Journal of the Knowledge Economy
https://doi.org/10.1007/s13132-024-02126-1

A Systematic Review of Personal Information Sharing in Smart Cities: Risks, Impacts, and Controls

Maha Ibrahim Alabsi[1,2] · **Asif Qumar Gill**[1]

Received: 19 October 2023 / Accepted: 2 June 2024
© The Author(s) 2024

Abstract
Smart cities aim to deliver smart services that rely on emerging technologies to their users. In order for users to get the provided services, they need to share their personal information with different parties. However, sharing personal information in smart cities may impact the privacy of that information. Thus, there is a need to address privacy risks relevant to sharing personal information in smart cities. This study aims to address this issue by conducting a systematic literature review (SLR) to identify and extract privacy risks, impacts, and existing controls associated with sharing personal information, considering elements involved and interacting during the sharing activity in smart cities. A set of 83 selected studies in both academic and industry fields were reviewed, and the results were categorised into three main groups: privacy risks, impacts, and controls. Moreover, the implications and future research directions were also reported. The proposed privacy risk taxonomy will provide a much-needed foundation for the industry and research community, intending to research and evaluate privacy risk frameworks and design solutions for sharing personal information in smart cities.

Keywords Information privacy · Privacy risk · Privacy requirements · Privacy control · Smart city · Privacy risk assessment

✉ Maha Ibrahim Alabsi
mabsi@taibahu.edu.sa

Asif Qumar Gill
Asif.Gill@uts.edu.au

[1] Faculty of Engineering and Information Technology, School of Computer Science, University of Technology Sydney, Ultimo, Sydney, NSW 2007, Australia

[2] Applied College, Taibah University, Al-Madinah Al-Munawarrah, Madina, Saudi Arabia

Published online: 24 June 2024

Introduction

More recently, the concept of smart cities has been getting significant attention from research and practice perspectives (Ahmad Mohamad et al., 2019). Several countries across the globe (e.g. Asia, Africa, America, and Europe) aim to consider their cities "smart" by developing and delivering smart services to their citizens and residents by using emerging ICT (information and communication technologies) (Ahmad Mohamad et al., 2019; Albino et al., 2015; Hsiao et al., 2021). The definitions of smart cities focus on the quality of citizens' performance and activities, along with enhancing economic competitiveness by managing city resources and improving information and communications technology (ICT) infrastructure (Giffinger et al., 2007, Caragliu et al. 2009, Vu & Hartley, 2018). Also, smart city is defined as a 4th industrial model where emerging technologies, such as the Internet of Things, cloud computing, and big data, are used to optimise the cities (Safiullin et al., 2019). Accordingly, smart cities are proposed in particular areas or sectors such as governments, health, energy, buildings, airports, and businesses/organisations (Khatoun & Zeadally, 2017).

Due to the strong relationship between ICT and smart services within the overarching concept of smart cities, a vast amount of personal information is collected from users, devices, and applications (Martinez-Balleste et al., 2013). Furthermore, sharing and exchanging information among parties, including individuals and organisations, is possible using different sharing platforms that play a vital role in smart cities (Kong et al., 2018, Kusumastuti et al., 2022). Internet of Things (IoT), Cloud, fog computing, and blockchain technology are examples of such platforms (Qian et al., 2018, Imine et al., 2020; Gill, 2021). However, the flow of personal information in smart cities may result in individuals suffering from serious privacy risks that may impact their information (Martinez-Balleste et al., 2013, Sharma et al., 2020).

According to NIST (Stoneburner et al., 2002), the risk is the possibility of a threat source exploiting a specific information system vulnerability and the resultant consequence. Assessing information privacy risks in smart cities is challenging due to information complexity and uncertain impact levels (Bogoda et al., 2019). In addition, privacy risks need to be assessed to minimise the risk impact by using appropriate controls (Hong et al., 2004). Thus, there is a need to assess privacy risks when sharing personal information in smart cities. This includes identifying and addressing privacy threats and vulnerabilities, their impacts, and appropriate privacy risk mitigation controls.

To the best of our knowledge, there is a lack of consolidated literature on this important topic of privacy assessments that cover privacy risks, impacts, and current controls for sharing personal information, considering the interaction among elements involved in sharing activity in smart cities. A consolidated view of the current work is needed to provide a foundation for further development in this important area of research.

Thus, this paper addresses this need by conducting a SLR and synthesising published research with a view to identify and extract privacy risks, impacts,

existing controls, and elements involved and interacting to share personal information in smart cities, along with relevant regulation, to influence this activity. Thus, this paper focuses on the following key research questions:

RQ1: What are the privacy risks associated with sharing personal information in the context of smart cities considering the elements involved and interacting while sharing personal information?
RQ2: What are the impacts of those personal information privacy risks?
RQ3: What current privacy controls are in place to mitigate the identified risks?

Motivation

This work builds on the earlier research on identifying privacy risks in smart airports (Alabsi & Gill, 2021). This paper extended this work to provide broader coverage of smart cities. This will help extract and define more comprehensive views of privacy risks, which will be used to design a holistic solution for assessing the privacy risks that may impact passengers' personal information in their interaction journey in smart airports within the border context of smart cities. This will ensure that important privacy concerns are not overlooked when dealing with information privacy in smart airports. The main motivation behind this paper is the future development of the privacy framework in a smart airport context. The development of the proposed framework is beyond this paper's scope and is subject to further research.

Contribution

The key contributions of this research are outlined below:

- This paper provides an updated knowledge base covering various articles published in academic and industrial databases between 2017 and 2021, including smart cities, sharing information, privacy risk, impact, and existing control.
- This paper provides both a theoretical and practical view of the review results by using the Adaptive EA and Concerns for Information Privacy framework (CFIP) as a theoretical lens and the NIST 800–30 framework as a practical lens. These lenses help identify the risk assessment components: privacy risk, the resulting impact, and current privacy control.
- This paper contributes to enhancing the understanding of the review results by proposing a privacy risk taxonomy using the Concerns for Information Privacy framework (CFIP) as a theoretical lens. Based on CFIP, the proposed taxonomy categorises threats and vulnerabilities into the following: collection, error, unauthorised use, and improper access types.
- This paper provides novel knowledge by mapping the privacy risks associated with sharing personal information with elements involved and interacting during the sharing activity by adopting the Adaptive EA framework as a theoretical lens. The mapping links the privacy risks dimensions under CFIP with the layers of Adaptive EA, including human, technology, facility, and environmental.

- This paper provides a set of actionable knowledge by providing a clear understanding and mapping of the identified privacy threats to the requirements and available existing controls.
- This paper provides future research directions regarding the privacy risks of sharing personal information in smart cities.

In a nutshell, this research provides a knowledge foundation, which can be casted into developing theoretical and practical frameworks and solutions for studying and enhancing personal information privacy in the contemporary context of smart cities.

This paper is organised as follows: the "Background and Related Work" section provides the research background and related works. The "Research Method" section explains the research method. Then, data extraction and synthesis are discussed in the "Data Extraction and Synthesis" section, followed by the SLR results in the "Results" section. The discussion of implications, study validity and limitations, and work directions is elaborated in the "Discussion" section. The last section encompasses the conclusion.

Background and Related Work

The meaning of privacy varies from one researcher to another. However, core components are common to most definitions of privacy. The most historical definition of privacy was "the right to be let alone" (Warren & Brandeis, 1890). Information privacy is defined as the relationship between an individual's right to privacy and the ability to access and control the information held by organisations (Cranor, 2012; Hoffman, 1977; Hough, 2009; Martinez-Balleste et al., 2013). At present, many definitions of privacy have been proposed, and through the years, these definitions have evolved based on societal changes and technological development (Hiller & Russell, 2017; Li & Palanisamy, 2018; Peppet, 2014).

The smart city context has recently risen, and technology has gradually developed. A smart city is identified as an urban area that uses information and communication technology (ICT) to improve its services and enhance its residents' quality of life (Giffinger et al., 2007; Kusumastuti et al., 2022). As a result, the individual shares their personal information with service providers, who share it with other organisations either explicitly—implying that the user is involved—or implicitly without the user's knowledge (Spiekermann & Cranor, 2008). Personal information can be used to identify an individual, either directly or indirectly, such as name, email, or biometric information email (Wolford, 2020).

Accordingly, information privacy and security concerns have been significantly increased because cities are digitally connected, and individuals' personal information has become more accessible and available (Hiller & Russell, 2017; Solove, 2011). This sometimes obstructs society's adoption of smart cities (Pal et al., 2021). For that, personal information privacy risks that arise when sharing personal information in smart cities should be considered carefully to seize new threats and find

reasonable solutions. This section briefs privacy risks, regulations, and privacy-enhancing technologies.

Privacy Risks

Privacy risk is defined as the expected losses related to personal information disclosure (Xu et al., 2011). Pervasive literature attempts to identify the privacy risks of personal information. For example, Nissenbaum (2004) 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. Henriksen-Bulmer et al. (2019)proposed a taxonomy using the same theoretical lens, IC, to address privacy risks in open data publishing. The privacy taxonomy developed by Solove (2006) aimed to improve the understanding of information privacy in the legal system. This taxonomy classified privacy risk into four elements: collection, processing, dissemination, and invasion (Solove, 2006). Avancha et al. (2012) developed a privacy taxonomy that classified privacy threats into identity threats, access threats, and disclosure threats in the health system. The framework designed by Deng et al. (2011) provides a comprehensive analysis of privacy threats to help analysts cover key issues in designing software. In the smart airport, unauthorised access, information leakage, and second use were discussed as privacy threats that affect passenger information (Choudhury & Rabbani, 2019; Khi, 2020; Tedeschi & Sciancalepore, 2019; Zhang, 2019). The review conducted by Ismagilova et al. (2020) focused on security, privacy, and risk in smart cities and how they impact the operational process of smart cities. In addition, a systematic literature review is conducted to identify privacy risks and current solutions relevant to passengers' information (Alabsi & Gill, 2021). In this work, the privacy risks were classified based on the CFIP theory into four types: collection, error, unauthorised use, and improper access.

This review of the literature shows that despite attempts to analyse privacy risks, they only focused on addressing threats without considering vulnerabilities as an essential factor in privacy risk analysis. Furthermore, there is a lack of addressing privacy risks relevant to personal information in other smart city themes, such as smart airport.

Privacy Regulations

The General Data Protection Regulation (GDPR) is a significant regulation that regulates information privacy. The EU adopted the GDPR in 2018 and incorporated principles for personal information processing (Wolford, 2020). The GDPR explains principles that help in protecting individual privacy (EUGDPR, 2018). Consent, breach announcement, and privacy by design are examples of GDPR principles (EUGDPR, 2018).

In the USA, the Fair Information Practices (FIPs) regulation was developed in 1973 to discuss the importance of protecting individual privacy, and it was adopted by the U.S. Privacy Act (Gellman, 2017; Li & Palanisamy, 2018).

Following that time, different sectors in the USA, such as the health and business sectors, developed their privacy regulations called the Health Insurance Portability and Accountability Act (HIPAA) (Silva et al., 2021).

In Australia, the Privacy Act 1988 (Act) developed the Australian Privacy Principles (APPs) to protect and guide the use of personal information (Office of the Australian Information Commissioner n.d.). The APPs consist of principles governing the collection, handling, accessing of personal information, and ensuring the accuracy and integrity of personal information (Office of the Australian Information Commissioner n.d.).

Based on the above review, it is clear that countries share a common objective in protecting the privacy of personal information and governing how to use it despite their differing regulations.

Privacy-Enhancing Technologies

The interest in privacy protection has been increasing since the 1990s. Thus, there has been a continuous flux of efforts to develop and use Privacy-Enhancing Technologies (PETs) (Hiller & Blanke, 2016). PETs are well-designed (ICT) systems for securing and protecting the privacy of information through the reduction, deletion, or avoidance of improper and unnecessary processing of personal data without decreasing the value of the individual information (Chun, 2015). The goal of using PET in smart cities is to enable the personal and sensitive information embedded in the collected data to be hidden and not be discovered by any third party or service provider (Curzon et al., 2019). Recently, many PETs have been proposed to protect the privacy of information. For example, Van Blarkom et al. (2003) described PETs techniques such as encryption, anonymisation, pseud-identity, biometric, identification, authorisation, and authentication. Heurix et al. (2015) provided PETs taxonomy that covered privacy aspects such as user privacy and data privacy across domains not covered in security classifications. Curzon et al. (2019) provided a detailed review of privacy-enhancing technologies, commonly classified as anonymisation (such as masking and disruption of sensitive data) and security techniques (such as hashing and cryptographic techniques), as the broad types of techniques used mostly for personal information privacy protection. The PETs classification proposed by Kang et al. (2007) includes three types based on the privacy information life-cycle, including operation technology, common-based technology, and administrative technologies.

