information

MDPI

Review

A Systematic Literature Review on Cyber Security and Privacy Risks in MaaS (Mobility-as-a-Service) Systems

Rahime Belen-Saglam [1,*], Haiyue Yuan [2], Maria Sophia Heering [3], Ramsha Ashraf [4] and Shujun Li [2]

[1] Computer Science and Digital Technologies, University of East London, London E16 2RD, UK
[2] Institute of Cyber Security for Society (iCSS) & School of Computing, University of Kent, Canterbury CT2 7NP, UK; hy221@kent.ac.uk (H.Y.); s.j.li@kent.ac.uk (S.L.)
[3] Department of Psychology, Alma Mater Studiorum University of Bologna, 40126 Bologna, Italy; m.s.heering@kent.ac.uk
[4] Faculty of Politics and International Relations, Northeastern University London, London E1W 1LP, UK; ra3505phd@students.nulondon.ac.uk
* Correspondence: rbelen@uel.ac.uk

Abstract: Mobility as a Service (MaaS) is anticipated to revolutionize transport by integrating conventional public transport with on-demand and shared services. This innovation promises enhanced convenience, flexibility, and sustainability in urban mobility, drawing interest from both researchers and industry. However, those systems heavily rely on the collection and sharing of personal data among various stakeholders, introducing security and privacy risks. To understand the scale and scope of cyber security and privacy concerns and risks associated with MaaS, we conducted a systematic literature review (SLR) covering 87 relevant research papers published between 2017 and April 2025. Our review represents the most comprehensive examination focusing on cyber security and privacy issues of MaaS systems. Our findings reveal three themes discussed within the MaaS literature: (i) cyber security and privacy risks inherent to MaaS systems, alongside proposed solutions to mitigate such risks; (ii) users' concerns about these risks and how they affect MaaS adoption; and (iii) laws and policies that govern cyber security and privacy aspects of MaaS systems and solutions. As such, our research serves to not only inform MaaS service providers and users but also advise policymakers and legislators on the potential risks involved and the regulatory measures required to address them.

Keywords: MaaS; cyber security; privacy; risks; users' concerns

Academic Editors: Antonio Comi and Aneta Poniszewska-Maranda

Received: 23 March 2025
Revised: 28 May 2025
Accepted: 6 June 2025
Published: 20 June 2025

Citation: Belen-Saglam, R.; Yuan, H.; Heering, M.S.; Ashraf, R.; Li, S. A Systematic Literature Review on Cyber Security and Privacy Risks in MaaS (Mobility-as-a-Service) Systems. *Information* **2025**, *16*, 514. https://doi.org/10.3390/info16070514

1. Introduction

Extensive use and reliance on vehicles have resulted in a multitude of challenges, encompassing climate change, congestion, and health issues, which have profound impacts on the economy, environment, and society as a whole [1]. As these challenges intensify, coupled with the growing prevalence of mobile technology, there has been a heightened demand for alternative mobility solutions. Among these alternatives, MaaS has been suggested as a feasible option, offering solutions to tackle these interconnected issues and potentially catalyze transformative changes in transport systems [2].

MaaS aims to offer passengers a seamless and end-to-end mobility service by integrating traditional services, such as public transport with on-demand and shared services (e.g., ride share, bike share, and car share), through a single platform. This platform enables users to plan, book, and pay for their entire journey [3–5]. Since the 2014 Intelligent Transportation Society (ITS) European Congress and the successful trials of the Whim app in

Helsinki, Finland in 2016 [2,6], the concept of MaaS has garnered increasing global attention. Despite being a relatively recent area of study, the literature on MaaS has grown exponentially in the last five years, and several review articles have already been published [2,7–9]. However, to the best of our knowledge, no previous work has been conducted to systematically look into concerns and risks related to the cyber privacy and cyber security of MaaS. Given that the role of data processing, which includes data exchange among different parties, is crucial in MaaS, the cyber security and privacy issues related to user data are expected to be a principal source of concern [10]. However, in the existing literature, cyber security issues are often relegated to a subtheme that emerges during reviews, lacking a comprehensive analysis of the problems and potential solutions. As stated by Mulley and Kronsel, the existing work only has some shallow discussions of concerns from different perspectives [11]. The predominant focus in these studies remains on barriers to MaaS adoption, with cyber security concerns being reported as one of these barriers, albeit with limited depth in the discussions [11].

