacy: A privacy-aware smart city is possible," *IEEE Commun. Mag.*, vol. 51, no. 6, pp. 136–141, Jun. 2013, doi: 10.1109/MCOM.2013.6525606.
[26] D. J. Solove, "A taxonomy of privacy," *Univ. PA Law Rev.*, vol. 154, no. 3, pp. 477–564, 2006, doi: 10.2307/40041279.
[27] H. Smith, S. Milberg, and S. J. Burke, "Information privacy: Measuring individuals' concerns about organizational practices," *MIS Quart.*, vol. 20, no. 2, pp. 167–196, 1996, doi: 10.2307/249477.
[28] D. Eckhoff and I. Wagner, "Privacy in the smart city—Applications, technologies, challenges, and solutions," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 1, pp. 489–516, 1st Quart., 2018, doi: 10.1109/COMST.2017.2748998.
[29] R. L. Finn, D. Wright, and M. Friedewald, "Seven types of privacy," in *European Data Protection: Coming of Age*. Dordrecht, The Netherlands: Springer, 2012, pp. 3–32.
[30] M. S. Rosenbaum, M. L. Otalora, and G. C. Ramírez, "How to create a realistic customer journey map," *Bus. Horizons*, vol. 60, no. 1, pp. 143–150, Jan. 2017, doi: 10.1016/j.bushor.2016.09.010.
[31] C. Van Slyke, J. Shim, R. Johnson, and J. Jiang, "Concern for information privacy and online consumer purchasing," *J. Assoc. Inf. Syst.*, vol. 7, no. 6, pp. 415–444, Jun. 2006, doi: 10.17705/1jais.00092.
[32] B. Willemsen and M. Cadee, "Extending the airport boundary: Connecting physical security and cybersecurity," *J. Airport Manage.*, vol. 12, no. 3, pp. 236–247, 2018.
[33] N. A. R. Negri, G. M. R. Borille, and V. A. Falcão, "Acceptance of biometric technology in airport check-in," *J. Air Transp. Manage.*, vol. 81, Oct. 2019, Art. no. 101720, doi: 10.1016/j.jairtraman.2019.101720.
[34] IATA. *Smart Security Getting Smarter*. Accessed: Jul. 13, 2020. [Online]. Available: https://airlines.iata.org/analysis/smart-security-getting-smarter#:~:text=Smart%20Security%20is%20a%20blending,adopted%20the%20Smart%20Security%20name
[35] Z. Zhang, "Technologies raise the effectiveness of airport security control," presented at the IEEE 1st Int. Conf. Civil Aviation Saf. Inf. Technol. (ICCASIT), Kunming, China, Oct. 2019.
[36] H. Harteveldt. *The Future of Airline Distribution 2016–2021*. Accessed: Feb. 9, 2021. [Online]. Available: https://www.iata.org/contentassets/6de4dce5f38b45ce82b0db42acd23d1c/ndc-future-airline-distribution-report.pdf
[37] V. Patel, "Airport passenger processing technology: A biometric airport journey," Dept. Electr., Comput., Softw., Syst. Eng., Embry-Riddle Aeronaut. Univ., Daytona Beach, FL, USA, Tech. Rep., 2018.
[38] ICAO. *Security and Facilitation*. Accessed: Jul. 4, 2020. [Online]. Available: https://www.icao.int/Security/FAL/PKD/Pages/ePassportBasics.aspx
[39] European Commission. *Passenger Name Record (PNR)*. Accessed: Feb. 11, 2021. [Online]. Available: https://ec.europa.eu/home-affairs/what-we-do/policies/police-cooperation/information-exchange/pnr_en
[40] J. S. Hiller and J. M. Blanke, "Smart cities, big data, and the resilience of privacy," *Hastings LJ*, vol. 68, no. 2, p. 309, 2016.