It is clear from previous and related research that the study of privacy-enhancing technology has been actively addressed, reflecting its importance in protecting the privacy of personal information.

In summary, protecting the privacy of personal information in smart cities is critical for its effective adoption by citizens or users. Studies have attempted to cover this topic by investigating many solutions and approaches. However, lack of systematic reviews effectively address and assess privacy risks, including threats, vulnerabilities, impacts, and exciting controls relevant to sharing personal information in

smart cities, considering who and what is involved and interacted during the sharing activity. This study aims to address this critical need by employing the well-known SLR approach detailed in the following section.

Research Method

This section presents the SLR method applied to conduct this systematic literature review (Kitchenham & Charters, 2007). This section includes the following SLR stages: (A) study inclusion and exclusion criteria, (B) data sources and search strategies, (C) study selection process, and (D) quality assessment.

Study Inclusion and Exclusion Criteria

In this study, a set of inclusion and exclusion criteria based on the research questions was used to select the relevant studies from well-known academic and industrial sources. It is important to note here that industry sources have been used to complement the academic sources. Academic studies must be peer-reviewed, including journal articles, conference papers, and book chapters. The studies must satisfy the following criteria: written in the English language, published between 2017 and 2021, include the specified search terms (see Table 1), and provide information to address the research questions listed in "Introduction" section. Studies that did not meet the inclusion criteria were excluded. This ensures that recent literature relevant to the scope of this study has been adequately covered.

Data Source and Search Strategy

The following well-known electronic databases were used to answer the identified research questions: IEEE Xplore (www.ieexplore.ieee.org/Xplore/), ScienceDirect (www.sciencedirect.com), ProQuest(www.proquest.com), Willy (onlinelibrary.wiley.com/), Gartner (www.gartner.com/).

The selected databases collectively cover a wide range of disciplines relevant to the topic at hand. Furthermore, this SLR includes academic and industrial studies, which distinguishes it from traditional SLR. However, the industrial sources were

Table 1 Search categories and keywords

Search categories	Search keywords
"Privacy-preserving"	Privacy threats, vulnerability, information privacy, personal privacy, privacy requirements, privacy goals, privacy properties, privacy controls, privacy Enhancing technology, non-technical control, privacy risk management, and privacy risk assessment
"Information sharing"	Information exchange, information transfer, information transmission, information flow
"Smart city"	Smart city, smart ecosystems, industry 4, digital cities, digital ecosystem

analysed separately to avoid mixing the non-peer-reviewed studies with academic sources. In the initial research stage, we used the selected search categories and terms presented in Table 1 to find the relevant studies that address the identified research questions. Each search term in the "privacy-preserving" category was combined with each term under the "information sharing" and "smart cities" categories with the operator "AND". Furthermore, the operator "OR" is used to combine similar terms in each category to ensure maximum coverage.

Study Selection Process

The study selection process assesses the inclusion and exclusion criteria through the following stages. In stage 1, all identified search terms and keywords (see Table 1) were searched in the selected databases (as explained earlier), and studies not relevant to inclusion and exclusion criteria were excluded. This stage resulted in 1089 industrial and academic studies. In stage 2, a set of 372 industrial and academic studies were selected after the titles and keywords assessment. In stage 3, further assessments were conducted for the abstract and conclusion, and 127 from both academic and industrial sources were included. A full-text assessment was applied in the final stage to obtain the final set of 83 studies. Further, the quality assessment has been performed on the final selected studies based on pre-identified assessment criteria (Table 3) (Kitchenham & Charters, 2007). The relevant studies from each stage were stored and managed using EndNote and then exported to Excel sheets to recode inclusion/exclusion decisions. A flowchart of the study selection process, including stages and the number of included studies in each stage, is shown in Fig. 1. Table 2 also presents the number of selected studies from each selected database in each stage.

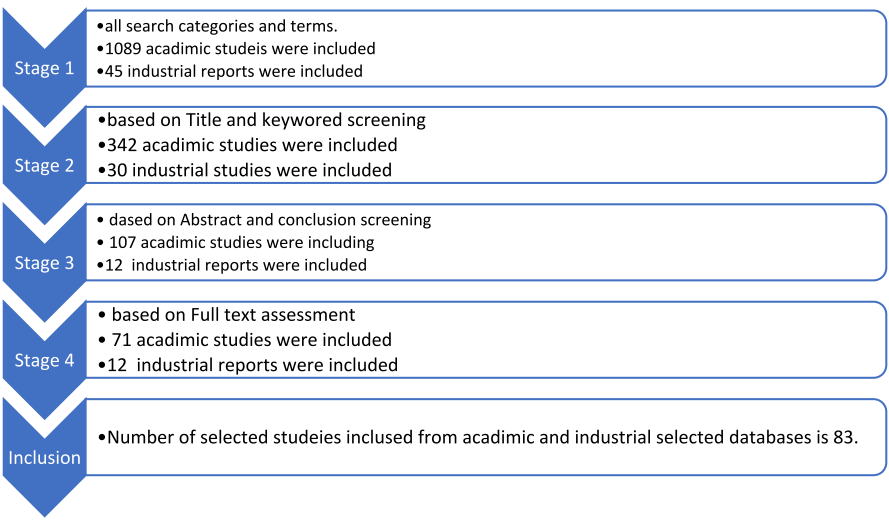

Fig. 1 Selection process stages and number of included studies

Table 2 Number of selected studies in each stage

Database	Stage 1	Stage 2	Stage 3	Stage 4
Willy	89	40	7	4
IEEE	93	39	20	23
ScienceDirect	415	114	50	31
ProQuest	456	194	30	13
Gartner	45	30	12	12
Total	1089	372	119	83

Table 3 Quality assessment criteria

Quality criteria
1. Does the study's context adequately address the related research?
2. Does the study clearly state its aim?
3. Is the study method appropriate for the study's aims?
4. Are the provided findings relevant to the study?
5. Does the study mention the future direction?

Quality Assessment

The quality assessment was performed based on the checklist made by Kitchenham and Charters (2007) to ensure the quality of this SLR. The quality assessment criteria items are presented in Table 3.

The questions of quality criteria were applied to identify the study's context, aim, and credibility. The selected studies were scored between 1 and 5 based on criteria items. The total score of the study reflects its quality. Each criterion got a score of "1" or "0". The selected studies from academic sources scored 1 in the research column. Four selected studies scored "0" in the aim column due to a lack of clarity about the study's aim, while a set of 3 selected studies scored "0" in the column of context because they did not include clear research context details. The majority of studies scored "1" in the finding column. A set of 12 selected studies scored "0" in the future column because of the lack of clarity about the future research directions. To sum up, as indicated in the last column of Table 4, the quality of selected studies is considered acceptable if the score is 3 or more out of 5 (60% or above).

Data Extraction and Synthesis

We systematically analysed and synthesised the selected studies using the Adaptive Enterprise Architecture (AEA) and Concerns for Information Privacy framework (CFIP) as a theoretical lens, besides the NIST 800–30 framework as a practical lens. We used the CFIP because it helps extract the privacy risk elements (threats and vulnerability) of sharing personal information, which was configured into a

Table 4 Selected studies based on quality assessment

Study	Research	Aim	Context	Finding	Future	Total
S1	1	1	1	1	1	5
S2	1	1	1	1	1	5
S3	1	1	1	0	0	3
S4	1	1	1	0	1	4
S5	1	1	1	1	1	5
S6	1	1	1	1	1	5
S6	1	1	1	1	1	5
S7	1	1	1	1	1	5
S8	1	1	1	0	0	3
S9	1	1	1	1	1	5
S10	1	1	1	1	1	5
S11	1	1	1	1	1	5
S12	1	1	1	1	1	5
S13	1	1	1	1	1	5
S14	1	1	1	1	1	5
S15	1	1	1	1	1	5
S16	1	1	1	1	1	5
S17	1	1	1	1	1	5
S18	1	1	1	1	1	5
S19	1	1	1	1	1	5
S20	1	1	1	1	1	5
S21	1	1	1	1	1	5
S22	1	1	1	1	1	5
S23	1	1	1	1	1	5
S24	1	1	1	1	1	5
S25	1	1	1	1	1	5
S26	1	1	1	1	1	5
S26	1	1	1	1	1	5
S27	1	0	1	0	1	4
S28	1	1	1	1	1	5
S29	1	1	1	0	0	3
S30	1	1	1	1	1	5
S31	1	1	1	1	1	5
S32	1	1	1	1	1	5
S33	1	1	1	0	0	3
S34	1	1	1	1	1	5
S35	1	1	1	1	1	5
S36	1	1	1	1	1	5
S37	1	1	1	1	1	5
S38	1	1	1	1	1	5
S39	1	1	1	1	1	5
S40	1	1	1	1	1	5
S41	1	0	1	0	1	3

Table 4 (continued)

Study	Research	Aim	Context	Finding	Future	Total
S42	1	1	1	1	1	5
S43	1	1	1	1	1	5
S44	1	1	1	1	1	5
S45	1	1	1	1	1	5
S46	1	1	1	1	1	5
S46	1	1	1	1	1	5
S47	1	1	1	1	1	5
S48	1	1	1	1	1	5
S49	1	1	1	1	1	5
S50	1	1	1	1	1	5
S51	1	0	1	1	1	4
S52	1	1	1	1	1	5
S53	1	1	1	1	1	5
S54	1	1	1	1	1	5
S55	1	1	1	1	1	5
S56	1	1	1	1	1	5
S56	1	1	1	1	1	5
S57	1	1	1	1	1	5
S58	1	1	1	1	1	5
S59	1	1	1	1	1	5
S60	1	1	1	1	1	5
S61	1	1	1	1	0	4
S62	1	1	1	1	1	5
S63	1	1	1	1	1	5
S64	1	1	1	1	1	5
S65	1	1	1	1	1	5
S66	1	1	1	1	1	5
S66	1	1	1	1	1	5
S67	1	1	1	1	1	5
S68	1	1	1	1	1	5
S69	1	1	1	1	1	5
S70	1	1	1	1	1	5
S71	1	0	1	1	1	4
N1	0	1	1	1	1	4
N2	0	1	1	1	1	4
N3	0	1	1	1	0	3
N4	0	1	0	1	0	3
N5	0	1	1	1	1	4
N6	0	1	1	1	0	3
N7	0	1	1	1	0	3
N8	0	1	1	1	1	4
N9	0	1	0	1	1	3
N10	0	1	1	1	0	3

Table 4 (continued)

Study	Research	Aim	Context	Finding	Future	Total
N11	0	1	1	1	0	3
N12	0	1	0	1	1	3

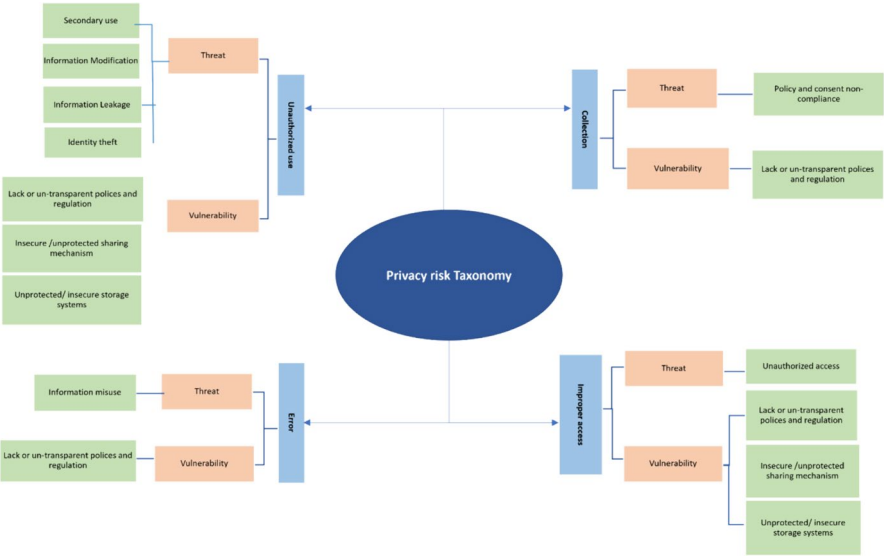

Fig. 2 Proposed privacy risk taxonomy based on CFIP framework

proposed privacy risk taxonomy (Fig. 2). Our proposed taxonomy consists of four categories based on CFIP: collection, error, unauthorised use, and improper access. CFIP seems to be an appropriate lens (Smith et al., 1996) to assess and analyse individual concerns regarding the privacy of organisational information practices. It is a multidimensional framework used as one of the most reliable tools for addressing individual information privacy concerns in many areas, such as e-commerce (Van Slyke et al., 2006). The extracted privacy risks under CFIP dimensions are mapped with the AEA framework's human, technology, facility, and environmental layers (Fig. 3). We also used Adaptive EA because it provides systematic layers to extract and map elements involved and interact while sharing personal information, besides relevant regulation as a governmental element that influences this activity. It is important to note here that sharing activity is considered the main element under the interaction layer. Adaptive EA (Gill, 2015) is a framework that guides the interaction in the digital ecosystems among five main layers: human, technology, facility, environment, and security. Further, we used NIST SP 800–30, the well-known standard, as a practical lens to identify and extract essential elements to assess privacy risks (Stoneburner et al. 2002). NIST was used to complement the theoretical lenses used in this study.