To date, we have noticed only seven SLRs covering cyber security and privacy issues as a subtheme in the MaaS literature. In one of those SLRs, Kayikci and Kabadurmus reviewed the literature with the aim of identifying the factors that could hinder the adoption of MaaS [12]. They recognized the lack of regulations in data security as a barrier to MaaS adoption. It has been noted that effective policies and laws play crucial roles in addressing privacy concerns, and the establishment of legislation is essential for maintaining robust governance structures. In the context of data privacy concerns, their study revealed that it is important to ensure that customer rights and the security of customer data are legally safeguarded. Their study also identified that the presence of non-standardized data poses a risk, potentially leading to security gaps and undermining customer trust [12]. However, despite this recognition, the existing deficiencies in these measures have not been adequately discussed.

In another SLR, again conducted to identify barriers faced by MaaS providers in their evolving business ecosystem, technology and data emerged as themes in the literature [13]. These themes were found to encompass four subthemes: data security and privacy, the lack of openness of data and standardization, the modernization of the ICT infrastructure's internet coverage, and real-time information availability. Additionally, the existence of unclear or absent platform architectures was noted [13]. However, that study did not delve into discussions on these themes, and issues related to cyber security and privacy were not elaborated upon.

In another study, an SLR was conducted on MaaS systems, aiming to explore the topics discussed in the MaaS literature [14]. Although that study recognized data security as a theme, it examined only nine publications addressing these concerns. The identified issues encompassed ensuring the protection, confidentiality, and privacy of personal data without compromising operational efficiency; clarifying the rights of actors in a MaaS ecosystem to own and control data; defining standards for data collection, management, and dissemination; and addressing concerns about being tracked. Finally, the researchers identified compliance with the EU's General Data Protection Regulation (GDPR) as a topic; however, further discussion on these matters was limited because of the constrained number of publications reviewed in that study [14].

Our research identified another SLR on MaaS adoption, which reviewed the new mobility technologies and services, especially in autonomous vehicles, drones, micromobility, and MaaS [15]. That study only conveyed that privacy was identified as a concern in the implementation of MaaS, with the potential risk of personal information leakage. The findings were limited to those statements, and details of the privacy concerns were not elaborated upon [15].

A recently published SLR [16] identified 'privacy and security aspects' as one of the eight main topics of MaaS. Although that paper was published in 2025, the SLR only includes research papers published up till 2020. The authors classified privacy and security aspects into four categories: (1) *privacy*, which is defined as aspects that are related to the protection of personal data in MaaS; (2) *threat*, which is concerned about privacy and security threats that have the potential to block the delivery of MaaS (e.g., denial-of-service attacks); (3) *cyber security* linked to MaaS; and (4) *countermeasures*, which are mitigation solutions for security and privacy threats [16]. This categorization largely aligns with the themes identified in our study; however, it does not have in-depth analysis and technical details for each category, which have been addressed in our work.

In addition, Anthony and Sarshar conducted an SLR that looked into data sovereignty for mobility services in smart cities [17]. Although their study did not mention or focus specifically on MaaS, its wide coverage of multiple means of intelligent transport in the smart city makes it relevant to MaaS. The authors highlighted the importance of data privacy in multiple occasions; however, they were from the perspectives of data governance and regulation/legislation.