[41] B. Wolford. *What is GDPR, the EU's New Data Protection Law?* Accessed: Feb. 2, 2020. [Online]. Available: https://gdpr.eu/what-is-gdpr/
[42] OAIC. *Australian Privacy Principles*. Accessed: Jun. 2, 2020. [Online]. Available: httpS://WWW.OAIC.GOV.AU/PRIVACY/AUSTRALIAN-PRIVACY-PRINCIPLES/
[43] N. Robson. *How GDPR is Affecting Airports*. Accessed: Jun. 2, 2020. [Online]. Available: https://www.rezcomm.com/blog/2019/07/16/gdpr-affecting-airports/
[44] Intersoft Consulting. *General Data Protection Regulation (GDPR)*. Accessed: Jun. 2, 2020. [Online]. Available: https://gdpr-info.eu/
[45] Australian Airport Association. *Privacy Policy*. Accessed: Jun. 2, 2020. [Online]. Available: httpS://AIRPORTS.ASN.AU/PRIVACY-POLICY/
[46] M. Ohkubo, K. Suzuki, and S. Kinoshita, "Efficient hash-chain based RFID privacy protection scheme," in *Proc. Int. Conf. Ubiquitous Comput., Workshop Privacy, Current Status Future Directions*, Jan. 2004.
[47] J. Ayoade, "Security implications in RFID and authentication processing framework," *Comput. Secur.*, vol. 25, no. 3, pp. 207–212, May 2006, doi: 10.1016/j.cose.2005.11.008.
[48] I. Makhdoom, M. Abolhasan, J. Lipman, R. P. Liu, and W. Ni, "Anatomy of threats to the Internet of Things," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 2, pp. 1636–1675, 2nd Quart., 2019, doi: 10.1109/COMST.2018.2874978.
[49] R. H. Weber, "Internet of Things—New security and privacy challenges," *Comput. Law Secur. Rev.*, vol. 26, no. 1, pp. 23–30, Jan. 2010, doi: 10.1016/j.clsr.2009.11.008.
[50] Y. Imine, A. Lounis, and A. Bouabdallah, "An accountable privacy-preserving scheme for public information sharing systems," *Comput. Secur.*, vol. 93, Jun. 2020, Art. no. 101786, doi: 10.1016/j.cose.2020.101786.
[51] P. R. Agrawal, "Digital information management: Preserving tomorrow's memory," in *Cloud Computing and Virtualization Technologies in Libraries*. Hershey, PA, USA: IGI Global, 2014, pp. 22–35.
[52] H. S. Choi, W. S. Lee, and S. Y. Sohn, "Analyzing research trends in personal information privacy using topic modeling," *Comput. Secur.*, vol. 67, pp. 244–253, Jun. 2017, doi: 10.1016/j.cose.2017.03.007.
[53] N. K. Malhotra, S. S. Kim, and J. Agarwal, "Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model," *Inf. Syst. Res.*, vol. 15, no. 4, pp. 336–355, Dec. 2004, doi: 10.1287/isre.1040.0032.
[54] K. Zhang, J. Ni, K. Yang, X. Liang, J. Ren, and X. S. Shen, "Security and privacy in smart city applications: Challenges and solutions," *IEEE Commun. Mag.*, vol. 55, no. 1, pp. 122–129, Jan. 2017, doi: 10.1109/MCOM.2017.1600267CM.
[55] L. Cui, G. Xie, Y. Qu, L. Gao, and Y. Yang, "Security and privacy in smart cities: Challenges and opportunities," *IEEE Access*, vol. 6, pp. 46134–46145, 2018, doi: 10.1109/ACCESS.2018.2853985.
[56] R. D. Labati, A. Genovese, E. Muñoz, V. Piuri, F. Scotti, and G. Sforza, "Biometric recognition in automated border control: A survey," *ACM Comput. Surv.*, vol. 49, no. 2, p. 24, 2016.

MAHA IBRAHIM ALABSI received the master's degree in information technology from the University of Melbourne, Melbourne, Australia. She is currently pursuing the Ph.D. degree with the Faculty of Engineering and Information Technology (FEIT), University of Technology Sydney, Australia. She investigates the privacy of digital information for passengers in smart airport. Her research interests include information privacy, smart cities, and privacy regulation and standards.

ASIF QUMER GILL received the M.Sc. degree in computing science and master of business and the Ph.D. degree in computing science. He is currently a Result-Oriented Academic cum Practitioner with extensive more than 20 years' experience in various sectors of IT, including banking, consulting, education, finance, government, non-profit, software, and telecommunication. He is also an Associate Professor and the Director of the DigiSAS Laboratory, School of Computer Science, University of Technology Sydney, Australia. He specializes in adaptive enterprise architecture and information-centric secure digital ecosystems.