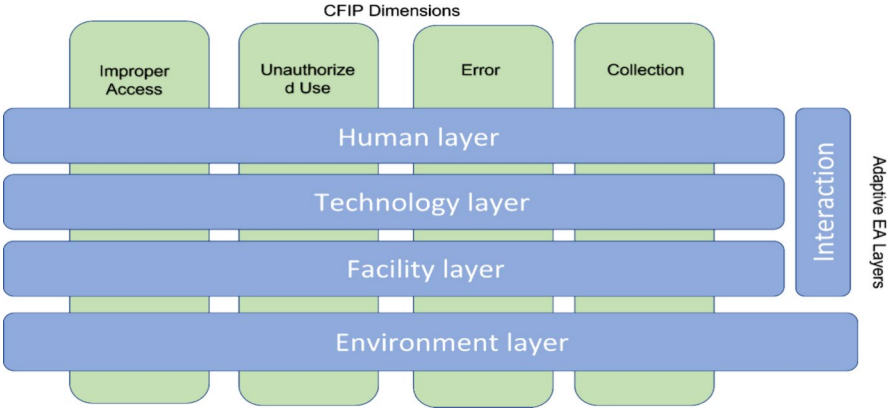

Fig. 3 Mapping CFIP with Adaptive EA

This was done to ensure that important points from practice were not overlooked. Thus, this study provides rich information incorporating both theoretical and practical perspectives. These elements include privacy threats, vulnerabilities, requirements, and privacy controls (see Fig. 4). The identified privacy controls include technical and non-technical controls (Fig. 4). The NIST 800–30 is used to carry out risk assessments according to the NIST guidelines (Peacock, 2021). The dimensions of CIFP cover different types of privacy risk components (threats and vulnerabilities) related to sharing personal information. Further, NIST 800–30 also

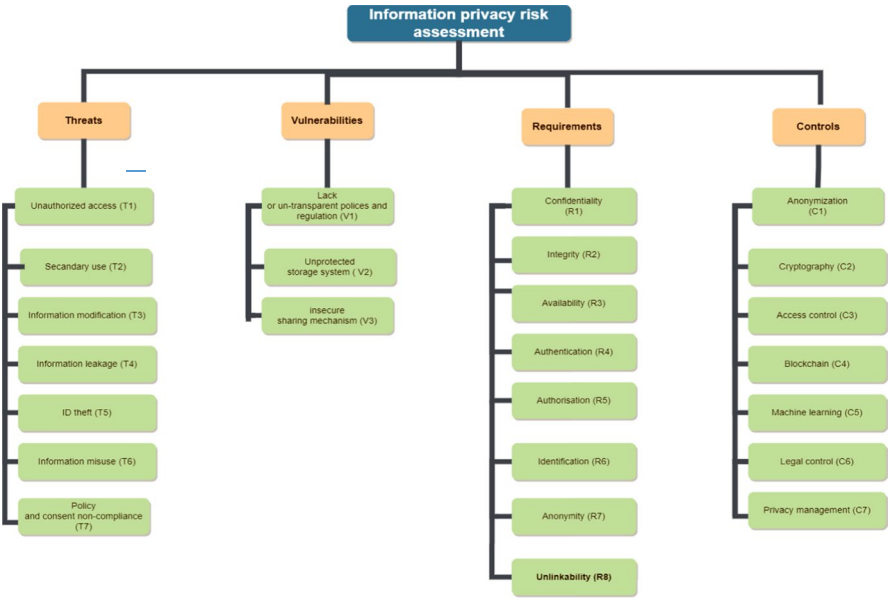

Fig. 4 Assessing information privacy risk based on NIST 800–30

offers a structured process that is used to assess privacy risks. Thus, we use CFIP and NIST 800–30 to report the results of this study, which are presented in the following section.

Results

To answer the indicated research questions, we analysed the final selected papers in Table 14 in the Appendix. We reviewed and analysed the selected studies using CFIP and NIST 800–30 frameworks to address the research questions to identify privacy risks (privacy threats, vulnerability), privacy risk impacts, and existing privacy controls. It is worth mentioning that the majority of the papers (86%) were taken from academic sources, whereas only 14% of selected studies were found relevant from the well-known industry Gartner data.

It is widely accepted that information risk is composed of threats and relevant vulnerabilities that may impact information assets (Norta et al., 2019). In this context, privacy controls are placed to mitigate the risk.

Privacy Risks

To answer RQ1, we use the CFIP and Adaptive EA as theoretical lenses. Firstly, we identify and categorise the privacy risk components, including privacy threats and vulnerabilities, related to the privacy risk of sharing personal information in smart cities by adopting the CFIP framework dimensions: collection, error, unauthorised use, and improper access (Smith et al., 1996). Then, we mapped the identified risks with the layers of Adaptive EA to present the elements involved and interacted in sharing personal information associated with the identified risks and relevant regulation as a governmental element that influences this sharing activity. Adaptive EA consists of the following layers: human, technology, facility, and environmental (Gill, 2015).

Privacy Threats

NIST defines threats as undesired and potential harm to the organisational assets such as information, operation and service, or individuals (National Institute of Standards and Technology 2013). We reviewed the selected studies to identify privacy threats that affect the sharing of personal information in smart cities in general and several smart city sectors such as smart healthcare, smart grid, smart governments, smart business/organisation, and smart transportation. Based on the CFIP framework, we identified seven types of privacy threats: collection, unauthorised use, improper access, and error from 41% of selected studies. Table 5 presents the identified threats, categories, and selected studies.

As shown in Table 5, the majority of selected studies (31%) discussed privacy threats under the unauthorised use category. This category includes the following threats: secondary use (T2), information modification (T3), information leakage

Table 5 Identified privacy threats from selected studies

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

(T4), and identity theft (T5). Seventeen percent of the reviewed studies highlighted unauthorised access (T1) as a privacy threat under the improper access category. The remaining studies discussed policy and regulation non-compliance privacy threat (T7) under the collection category (6%), with a few studies (2%) focused on information misuse (T6) privacy threats under the error category (3).

As shown in Table 5, the privacy threats related to patient information sharing in smart health have been widely discussed in the reviewed studies (N3, S4, S5, S6, S7, S8, S12, S17, S3, S27). For example, unauthorised access (T1), information misuse (T6), and modification (T3) threats have been identified as the most common threats that affect the privacy of patient information (Iwaya et al., 2019). Patient biometric data are collected and shared with many parties in the smart health sector, which leads to secondary use (T2) and ID theft (T5) threats (Romanou, 2018). Regulators and ethics committees are relevant to the health sector classified information leakage (T4) as a privacy threat that affects the collection, use, and sharing of personal information in smart health (Thapa & Camtepe, 2020).

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

As shown in Table 5, 6% of reviewed studies identified non-compliance with privacy policies and regulations (T7) as a privacy threat. Several countries and organisations have taken considerable steps toward data privacy policies and regulations in order to protect personal information. According to Wall et al. (2015), privacy compliance refers to an organisation's adherence to regulatory privacy requirements to protect personal information. Studies have discussed the increasing information privacy issues in organisations due to non-compliance with privacy policies

Table 6 Identified vulnerabilities

	Identified vulnerability	Study	Percentage
V1	Lack or un-transparent policies and regulation	S23, S24, S25, S30	5%
V2	Unprotected/ insecure storage systems	S12, S32	2%
V3	Insecure /unprotected sharing mechanism	S12, S32, S3	4%

and regulations in different sectors, including smart cities. For example, healthcare industries handle patients' information in the USA without explicit patient consent, which is at odds with granular consent under the Health Insurance Portability and Accountability Act (HIPAA) (Runyon, 2020).

Vulnerability

According to NIST (National Institute of Standards and Technology 2013), vulnerability is the weakness of an asset (e.g. information and system) plausibly exploited by threats. This section reviewed the selected studies based on this definition to extract the perceived vulnerabilities that identified threats might exploit.

As shown in Table 6, we identified three types of vulnerabilities relevant to the identified threats. Based on our review, 5% of selected studies mentioned that lack and un-transparent policies lead to several privacy threats (Chua et al., 2017; Hou et al., 2018; Taplin, 2021). Examples of these policies include consent, ethics, and privacy policies. Furthermore, the lack of privacy regulation related to handling and sharing personal information, including biometric data, could make this information vulnerable to several privacy threats (S30) (Khi, 2020). Insecure/unprotected storage systems and insecure/unprotected sharing mechanisms were identified as vulnerabilities in 3% of selected studies. Insecure storage refers to storing sensitive data without appropriately controlling access. Sharing information in unsecured or unprotected environments leads to privacy risks in smart cities (Agrawal et al., 2021; Romanou, 2018).

Mapping CFIP Dimensions with Adaptive EA Layers

Our review focused on the threats that affect personal information shared in smart cities in general and different smart city sectors such as smart health, smart grid, smart government, and smart business/organisation. Furthermore, we considered who and what are involved and interacted in the sharing activity, besides relevant regulation as a governmental element that influences this activity (based on Adaptive EA). Tables 7, 8, 9, 10, and 11 present the elements relevant to Adaptive EA layers: human, technology, facility, and environment, in smart cities. Figures 5, 6, 7, and 8 represent the map of CFIP dimensions with Adaptive EA layers.

As illustrated in Fig. 5, in the smart health context, elements under human layers are identified from 11% of selected studies that discussed the unauthorised use privacy risk associated with sharing patients' information in smart health. In contrast,

Table 7 Elements under AEA layers in smart health

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

Table 8 Elements under AEA layers in smart grid

Adaptive EA layers	Elements	Studies	Percentage
Human	Actors	S9, s16, s19	4%
Technology	Infrastructure, data storage, application	S9, s16, s18, s19, S23	6%
Facility	Building, utility	S9, s16, s18, s19, S23	6%

Table 9 Elements under AEA layers in smart city

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

Table 10 Elements under AEA layers in smart business/organisation

Adaptive EA layers	Elements	Studies	Percentage
Human	Actors	N11, N2, S22	4%
Technology	Infrastructure and data storage	N11, N2, S22, S26	5%
Facility	Building	N2, N5, S22, N11, S26, S25	7%
Governmental	Legal and policies	N4, N5, N11, S25	5%

Table 11 Elements under AEA layers in smart government and smart transportation

Context	AEA layers	Elements	Studies	Percentage
Smart government	Human	Actors	S10, S23	2%
	Technology	Application, data storage	S10, S23	
	Facility	Building	S10, S23	
Smart transportation	Human	Actors	S49	1%
	Technology	infrastructure	S49	
	Facility	Vehicle	S49	

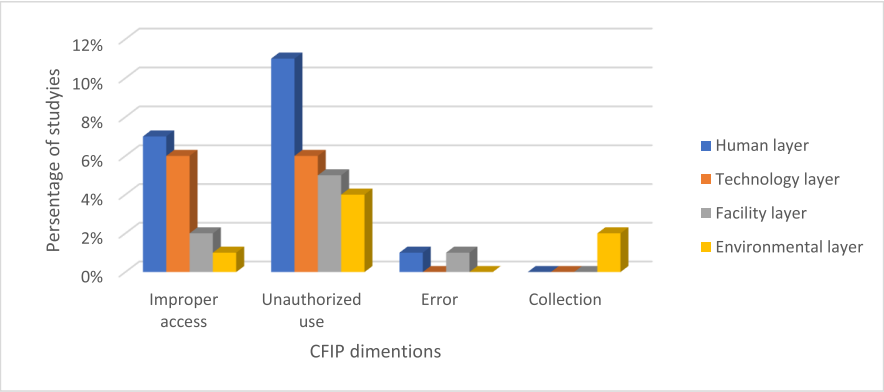

Fig. 5 Mapping CFIP dimensions with AEA layers in smart health

Fig. 6 Mapping CFIP dimensions with AEA layers in the smart grid

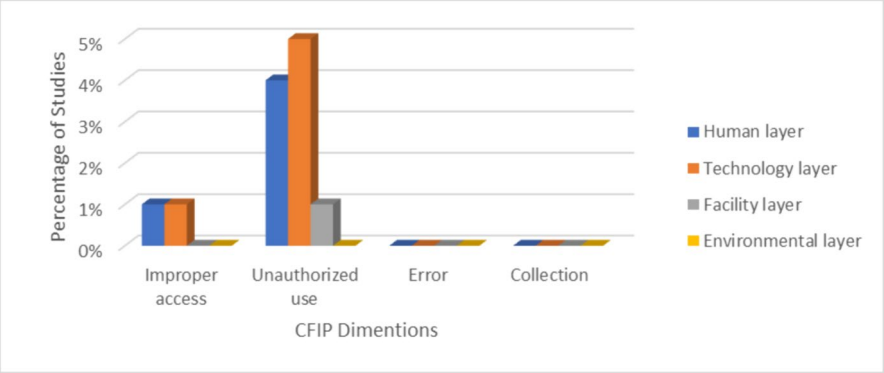

Fig. 7 Mapping CFIP dimensions with AEA layers in smart city

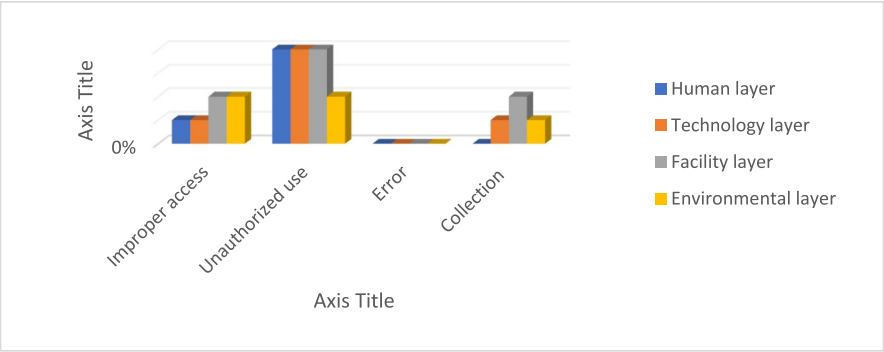

Fig. 8 Mapping CFIP dimensions with AEA layers in smart business/organisation

with improper access and error risks, the studies' percentages dropped to 7% and 1%. On the other hand, elements under technology layers are discussed in 6% of selected studies that investigated improper access and unauthorised use privacy risks, with 0% of studies in error and collection risks. However, the environmental layer is considered in selected studies (4%) when addressing privacy risks categorised under unauthorised use more than in improper access (1%) and collection dimensions (2%). We identified patients, service providers, and doctors as the main actors under human layers from 13% of selected studies. At the same time, infrastructure such as IoT and data storage, such as centralised databases, are identified under technology layers in 11% of selected studies. Facility layers are discussed in 6% of selected studies. The facility layer presents different smart health buildings, such as hospitals, medical centres, laboratories, and clinics. Privacy regulations are mainly discussed under the environmental layer in 6% of selected studies, which can be used to define or inform a separate layer of privacy. This seems to suggest the extension of the Adaptive EA framework through the introduction of the privacy layer. Table 7 presents elements under each layer of Adaptive AE in smart health context.

In the smart grid, Fig. 6 shows that more selected studies mentioned human, technology, and facility layers when addressing improper access and unauthorised use privacy risks associated with sharing users' information, while no studies discussed theses layers with error and collection privacy risks.

In Table 8, 4% of selected studies identified different actors under the human layer in the smart grid context, including users and customer service providers. Based on our review, 6% of selected studies discuss the usage of the cloud as the main data storage in the smart grid, while IoT applications and smart metres are the main infrastructures discussed in the smart grid system. Elements under facilities layers are found in 6% of selected studies that discuss privacy risks associated with sharing personal information in the smart grid. Examples of facility layer elements are control centres, power sources, and home gateways.

As presented in Fig. 7, almost a few percent of studies only mentioned human and technology layers with improper access risk compared with studies that addressed

unauthorised use privacy risks associated with sharing users' information in the smart city context.

Based on Table 9, from 5% of selected studies, we identified two main actors under human layers who are involved in sharing personal information in smart cities. The main actors include individuals, such as citizens and users, and organisations, including service providers and data holders. Moreover, IoT devices, Cloud systems, and smart city applications are identified in 6% of selected studies as elements under technology layers used in sharing personal information in smart cities.

As illustrated in Fig. 8, most selected studies in the smart business/organisation context explain elements in human, technology, and facilities layers when addressing unauthorised privacy risks associated with sharing personal information, whereas this percentage decreased with improper access privacy risk. On the other hand, the environmental layer is mentioned in 2% of studies that addressed privacy risks under improper access and unauthorised risks, with 1% with collection privacy risks.

Based on Table 10, we identified several actors, such as employees, customers, and experts, under the human layer from 4% of selected studies. The facility layer includes buildings, such as organisations, public workplaces, and industry, discussed in 7%. On the other hand, technical layer elements, such as infrastructure and data storage, and environmental elements, such as privacy regulation, are discussed in 5% of selected studies.

As shown in Table 11, human, technology, and facility layers have been mentioned in 2% of selected studies that discussed improper access and unauthorised use privacy risks in smart government, with 1% of studies addressing unauthorised use in the smart transportation context.

Privacy Risks Impacts

To answer RQ2, we reviewed the selected studies to identify and extract privacy requirements impacted by the identified privacy risks. The proper privacy requirements should be considered when personal information is shared in smart cities. Thus, we reviewed the selected studies to extract the privacy requirements that the identified threats might impact (Table 12 maps the requirements with relevant threats). As shown in Table 12, we identified eight classified requirements. The classifications include the CIA triad (confidentiality, integrity, availability) and IAAA (identification, authentication, authorization, accounting). In addition, we extracted the privacy requirements based on the classification proposed by Pfitzmann and Hansen (2010), which is very common in the privacy domain. The classification consists of anonymity and pseudonymity, unlinkability, undetectability, and unobservability. Table 12 includes a list of privacy requirements that need to be satisfied when sharing personal information in smart cities.

Concerning the CIA classification, 20% of selected studies discussed confidentiality and integrity as essential requirements to achieve privacy (Table 12). In contrast, availability is discussed in 10% of selected studies to achieve security besides privacy. In smart health, Health Information Exchange (HIE) has been adopted to enable the electronic sharing of patient information between several parties (Mutanu

Table 12 Identified privacy requirements

Associated threats	Affected requirements	Definition	Study	Percentage
T1, T3, T4, T6	Confidentiality (R1)	Restricting access to the information to authorised (National Institute of Standards and Technology, 2013)	S14, S4, S37, S39, S6, S40, S7, S41, S16, S9, S42, S21, S43, S45, S38, S46, S3	20%
T1, T3, T4, T6	Integrity (R2)	Preventing unauthorised change and ensuring the authenticity of information (National Institute of Standards and Technology, 2013)	S14, S4, S37, S39, S6, S40, S7, S41, S16, S9, S42, S21, S43, S45, S38, S46, S3, S71	20%
T1, T3, T4, T6	Availability (R3)	Providing timely and dependable access to and utilisation of information (National Institute of Standards and Technology, 2013)	S4, S14, S39, S16, S36, S42, S43, S48	10%
T1, T3, T4	Authentication (R4)	Verify the user's identification before accessing information system resources (National Institute of Standards and Technology, 2013)	S14, S6, S37, S7, S18, S36, S9, S21, S22, S45, S49	13%
T1, T3	Authorisation (R5)	Permitting access to a system resource, e.g. information (National Institute of Standards and Technology, 2013)	S14, S37, S8, S48	5%
T4	Identification (R6)	Only authorised people can access the stored information (Kalloniatis et al., 2008)	S18, S37	2%
T4, T1	Anonymity (R7)	Others do not identify The subject's identity (Pfitzmann & Hansen, 2010)	S37, S7, S36, S21, S43, S44, S38, S50, S49, S3	12%
T4	Unlinkability (R8)	It cannot determine whether the information set is related (Pfitzmann & Hansen, 2010)	S44	1%

et al., 2022). Thus, confidentiality, integrity, and availability are essential to preserve patient information privacy and security (Yi et al., 2013). In addition, the CIA triad should be satisfied with a smart grid and smart transportation to protect privacy as the information is shared between relevant parties to provide various services to the users (Yang et al. 2014).

As for the IAAA classification, 13% of selected studies discussed authentication as a requirement for privacy (Table 12). However, authorization was discussed in 5% of selected studies, whereas identification was discussed in 2% of selected studies. In the smart grid, identification and authentication requirements need to be satisfied to secure access to the information or system component (Ferrag et al., 2018; Sadhukhan et al., 2021). In smart health, authentication, authorization, and identification requirements should be satisfied when sharing patient information to ensure that privacy is not compromised (Shamshad et al., 2020; Wang et al., 2019).

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

Existing Privacy Control

To answer the RQ3, we reviewed the privacy-preserving schemes for sharing personal information in smart cities. We also extracted the existing privacy controls proposed to mitigate the identified risks from the selected studies (Table 13 maps the privacy controls with identified threats). Further, we classified the identified control under technical and non-technical, as shown in Table 13. Figure 9 represents the percentage of the identified privacy controls from the selected studies. Technical control methods include security-based solutions, such as encryption, access control, etc., whereas non-technical methods refer to policies, procedures and standards (National Institute of Standards and Technology, 2013).

Considering the technical solution, we identified ten technical controls categorised into four groups: anonymisation, cryptographic techniques, access control techniques, blockchain, and machine learning (Table 13). In this study, the classification of technical solutions is based on the classification of PETs proposed by Van Blarkom et al. (2003) and Curzon et al. (2019). In addition, we reviewed technical controls developed on blockchain and machine learning.

Data Anonymization

As sown in Table 13, 7% of reviewed studies discussed anonymization techniques as technical privacy controls. This includes K-anonymity, differential privacy, and pseudonym. Data anonymization is the method used to protect personal information by preventing linking their identities (Curzon et al., 2019; Iyengar, 2002; Silva

Table 13 Existing privacy controls

Associated threats	Privacy control classification	Type	Subtype	Study	Percentage
T2, T4, T5	Technical-based	Anonymization (C1)	k-anonymity	S54, S55, S56	7%
			Differential privacy	S12, S55	
			Pseudonym	S49	
T1, T2, T4, T5		Cryptographic techniques (C2)	Attribute-based encryption (ABE)	S7, S57	8%
			Identity-based encryption	S57	
			Biometric encryption	S12	
			Elliptic curve cryptography	S36,28	
			Homomorphic encryption	S58	
T1, T4,		Access control mechanism (C3)	Fine-grained access control	S7, S59, S60, S2	6%
			Multi-layer access control mechanism (MLAC)	S38	
T1, T2, T3, T4, T6		Blockchain (C4)		S9, S11, S10, S20, S41, S4, S6, S61, S47, S39, S37, S8, S14, S45, S21, S22, S62, S46, S48, S50, S63, S64, S58, S27, S29, S31, S33, S34, S35, S51, S52, S53, S69, S70, S71	42%
T5		Machine learning (C5)		S65, S58	2%
T1, T2, T3, T4, T5, T7	Non-technical solution	Policies and regulation (C6)		S12, S5, S66, S4, S6, S20, S41, S48, S50, S23, S24, 25, S61, N12, S1	18%
T1, T2, T5, T7		Privacy risk management (C7)		S67, S42, S68, S13, N1, N6, N7, N8, N9, N10, N11, N12, N4, S23	17%

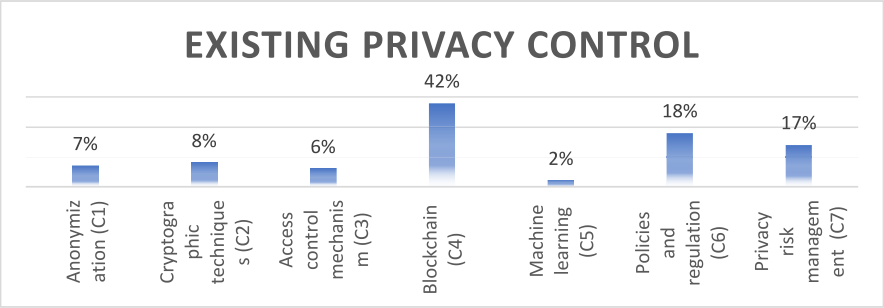

Fig. 9 Existing privacy control

et al., 2021). K-anonymity and differential privacy are the most common methods of anonymization technique (Iyengar, 2002). As for smart health, the reviewed study (S12) discussed the popularity of using anonymity to preserve the privacy of transmitted personal information between parties. On the other hand, the pseudonym is discussed in (S49) as an anonymous technique that is proposed to preserve the privacy of sharing information in smart transportation.

Cryptographic Technique

Table 13 includes cryptographic techniques used in privacy-preserving schemes for sharing personal information in smart cities. The techniques were extracted from 8% of selected studies. Cryptographic technology entails ways of totally hiding data equivalent to the intensity of the cryptographic key and algorithm employed. Encrypting transmitted or stored personal information in smart cities is a broadly used technology that protects from leakage and achieves privacy requirements (Curzon et al., 2019; Gaire et al., 2019). For example, attribute-based encryption (ABE) is proposed to preserve patient information sharing in smart health (S7, S57). Cryptographic technique for processing biometric data is presented in (S12); in this method, the digital key is securely linked by a biometric sample that is used to encrypt and decrypt the key. Elliptic curve cryptography to secure and authenticate the communication between the consumer and the service provider in the smart grid is discussed in (S36, S28).

Access Control Mechanism

Access control is defined as security methods to control the access and use of information by applying access policies (Sandhu & Samarati, 1994). In Table 13, 6% of reviewed studies discussed privacy-preserving schemes developed based on the access control mechanism. For example, schemes presented in selected studies proposed several access control mechanisms, such as fine-grained access control and multi-layer access control (MLAC), to preserve the privacy of patient information shared between different parties in a cloud-based environment.

Machine Learning

Table 13 shows that privacy-preserving schemes for sharing information in smart cities using machine learning techniques are discussed in 2% of selected studies. A self-organising map (SOM) is a machine learning technique used to share information about electricity usage between parties in the smart grid (S65). The machine learning technique, federated learning, is used to share and analyse medical cases in smart health without compromising patient privacy (S58).

Blockchain

As shown in Table 13, 42% of selected studies proposed privacy-preserving schemes for sharing information using Blockchain technology. Blockchain is a decentralized cryptographic scheme employed to privatise and safeguard transactions in the confines of a network (Curzon et al., 2019). It has been noticed that the privacy-preserving schemes in selected studies integrated blockchain with other PETs to share personal information without compromising their privacy. For example, access control mechanisms and blockchain are proposed in studies (S4, S6, S20, S41, S48, S50, S6, S8, S26, S27, S33, S34) mainly for two purposes. The first one is to allow individuals to monitor and regulate their information sharing between parties in smart cities. The second purpose is to authenticate the identity while sharing and accessing the information in smart cities. The selected studies (S9, S39, S14, S63, S21, S45, S31) proposed privacy-preserving schemes that use several cryptographic techniques, including signature, identity-based proxy, proxy re-encryption, zero-knowledge, and attribute-based encryption, with blockchain to protect the privacy of individual information in smart grid and smart health.

Non-technical Control

Among the selected studies, a total of 35% discussed non-technical privacy control to mitigate the identified threats (Table 13). For example, the importance of privacy by design (PbD) as a principle of GDPR is discussed in an attempt to protect the privacy of personal information in smart health and biometric applications (S12). Several policy-based schemes are discussed to capture the imposed requirements and restrictions that enhance the privacy of shared information in smart cities (S5, S66). On the other hand, privacy management is discussed in the selected studies as a type of non-technical privacy controls (S42, S13, S68, S67). As shown in Table 13, the non-technical privacy controls are discussed widely in the industrial reports (N1, N6, N7, N8, N9, N10, N11, N12, N4). Organisations need to reduce information disclosure as it leads to privacy and financial risks (Brian Lowans & Meunier, 2019). Effective privacy management programs should address privacy risk prevention and incorporate privacy-by-design principles into all business activities (Bart Willemsen, 2017). In this context, many risk management approaches, such as integrated risk management (IRM), data security governance (DSG) framework, privacy impact assessment(PIA), and continuous adaptive risk and trust assessment (CARTA), are discussed to help businesses dealing with risks and their

consequences and also to ensure the sustainability of the protection of any project (N6, N7, N1, N11). Furthermore, the importance of designing a privacy-aware risk programme to define and assess the risk of using blockchain technology for sharing personal information is discussed in industry publications (N8, N9).

Discussion

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

Implications

Privacy Risk

Many studies have proposed threat taxonomies that organise threats into different categories (Deng et al., 2011; Xiong & Lagerström, 2019). However, to the best of our knowledge, there is a lack of systematic and theoretical understanding, which is filled by this study using the CFIP as a theoretical lens. This study proposed a taxonomy of privacy risks of sharing personal information in smart cities, including threats and vulnerabilities, based on the CFIP theoretical lens. Based on Table 5, our findings show that the selected studies do not properly investigate policies and consent non-compliance, misuse, and ID theft as serious threats that widely affect the privacy of sharing personal information in smart cities. Furthermore, we found that selected studies did not clearly distinguish between threats' events and their sources, making it hard to identify the relevant privacy threats to the scope of this study. Thus, there is still a great deal of work to be done in this area in both academic and industrial research.

On the other hand, based on Table 5, we found that most selected studies discussed privacy threats associated with sharing personal information in smart cities in general and in the smart health system. In contrast, studies that discussed the same topic under the smart grid, smart government, smart business, and smart transportation systems were limited. One immediate impact of this finding on the digital economy is the reinforcement of the importance of investing in robust technological

solutions and infrastructures, as well as developing risk management frameworks to mitigate the privacy and security risks associated with personal information in smart cities (Ahmed, 2021, Jnr et al., 2023, Jin, 2024).

The digital economy is the deep integration of digital technology and production factors in smart cities to manage the transformation cost, improve cities' capabilities and implement innovative solutions (Sotirelis et al., 2022; Vinod Kumar & Dahiya, 2017; Wang et al., 2021; Zhiyong et al., 2024).

The emphasis on privacy risks of sharing personal information in smart cities highlights the need for innovative solutions that simultaneously advance their capabilities while rigorously safeguarding individual privacy. This could increase investment in implementing privacy controls to protect individual information handled within smart city sectors (Jin, 2024).

As smart city sectors heavily rely on sharing individual information by integrating smart technologies, there is a pressing need to address privacy risks associated with personnel. This could spur investment in privacy-enhancing technologies, regulatory frameworks, and public awareness campaigns tailored to these specific domains. This draws our attention to the need for more studies in order to cover this gap.

On the other hand, selected studies from industry sources discussed the identified privacy threats relevant to personal information without mentioning their relationship with smart cities or any other smart system.

On the other hand, it is well-accepted that any risk analysis should be done based on identified threats and relevant vulnerabilities (Stoneburner et al. 2002, Norta et al., 2019). The identification of vulnerabilities is an essential factor that plays a role in identifying privacy risks. Based on Table 6, we found that selected studies do not investigate vulnerabilities as a significant factor in addressing privacy risks relevant to sharing personal information in smart cities. As a result, the knowledge about the identified privacy risks was limited. Thus, there is a need to understand the threats and vulnerabilities to identify and mitigate privacy risks.

Based on our review, very limited studies currently explain who and what elements are involved when addressing privacy risks associated with sharing personal information in smart cities. Furthermore, to the best of our knowledge, no previous studies have demonstrated the interaction among the elements involved when addressing the topic mentioned above. To overcome the shortcomings of previous studies outlined above, we adopted Adaptive EA as a theoretical lens to map the identified privacy risks relevant to sharing personal information in smart cities, with elements involved and interacting in sharing activity. This study mapped the identified privacy risks based on CFIP dimensions, including improper access, unauthorised use, error, and collection, with Adaptive EA layers that include human, technology, facility, and environmental. Based on Figs. 5, 6, 7, and 8, we found that out of all the studies that addressed privacy risks associated with sharing personal information, most studies discussed human and technical layers, followed by the facility layer in all smart city sectors. However, few studies discussed the environmental layer, including privacy regulation and policies, only when addressing improper access and unauthorised use of privacy risks relevant to sharing personal information in smart health and smart business/organisation contexts.

Furthermore, according to Tables 7, 8, 9, 10, and 11, we found that most studies that defined elements under human and technology layers are relevant to smart health, with few studies in other smart city sectors. Additionally, although applying policies and regulations is vital to mitigate privacy risks associated with personal information in any smart city, we noticed that these elements, mainly categorised under the environmental layer, have not been investigated enough in the selected studies. Based on the above, there is a need to cover these gaps in future work.

Impacts

Undoubtedly, defining privacy requirements helps to study the consequences of privacy risks relevant to personal information. Moreover, it helps to choose the proper treatment for the identified risks. In this regard, we reviewed the selected studies to identify the privacy requirements based on well-known classifications such as CIA, IAAA, and the privacy requirement terminology (Pfitzmann & Hansen, 2010). Based on Table 12, our findings reveal that current studies investigate CIA triad and identification, authorization, authentication, and anonymity requirements for privacy risk in smart cities. However, addressing the impact of privacy risk on accounting, undetectability, unobservability, and pseudonymity is still largely unclear. This draws our attention to the need for more studies defining those requirements when discussing the privacy risks of sharing personal information in smart cities. Another finding shows that most selected studies link the requirements with the proposed technical controls. They test proposed solutions against those requirements to explain how they should satisfy them. However, there is a lack of studies that discuss the link between these requirements and privacy risks. For example, to the best of our knowledge, secondary use, ID theft, and policy and consent non-compliance threats are not linked with any one of the identified requirements; thus, more studies need to cover this gap to address the consequences and impacts of these risks.

Existing Control

We reviewed the selected studies to extract the existing privacy controls to preserve the privacy of sharing personal information in smart cities. We categorised privacy controls based on the well-known practical framework NIST 800–30 into technical and non-technical controls. Based on Table 13, our findings show that technical privacy controls, such as cryptography, anonymity, access control, blockchain, and machine learning, are frequently discussed in the selected studies. However, those controls are insufficient to preserve personal information privacy in smart cities because they are poorly developed due to technical and cost restrictions. Another finding shows that a set of 23 selected studies proposed technical solutions without implicitly explaining what kind of privacy threats could be mitigated by the proposed solution. This means they proposed the solution to preserve privacy issues in smart cities. Thus, linking the technical solution with specific privacy threats needs more investigation in the literature. Table 13 also finds that blockchain is widely used in privacy-preserving schemes proposed in academic literature. This indicates the importance and effectiveness of using it to share personal information in smart

cities without compromising privacy when integrating it with different PETs. On the other hand, our findings show that risk management has fewer research activities in academic fields; thus, this area requires further investigation.

Finally, the current research investigates risks, impact, and existing controls in different areas of focus (e.g. information security/privacy), and across various domains (e.g. smart health, smart grid, smart airport, and smart organisations). However, based on the analysis results, these studies seem to lack a systematic and common understanding of information privacy risks in smart cities. To address this challenge, there is a need to develop an ontology-based privacy risk assessment framework for a systematic and common understanding of privacy risks associated with sharing personal information in smart cities. Thus, this study is the first step to systematically synthesis and conceptualise the knowledge dispersed across different papers. It will provide a knowledge base and foundation for developing the personal information privacy risk ontology. The ontology will help enhance understanding the complex concepts and their relationships. Furthermore, it will help establish a common understanding for assessing and mitigating privacy risks in an informed manner. The development and evaluation of such ontology are beyond this paper's scope and subject to further research. However, this paper provided a strong foundation for this much-needed ontology work.

Validity and Limitations

This work has some limitations like any other SLR. Given this study's scope, we used well-known academic and industry databases to ensure sufficient coverage of the research topic. This provided a combination of academic and industrial studies explicitly emphasised in the analysis.

Given our emphasis on rigorously identifying and selecting relevant publications through systematic search strategies, the research methodology used in this study was suitable because it provided a multistage process. The process includes applying predefined inclusion and exclusion criteria and synthesising findings to derive meaningful insights to ensure that the process is unbiased.

One potential methodological limitation of the employed methodology in this study is the reliance on predefined databases, which may limit the comprehensiveness of the literature search. However, the identified databases encompass academic and industry sources, totalling six. This ensures that the selected databases cover a wide range of studies relevant to the topic at hand.

To ensure the validity and rigour of the adopted research methodology, we tested the search terms and keywords based on the identified research questions across the pre-selected databases. Furthermore, the process was reviewed to confirm the research's quality and coverage prior to the documentation stage. In addition, the quality assessment criteria were used to avoid researcher bias and ensure the selected studies' relevance and quality. Human error might lead to inconsistencies when conducting such research. Thus, regular meetings between the senior researcher and this study's author were held to minimise the possibility of human error and ensure the quality of the research process and results. This also includes reviewing and learning

from the SLRs published in different domains in quality academic outlets. Integrating the employed approach with an additional one to enhance the rigour and comprehensiveness of reviews is suggested as a future research direction.

Conclusion

The term "smart city" has become the focus of several countries striving to improve their population quality, enhance their economies, and ensure sustainability. To achieve their objectives, cities have adopted innovative technologies and applications and developed their ICT infrastructure to support smart city initiatives in many sectors. These sectors include health, government, transportation, business, and organisation. However, due to the strong relationship between ICT and smart cities, personal information is easily shared among relevant parties, leading to serious privacy risks that may affect individuals and organisations. These risks need to be addressed, as highlighted in this SLR. This study analysed and synthesised published research to identify and extract privacy risks, impacts, and existing controls related to sharing personal information in different sectors in smart cities. It also considers elements involved and interacting in the sharing activity based on the well-known CFIP framework and Adaptive EA as theoretical lenses and NIST 800–30 as a practical lens. Based on NIST 800–30, we identified seven privacy threats, three vulnerabilities, and eight requirements that might be impacted by the identified threats, along with seven privacy controls classified into technical and non-technical types. Furthermore, we used CFIP as a theoretical lens to identify and categorise privacy threats and vulnerabilities relevant to the scope of this study. Based on CFIP, we categorised the identified privacy risks (threats and vulnerabilities) into four main groups: collection, unauthorised access, improper use, and errors.

Furthermore, we mapped the identified risks to identified requirements and current controls. The Adaptive EA is used to map the identified risks under CFIP dimensions with layers that interact while sharing personal information in smart cities. Our findings show the need for contemporary solutions to improve the privacy level of sharing personal information in smart cities. Furthermore, there is a need to represent privacy risk assessment components and their relationship and the relation among elements involved in sharing personal information using ontology to facilitate common understanding and sharing of the relevant concepts between different parties involved in connected smart cities. This SLR can benefit both academia and industry by helping them better understand the privacy of sharing personal information in smart cities and providing a synthesised foundation for further work in this important area of research.

Appendix

Table 14

Table 14 Final selected studies

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

Table 14 (continued)

Study number	Study title
S16	A. Agarkar and H. Agrawal, "A review and vision on authentication and privacy preservation schemes in smart grid network," Security and Privacy, vol. 2, no. 2, p. e62, 2019
S17	T. Kanwal, A. Anjum, A. Khan, A. Asheralieva, and G. Jeon, "A formal adversarial perspective: Secure and efficient electronic health records collection scheme for multi-records datasets," Transactions on Emerging Telecommunications Technologies, p. e4180, 2020
S18	M. A. Ferrag, L. A. Maglaras, H. Janicke, J. Jiang, and L. Shu, "A systematic review of data protection and privacy preservation schemes for smart grid communications," Sustainable cities and society, vol. 38, pp. 806–835, 2018
S19	J. Liu, J. Hou, X. Huang, Y. Xiang, and T. Zhu, "Secure and efficient sharing of authenticated energy usage data with privacy preservation," Computers & Security, vol. 92, p. 101756, 2020
S20	I. Makhdoom, I. Zhou, M. Abolhasan, J. Lipman, and W. Ni, "PrivySharing: A blockchain-based framework for privacy-preserving and secure data sharing in smart cities," Computers & Security, vol. 88, p. 101653, 2020
S21	Y. Zhang, D. He, and K.-K. R. Choo, "BaDS: Blockchain-based architecture for data sharing with ABS and CP-ABE in IoT," Wireless Communications and Mobile Computing, vol. 2018, 2018
S22	Q. Zhang, Y. Li, R. Wang, L. Liu, Y. a. Tan, and J. Hu, "Data security sharing model based on privacy protection for blockchain-enabled industrial Internet of Things," International Journal of Intelligent Systems, vol. 36, no. 1, pp. 94–111, 2021
S23	R. Khatoun and S. Zeadally, "Cybersecurity and Privacy Solutions in Smart Cities," IEEE Communications Magazine, vol. 55, no. 3, pp. 51–59, 2017
S24	Y. Hou, P. Gao, and B. Nicholson, "Understanding organisational responses to regulative pressures in information security management: The case of a Chinese hospital," Technological Forecasting and Social Change, vol. 126, pp. 64–75, 2018
S25	H. N. Chua, A. Herbland, S. F. Wong, and Y. Chang, "Compliance to personal data protection principles: A study of how organisations frame privacy policy notices," Telematics and Informatics, vol. 34, no. 4, pp. 157–170, 2017
S26	P. Brous, M. Janssen, and P. Herder, "The dual effects of the Internet of Things (IoT): A systematic review of the benefits and risks of IoT adoption by organisations," International Journal of Information Management, vol. 51, p. 101952, 2020
S27	S. Cao, J. Wang, X. Du, X. Zhang, and X. Qin, "CEPS: A Cross-Blockchain based Electronic Health Records Privacy-Preserving Scheme," in *ICC 2020—2020 IEEE International Conference on Communications (ICC)*, 7–11 June 2020 2020, pp. 1–6
S28	H. Djigal, F. Jun, and J. Lu, "Secure Framework for Future Smart City," in *2017 IEEE 4th International Conference on Cyber Security and Cloud Computing (CSCloud)*, 26–28 June 2017 2017, pp. 76–83
S29	N. Andola, Raghav, S. Prakash, S. Venkatesan, and S. Verma, "SHEMB:A secure approach for healthcare management system using blockchain," in *2019 IEEE Conference on Information and Communication Technology*, 6–8 Dec. 2019 2019, pp. 1–6
S30	I. A. Khi, "Ready for take-off: how biometrics and blockchain can beat aviation's quality issues," *Biometric Technology Today,* vol. 2020, no. 1, pp. 8–10, 2020
S31	D. Han, J. Chen, L. Zhang, Y. Shen, X. Wang, and Y. Gao, "Access control of blockchain based on dual-policy attribute-based encryption," in *2020 IEEE 22nd International Conference on High Performance Computing and Communications; IEEE 18th International Conference on Smart City; IEEE 6th International Conference on Data Science and Systems*. 2020

Table 14 (continued)

Study number	Study title
S32	T. K. Agrawal, V. Kumar, R. Pal, L. Wang, and Y. Chen, "Blockchain-based framework for supply chain traceability: A case example of textile and clothing industry," *Computers & industrial engineering,* vol. 154, p. 107130, 2021
S33	G. Magyar, "Blockchain: Solving the privacy and research availability tradeoff for EHR data: A new disruptive technology in health data management," in *2017 IEEE 30th Neumann Colloquium (NC)*, 24–25 Nov. 2017 2017, pp. 000135–000140
S34	M. M. Mahdy, "Semi-Centralized Blockchain Based Distributed System for Secure and Private Sharing of Electronic Health Records," in *2020 International Conference on Computer, Control, Electrical, and Electronics Engineering (ICCCEEE)*, 26 Feb.–1 March 2021 2021, pp. 1–4
S35	M. T. Quasim, A. A. E. Radwan, G. M. M. Alshmrani, and M. Meraj, "A Blockchain Framework for Secure Electronic Health Records in Healthcare Industry," in *2020 International Conference on Smart Technologies in Computing, Electrical and Electronics (ICSTCEE)*, 9–10 Oct. 2020 2020, pp. 605–609
S36	D. Sadhukhan, S. Ray, M. S. Obaidat, and M. Dasgupta, "A secure and privacy preserving lightweight authentication scheme for smart-grid communication using elliptic curve cryptography," *Journal of Systems Architecture,* vol. 114, p. 101938, 2021
S37	S. Shamshad, K. Mahmood, S. Kumari, and C.-M. Chen, "A secure blockchain-based e-health records storage and sharing scheme," *Journal of Information Security and Applications,* vol. 55, p. 102590, 2020
S38	S. Chenthara, A. Khandakar, and F. Whittaker, "Privacy-Preserving Data Sharing using Multi-layer Access Control Model in Electronic Health Environment," (in English), EAI Endorsed Transactions on Scalable Information Systems, vol. 6, no. 22, 2019
S39	H. Huang, P. Zhu, F. Xiao, X. Sun, and Q. Huang, "A blockchain-based scheme for privacy-preserving and secure sharing of medical data," Computers & Security, vol. 99, p. 102010, 2020
S40	B. Shen, J. Guo, and Y. Yang, "MedChain: Efficient Healthcare Data Sharing via Blockchain," (in English), Applied Sciences, vol. 9, no. 6, 2019
S41	E. Zaghloul, T. Li, and J. Ren, "Security and privacy of electronic health records: decentralized and hierarchical data sharing using smart contracts," in 2019 International Conference on Computing, Networking and Communications (ICNC), 2019: IEEE, pp. 375–379
S42	J. den Hartog and N. Zannone, "Security and privacy for innovative automotive applications: A survey," *Computer Communications,* vol. 132, pp. 17–41, 2018
S43	Z. Xiao, X. Fu, and R. S. M. Goh, "Data Privacy-Preserving Automation Architecture for Industrial Data Exchange in Smart Cities," *IEEE Transactions on Industrial Informatics,* vol. 14, no. 6, pp. 2780–2791, 2018
S44	Z. Li, M. Alazab, S. Garg, and M. S. Hossain, "PriParkRec: Privacy-Preserving Decentralized Parking Recommendation Service," *IEEE Transactions on Vehicular Technology,* pp. 1–1, 2021
S45	X. Yang, T. Li, W. Xi, A. Chen, and C. Wang, "A Blockchain-Assisted Verifiable Outsourced Attribute-Based Signcryption Scheme for EHRs Sharing in the Cloud," *IEEE Access,* vol. 8, pp. 170713–170731, 2020
S46	S. Zhang, J. Rong, and B. Wang, "A privacy protection scheme of smart meter for decentralized smart home environment based on consortium blockchain," *International Journal of Electrical Power & Energy Systems,* vol. 121, p. 106140, 2020

Table 14 (continued)

Study number	Study title
S47	J. Cha, S. K. Singh, T. W. Kim, and J. H. Park, "Blockchain-empowered cloud architecture based on secret sharing for smart city," *Journal of Information Security and Applications,* vol. 57, p. 102686, 2021
S48	D. C. Nguyen, P. N. Pathirana, M. Ding, and A. Seneviratne, "Blockchain for Secure EHRs Sharing of Mobile Cloud Based E-Health Systems," *IEEE Access,* vol. 7, pp. 66792–66806, 2019
S49	M. Han, S. Liu, S. Ma, and A. Wan, "Anonymous-authentication scheme based on fog computing for VANET," *PLoS one,* vol. 15, no. 2, p. e0228319, 2020
S50	J. Sun, L. Ren, S. Wang, and X. Yao, "A blockchain-based framework for electronic medical records sharing with fine-grained access control," (in English), *PLoS One,* vol. 15, no. 10, Oct 2020
S51	G. S. Reen, M. Mohandas, and S. Venkatesan, "Decentralized Patient Centric e- Health Record Management System using Blockchain and IPFS," in *2019 IEEE Conference on Information and Communication Technology*, 2019, pp. 1–7
S52	M. S. Swetha, S. K. Pushpa, M. S. Muneshwara, and T. N. Manjunath, "Blockchain enabled secure healthcare Systems," in *2020 IEEE International Conference on Machine Learning and Applied Network Technologies (ICMLANT)*,2020, pp. 1–6
S53	M. T. Quasim, F. Algarni, A. A. E. Radwan, and G. M. M. Alshmrani, "A Blockchain based Secured Healthcare Framework," in *2020 International Conference on Computational Performance Evaluation (ComPE)*,2020, pp. 386–391
S54	B. Y. He and J. Y. J. Chow, "Optimal privacy control for transport network data sharing," presented at the Transportation Research Procedia, 2019/01/01/, 2019. [Online]
S55	Y. Li, D. Yang, and X. Hu, "A differential privacy-based privacy-preserving data publishing algorithm for transit smart card data," *Transportation Research Part C: Emerging Technologies,* vol. 115, p. 102634, 2020
S56	F. Liu and T. Li, "A clustering-anonymity privacy-preserving method for wearable iot devices," *Security and Communication Networks,* vol. 2018, 2018
S57	Q. Huang, L. Wang, and Y. Yang, "Secure and Privacy-Preserving Data Sharing and Collaboration in Mobile Healthcare Social Networks of Smart Cities," (in English), *Security and Communication Networks,* vol. 2017, p. 12, 2017
S58	W. Cheng, W. Ou, X. Yin, W. Yan, D. Liu, and C. Liu, "A privacy-protection model for patients," *Security and Communication Networks,* vol. 2020, 2020
S59	P. S. W. Shieng, J. Jansen, and S. Pemberton, "Fine-grained access control framework for igor, a unified access solution to the internet of things," presented at the Procedia Computer Science, 2018
S60	O. Olakanmi and K. Odeyemi, "FEACS: A fog enhanced expressible access control scheme with secure services delegation among carers in E-health systems," *Internet of Things,* vol. 12, p. 100278, 2020
S61	S. Amofa et al., "A Blockchain-based Architecture Framework for Secure Sharing of Personal Health Data," in *2018 IEEE 20th International Conference on e-Health Networking, Applications and Services (Healthcom)*, 17–20 Sept. 2018
S62	Q. Xia, S. Emmanuel Boateng, A. Smahi, S. Amofa, and X. Zhang, "BBDS: Blockchain-Based Data Sharing for Electronic Medical Records in Cloud Environments," (in English), *information,* vol. 8, no. 2, p. 44, 2017
S63	T. T. Thwin and S. Vasupongayya, "Blockchain-Based Access Control Model to Preserve Privacy for Personal Health Record Systems," (in English), *Security and Communication Networks,* vol. 2019, p. 15, 2019

Table 14 (continued)

Study number	Study title
S64	X. Liang, S. Shetty, D. Tosh, D. Bowden, L. Njilla, and C. Kamhoua, "Towards blockchain empowered trusted and accountable data sharing and collaboration in mobile healthcare applications," *EAI Endorsed Transactions on Pervasive Health and Technology,* Article 2018
S65	Y. Nakamura, K. Harada, and H. Nishi, "A privacy-preserving sharing method of electricity usage using self-organising map," ICT Express, vol. 4, no. 1, pp. 24–29, 2018/03/01/ 2018
S66	Q. H. Cao, M. Giyyarpuram, R. Farahbakhsh, and N. Crespi, "Policy-based usage control for a trustworthy data sharing platform in smart cities," *Future Generation Computer Systems,* vol. 107, pp. 998–1010, 2020/06/01/ 2020
S67	T. A. Butt, R. Iqbal, K. Salah, M. Aloqaily, and Y. Jararweh, "Privacy management in social internet of vehicles: review, challenges and blockchain based solutions," *IEEE Access,* vol. 7, pp. 79694–79713, 2019
S68	D. Eckhoff and I. Wagner, "Privacy in the Smart City—Applications, Technologies, Challenges, and Solutions," *IEEE Communications Surveys & Tutorials,* vol. 20, no. 1, pp. 489–516, 2018, https://doi.org/10.1109/COMST.2017.2748998
S69	M. Du, Q. Chen, J. Chen, and X. Ma, "An Optimized Consortium Blockchain for Medical Information Sharing," IEEE transactions on engineering management, vol. 68, no. 6, pp. 1677–1689, 2021
S70	L.-Y. Yeh, P. J. Lu, S.-H. Huang, and J.-L. Huang, "SOChain: A Privacy-Preserving DDoS Data Exchange Service Over SOC Consortium Blockchain," IEEE transactions on engineering management, vol. 67, no. 4, pp. 1487–1500, 2020
S71	O. Ajayi, M. Abouali, and T. Saadawi, "Secure Architecture for Inter-Healthcare Electronic Health Records Exchange," in 2020 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS), 9–12 Sept. 2020 2020, pp. 1–6
N1	B. Willemsen, "Use a Privacy Impact Assessment to Ensure Baseline Privacy Criteria", Gartner, 20
N2	R. C. Patrick Long, "5 Tips to Protect Data for Midsize Enterprise Remote Workers," Gartner, 2020
N3	B. Runyon, "Healthcare CIOs: Prepare for Granular Patient Consent," Gartner, 2020
N4	S. J. Guido De Simoni, "Implement Your Data and Analytics Governance Through 5 Pragmatic Steps," Gartner, 2020
N5	R. G. Richard Hunter, Neil MacDonald, Bart Willemsen, Jay Heiser, "Address Digital Business Risk by Using Adaptive Governance," Gartner, 2020
N6	J. A. Wheeler, "Hype Cycle for Risk Management, 2018," Gartner, 2018
N7	B. W. Nader Henein, "The State of Privacy and Personal Data Protection, 2019–2020," Gartner, 2019
N8	M. H. Nader Henein, "5 Steps to Managing Privacy in the Blockchain," Gartner, 2018
N9	M. R. Avivah Litan, "Managing the Risks of Enterprise Blockchain Smart Contracts," Gartner, 2020
N10	B. W. Brian Lowans, Marc-Antoine Meunier, "Use the Data Security Governance Framework to Balance Business Needs and Risks," Gartner, 2019
N11	A. M. Samantha Searle, "How to Develop the Right Technical and Human Architectures for Digital Business," Gartner, 2019
N12	P. B. Bart Willemsen, "The Four Do's and Don'ts of Implementing Your Privacy Program," Gartner, 2017

Author Contribution All authors have contributed to this manuscript and approved the published version. The first author participated in all the work, including drafting, reviewing, and updating the article. The second author contributed to the research approach, review, and revisions of the article.

Funding Open Access funding enabled and organized by CAUL and its Member Institutions. This work was supported by Taibah University, Saudi Arabia, which provided a Ph.D. scholarship that covered funding for this work. This work was done at the University of Technology Sydney, Australia.

Data Availability Not applicable.

Declarations

Competing Interests The authors declare no competing interests.

Open Access This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit http://creativecommons.org/licenses/by/4.0/.

References

Agrawal, T. K., Kumar, V., Pal, R., Wang, L., & Chen, Y. (2021). Blockchain-based framework for supply chain traceability: A case example of textile and clothing industry. *Computers & Industrial Engineering, 154*, 107130.

Ahmad Mohamad, A.-S., Alsmadi, M. K., Abdel Karim, B., Ibrahim, A., Abouelmagd, H., & Osman SaadShidwan, A. (2019). Emergent situations for smart cities: A survey. *International Journal of Electrical and Computer Engineering, 9*(6), 4777–4787.

Ahmed, E. M. (2021). Modelling Information and communications technology cyber security externalities spillover effects on sustainable economic growth. *Journal of the Knowledge Economy, 12*(1), 412–430.

Alabsi, M. I., & Gill, A. Q. (2021). A review of passenger digital information privacy concerns in smart airports. *IEEE Access, 9*, 33769-33781.

Albino, V., Berardi, U., & Dangelico, R. M. (2015). Smart cities: Definitions, dimensions, performance, and initiatives. *Journal of Urban Technology, 22*(1), 3–21.

Avancha, S., Baxi, A., & Kotz, D. (2012). Privacy in mobile technology for personal healthcare. *ACM Computing Surveys (CSUR), 45*(1), 1–54.

Bart Willemsen, P. B. (2017). *The four do's and don'ts of implementing your privacy program*. Gartner.

Bogoda, L., Mo, J., Bil, C., & Ieee, (2019). A systems engineering approach to appraise cybersecurity risks of cns/atm and avionics systems. In *2019 Integrated Communications, Navigation and Surveillance Conference*.

BrianLowans, B. W., & Meunier, M.-A. (2019). *Use the data security governance framework to balance business needs and risks*. Gartner.

Caragliu, A., Del Bo, C., & Nijkamp, P. (2009). Smart cities in Europe. *Journal of Urban Technology, 18*, 65–82.

Chenthara, S., Khandakar, A., & Whittaker, F. (2019). Privacy-preserving data sharing using multi-layer access control model in electronic health environment. *EAI Endorsed Transactions on Scalable Information Systems*, *6,* 22. https://doi.org/10.4108/eai.13-7-2018.159356

Choudhury, Z. H., & Rabbani, M. M. A. (2019). Biometric passport for national security using multi-biometrics and encrypted biometric data encoded in the QR code. *Journal of Applied Security Research, 15*, 1–31.

Chua, H. N., Herbland, A., Wong, S. F., & Chang, Y. (2017). Compliance to personal data protection principles: A study of how organisations frame privacy policy notices. *Telematics and Informatics, 34*(4), 157–170.

Chun, S.-H. (2015). Privacy enhancing technologies (PETs) and investment strategies for a data market. *Procedia-Social and Behavioral Sciences, 185*, 271–275.

Cranor, L. F. (2012). Necessary but not sufficient: Standardized mechanisms for privacy notice and choice. *J on Telecomm & High Tech L, 10*, 273.

Curzon, J., Almehmadi, A., & El-Khatib, K. (2019). A survey of privacy enhancing technologies for smart cities. *Pervasive and Mobile Computing, 55*, 76–95.

Deng, M., Wuyts, K., Scandariato, R., Preneel, B., & Joosen, W. (2011). A privacy threat analysis framework: Supporting the elicitation and fulfillment of privacy requirements. *Requirements Engineering, 16*(1), 3–32.

EUGDPR. (2018). "GDPR key changes." Retrieved 20 Sep, 2019, from http://www.eugdpr.org/key-changes.html.

Ferrag, M. A., Maglaras, L. A., Janicke, H., Jiang, J., & Shu, L. (2018). A systematic review of data protection and privacy preservation schemes for smart grid communications. *Sustainable Cities and Society, 38*, 806–835.

Gaire, R., Ghosh, R. K., Kim, J., Krumpholz, A., Ranjan, R., Shyamasundar, R., & Nepal, S. (2019). *Crowdsensing and privacy in smart city applications* (pp. 57–73). Elsevier.

Gellman, R. (2017). Fair information practices: A basic history. Available at SSRN 2415020.

Giffinger, R., Fertner, C., Kramar, H., Kalasek, R., Milanović, N., & Meijers, E. (2007). *Smart cities - Ranking of European medium-sized cities*. Centre of Regional Science, Vienna University of Technology.

Gill, A. Q. (2015). *Adaptive cloud enterprise architecture*. World Scientific.

Gill, A. Q. (2021). A theory of information trilogy: Digital ecosystem information exchange architecture. *Information, 12*(7), 283.

Henriksen-Bulmer, J., Faily, S., & Jeary, S. (2019). Privacy risk assessment in context: A meta-model based on contextual integrity. *Computers & Security, 82*, 270–283.

Heurix, J., Zimmermann, P., Neubauer, T., & Fenz, S. (2015). A taxonomy for privacy enhancing technologies. *Computers & Security, 53*, 1–17.

Hiller, J. S., & Blanke, J. M. (2016). Smart cities, big data, and the resilience of privacy. *Hastings LJ, 68*, 309.

Hiller, J. S., & Russell, R. S. (2017). Privacy in crises: The NIST privacy framework. *Journal of Contingencies and Crisis Management, 25*(1), 31–38.

Hoffman, L. (1977). *Modern methods for computer security and privacy*. Englewood Cliffs: Prentice-Hall.

Hong, J. I., Ng, J. D., Lederer, S., & Landay, J. A. (2004). Privacy risk models for designing privacy-sensitive ubiquitous computing systems. In *Proceedings of the 5th conference on Designing interactive systems: processes, practices, methods, and techniques*.

Hou, Y., Gao, P., & Nicholson, B. (2018). Understanding organisational responses to regulative pressures in information security management: The case of a Chinese hospital. *Technological Forecasting and Social Change, 126*, 64–75.

Hough, M. G. (2009). Keeping it to ourselves: Technology, privacy, and the loss of reserve. *Technology in Society, 31*(4), 406–413.

Hsiao, Y.-C., Wu, M.-H., & Li, S. C. (2021). Elevated performance of the smart city-A case study of the IoT by innovation mode. *IEEE Transactions on Engineering Management, 68*(5), 1461–1475.

Imine, Y., Lounis, A., & Bouabdallah, A. (2020). An accountable privacy-preserving scheme for public information sharing systems. *Computers & Security, 93*, 101786.

Ismagilova, E., Hughes, L., Rana, N. P., & Dwivedi, Y. K. (2020). Security, privacy and risks within smart cities: Literature review and development of a smart city interaction framework. Information Systems Frontiers.

Iwaya, L. H., Fischer-Hübner, S., Åhlfeldt, R.-M., & Martucci, L. A. (2019). Mobile health systems for community-based primary care: Identifying controls and mitigating privacy threats. *JMIR mHealth and uHealth, 7*(3), e11642.

Iyengar, V. S. (2002). Transforming data to satisfy privacy constraints. In *Proceedings of the eighth ACM SIGKDD international conference on Knowledge discovery and data mining*.

Jin, W. (2024). Security and privacy of digital economic risk assessment system based on cloud computing and blockchain. *Soft Computing, 28*(3), 2753–2768.

Jnr, B. A., Sylva, W., Watat, J. K., & Misra, S. (2023). A framework for standardization of distributed ledger technologies for interoperable data integration and alignment in sustainable smart cities. *Journal of the Knowledge Economy*.

Kalloniatis, C., Kavakli, E., & Gritzalis, S. (2008). Addressing privacy requirements in system design: The PriS method. *Requirements Engineering, 13*(3), 241–255.

Kang, Y., Lee, H., Chun, K., & Song, J. (2007). Classification of privacy enhancing technologies on life-cycle of information. The International Conference on Emerging Security Information, Systems, and Technologies (SECUREWARE 2007), IEEE.

Khatoun, R., & Zeadally, S. (2017). Cybersecurity and privacy solutions in smart cities. *IEEE Communications Magazine, 55*(3), 51–59.

Khi, I. A. (2020). Ready for take-off: How biometrics and blockchain can beat aviation's quality issues. *Biometric Technology Today, 2020*(1), 8–10.

Kitchenham, B., & Charters, S. (2007). *Guidelines for performing systematic literature reviews in software engineering, 2*(3).

Kong, Y., Zhao, J., Yuan,, L., Dong, N., Lin, Y. & Yang, B. (2018). Research on data sharing analysis and key technology of smart city. In *2018 26th International Conference on Geoinformatics*.

Kusumastuti, R. D., Nurmala, N., Rouli, J., & Herdiansyah, H. (2022). Analyzing the factors that influence the seeking and sharing of information on the smart city digital platform: Empirical evidence from Indonesia. *Technology in Society, 68*, 101876.

Li, C., & Palanisamy, B. (2018). Privacy in Internet of Things: From principles to technologies. *IEEE Internet of Things Journal, 6*(1), 488–505.

Martinez-Balleste, A., Perez-Martinez, P. A., & Solanas, A. (2013). The pursuit of citizens' privacy: A privacy-aware smart city is possible. *IEEE Communications Magazine, 6*, 136.

Mutanu, L., Gupta, K., & Gohil, J. (2022). Leveraging IoT solutions for enhanced health information exchange. *Technology in Society, 68*, 101882. https://doi.org/10.1016/j.techsoc.2022.101882

National Institute of Standards and Technology, (2013). Guide for conducting risk assessments. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

Nissenbaum, H. (2004). Privacy as contextual integrity. *Wash. l. Rev., 79*, 119.

Norta, A., Matulevičius, R., & Leiding, B. (2019). Safeguarding a formalized Blockchain-enabled identity-authentication protocol by applying security risk-oriented patterns. *Computers & Security, 86*, 253–269.

Office of the Australian Information Commissioner (n.d.). "Australian privacy principles." Retrieved 2 Jun, 2020, from https://www.oaic.gov.au/privacy/australian-privacy-principles

Pal, D., Zhang, X., & Siyal, S. (2021). Prohibitive factors to the acceptance of Internet of Things (IoT) technology in society: A smart-home context using a resistive modelling approach. *Technology in Society, 66*, 101683.

Peacock, J. (2021). What is NIST SP 800 30. Retrieved 9 September 2021, from https://www.cybersaint.io/blog/what-is-nist-sp-800-30

Peppet, S. R. (2014). Regulating the internet of things: First steps toward managing discrimination, privacy, security and consent. *Tex. l. Rev., 93*, 85.

Pfitzmann, A., & Hansen, M. (2010). *A terminology for talking about privacy by data minimization: Anonymity, unlinkability, undetectability, unobservability, pseudonymity, and identity management*. Dresden.

Qian, Y., Liu, Z., Yang, J. & Wang, Q. (2018). A method of exchanging data in smart city by blockchain. In *2018 IEEE 20th International Conference on High Performance Computing and Communications; IEEE 16th International Conference on Smart City; IEEE 4th International Conference on Data Science and Systems (HPCC/SmartCity/DSS)*.

Romanou, A. (2018). The necessity of the implementation of Privacy by Design in sectors where data protection concerns arise. *Computer Law & Security Review, 34*(1), 99–110.

Runyon, B. (2020). *Healthcare CIOs: Prepare for granular patient consent*. Gartner.

Sadhukhan, D., Ray, S., Obaidat, M. S., & Dasgupta, M. (2021). A secure and privacy preserving lightweight authentication scheme for smart-grid communication using elliptic curve cryptography. *Journal of Systems Architecture, 114*, 101938.

Safiullin, A., Krasnyuk, L., & Kapelyuk, Z. (2019). Integration of Industry 4.0 technologies for "smart cities" development. IOP conference series: materials science and engineering, IOP Publishing.

Sandhu, R. S., & Samarati, P. (1994). Access control: Principle and practice. *IEEE Communications Magazine, 32*(9), 40–48.
Shamshad, S., Mahmood, K., Kumari, S., & Chen, C.-M. (2020). A secure blockchain-based e-health records storage and sharing scheme. *Journal of Information Security and Applications, 55*, 102590.
Sharma, S., Singh, G., Sharma, R., Jones, P., Kraus, S., & Dwivedi, Y. K. (2020). Digital health innovation: exploring adoption of COVID-19 digital contact tracing apps. In *IEEE transactions on engineering management*, 1–17.
Silva, P., Monteiro, E., & Simões, P. (2021). Privacy in the Cloud: A survey of existing solutions and research challenges. *IEEE Access, 9*, 10473–10497.
Smith, H., Milberg, S., & Burke, S. J. (1996). Information privacy: Measuring individuals' concerns about organisational practices. *MIS Quarterly, 20*, 167–196.
Solove, D. J. (2006). A taxonomy of privacy. *University of Pennsylvania Law Review, 154*(3), 477–564.
Solove, D. J. (2011). "Nothing to hide: The false tradeoff between privacy and security (Introduction)."
Sotirelis, P., Nakopoulos, P., Valvi, T., Grigoroudis, E., & Carayannis, E. (2022). Measuring smart city performance: A multiple criteria decision analysis approach. *Journal of the Knowledge Economy, 13*(4), 2957–2985.
Spiekermann, S., & Cranor, L. F. (2008). Engineering privacy. *IEEE Transactions on Software Engineering, 35*(1), 67–82.
Stoneburner, G., Goguen, A., & Feringa, A. (2002). Risk management guide for information technology systems, special publication (NIST SP), National Institude of Standard and Technology.
Taplin, K. (2021). South Africa's PNR regime: Privacy and data protection. *Computer Law & Security Review, 40*, 105524.
Tedeschi, P., & Sciancalepore, S. (2019). Edge and fog computing in critical infrastructures: Analysis, security threats, and research challenges. In *2019 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*.
Thapa, C., & Camtepe, S. (2020). Precision health data: Requirements, challenges and existing techniques for data security and privacy. *Computers in Biology and Medicine*, 104130.
Van Blarkom, G., Borking, J. J., & Olk, J. E. (2003). Handbook of privacy and privacy-enhancing technologies. Privacy Incorporated Software Agent (PISA) Consortium, The Hague 198.
Van Slyke, C., Shim, J., Johnson, R., & Jiang, J. (2006). Concern for information privacy and online consumer purchasing. *Journal of the Association for Information Systems*, *7*(6). https://doi.org/10.17705/1jais.00092
Vinod Kumar, T., & Dahiya, B. (2017). "Smart economy in smart cities. In Smart economy in smart cities: International collaborative research: Ottawa, St. Louis, Stuttgart, Bologna, Cape Town, Nairobi, Dakar, Lagos, New Delhi, Varanasi, Vijayawada, Kozhikode, Hong Kong, 3–76.
Vu, K., & Hartley, K. (2018). Promoting smart cities in developing countries: Policy insights from Vietnam. *Telecommunications Policy, 42*(10), 845–859.
Wall, J., Lowry, P. B., & Barlow, J. B. (2015). Organisational violations of externally governed privacy and security rules: Explaining and predicting selective violations under conditions of strain and excess. *Journal of the Association for Information Systems, 17*(1), 39–76.
Wang, Y., Zhang, A., Zhang, P., & Wang, H. (2019). Cloud-assisted EHR sharing with security and privacy preservation via consortium blockchain. *IEEE Access, 7*, 136704–136719.
Wang, C., Zhang, N., & Wang, C. (2021). Managing privacy in the digital economy. *Fundamental Research, 1*(5), 543–551.
Warren, S. D., & Brandeis, L. D. (1890). Right to privacy. *Harvard Law Review, 4*, 193.
Wolford, B. (2020). "What is GDPR, the EU's new data protection law?" Retrieved 2 Feb, 2020, from https://gdpr.eu/what-is-gdpr/.
Xiong, W., & Lagerström, R. (2019). Threat modeling – A systematic literature review. *Computers & Security, 84*, 53–69.
Xu, H., Dinev, T., Smith, J., & Hart, P. (2011). Information privacy concerns: Linking individual perceptions with institutional privacy assurances. *Journal of the Association for Information Systems, 12*(12), 1.
Yang, Y., Zheng, X., Guo, W., Liu, X., & Chang, V. (2018). Privacy-preserving fusion of IoT and big data for e-health. *Future Generation Computer Systems, 86*, 1437–1455.
Yang, L., Xue, H., & Li, F. (2014). Privacy-preserving data sharing in smart grid systems. In *2014 IEEE International Conference on Smart Grid Communications (SmartGridComm)*, IEEE.
Yi, X., Miao, Y., Bertino, E. & Willemson, J. (2013). Multiparty privacy protection for electronic health records. In *2013 IEEE Global Communications Conference (GLOBECOM)*, IEEE.

Zhang, Z. (2019). Technologies raise the effectiveness of airport security control. In *2019 IEEE 1st International Conference on Civil Aviation Safety and Information Technology (ICCASIT)*.

Zhiyong, Z., Yongbin, X., & Jiaying, C. (2024). Digital economy, industrial structure upgrading and green innovation efficiency of family enterprises. *International Entrepreneurship and Management Journal, 20*(1), 479–503.

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.