Finally, there are a few literature review studies that focus primarily on data privacy or cyber security in MaaS systems. For instance, in a recent (less systematic) survey paper [18], data privacy was the main focus, and the privacy-related keywords were included while searching for papers, such as "data privacy", "privacy challenges", "privacy-preserving techniques", and "legal and regulatory in MaaS". However, despite its comprehensive coverage, that work remains unpublished, lacking crucial statistics that an SLR study is expected to provide, including the number of included papers, the search date, and an exact list of databases where the search was conducted. On the other hand, the same researchers recently published an SLR that also identified data privacy issues as the primary focus of their study [19]. They used the terms "privacy" and "data privacy" in their search queries, limiting their results to articles that explicitly discuss privacy-related topics. Additionally, studies addressing broader cyber security concerns without a clear emphasis on data privacy were excluded from their analysis. In contrast, we intentionally did not restrict our search to these specific terms, allowing us to capture studies where privacy was not the central focus or explicitly mentioned in the title or abstract but was still discussed in relation to security. This approach aligns with our study's broader scope, which also considers cyber security risks as a key concern.

Our study corroborates their findings on identified data privacy issues and the techniques proposed to address them. However, by reviewing 87 papers—compared to the 32 analyzed by Garoussi et al. [19]—we provide a more comprehensive perspective. Although their study focuses on techniques to mitigate privacy risks, we go further by first identifying these risks—such as profiling and third-party access—before discussing potential solutions. This distinction offers a deeper understanding of both the challenges and mitigation strategies related to data privacy and cyber security in MaaS. A similar, more technical review was conducted by Ekpo et al., where "security" or "privacy" was included in the search queries, resulting in the selection of 22 papers [20]. Our study complements this work by offering a broader perspective, covering high-level concepts and non-technical security threats. In summary, although prior literature reviews have acknowledged cyber security and privacy as important issues in MaaS, they often do so briefly, selectively, or without sufficient technical or conceptual depth. Our study provides a more expansive and detailed account of these issues by adopting a broader scope, reviewing a larger number of publications, and integrating both high-level governance challenges and technical threat models. Additionally, we differentiate between the privacy and security risks recognized by MaaS researchers and those perceived by MaaS users. By comparing

these perspectives, we highlight critical gaps in user awareness and point to important directions for future research, particularly around user privacy literacy and the acceptance of security-enhancing technologies.

Below, we summarize the key differences that distinguish our work from existing SLRs:

- Unlike previous SLRs that relied on keywords such as "privacy" or "data privacy" in their search strategies, we deliberately excluded these terms and instead applied carefully designed inclusion and exclusion criteria to identify relevant papers. This approach allowed us to capture a broader and more diverse set of studies, including those where security and privacy concerns were discussed but not the central focus;
- A Higher Volume of Reviewed Literature: We reviewed 87 publications, substantially more than most previous SLRs, providing a more comprehensive and nuanced understanding of the field;
- Differentiation Between Researcher and User Perspectives: Our review is the first to explicitly compare risks highlighted by MaaS researchers with those identified by end users, exposing a gap between the technical focus and users' concerns. This comparison lays the foundation for future research on privacy awareness, trust, and technology acceptance among MaaS users;
- Consideration of Driver Privacy: In contrast to most prior studies that focus exclusively on passengers, we also acknowledge and analyze privacy risks for drivers, recognizing their vulnerabilities within the MaaS ecosystem;
- Coverage of Non-Technical Issues: In addition to technical threats, our review includes non-technical concerns, such as regulatory gaps, standardization challenges, and governance issues, which are often overlooked in technical SLRs.

Our comprehensive approach allows our study to contribute to a more holistic understanding of the cyber security and privacy landscape in MaaS while also identifying practical and conceptual blind spots that deserve attention in future research.

In summary, the main aim of conducting this SLR is to explore and learn the landscape of MaaS, particularly focusing on interdisciplinary aspects that are related to privacy and cyber security concerns and risks. In the rest of the paper, when no confusion can arise, we will use the shorter term "security" to denote "cyber security". Note that for MaaS, cyber security is mostly cyber–physical, so it is not purely cyber.

To better put different aspects into perspective in past research, we decided to define the following research questions (RQs), as presented in Table 1.

Table 1. Research questions (RQs) defined for the SLR.

RQ1	What cyber security and privacy risks associated with the use of MaaS systems have been reported in past research?
RQ2	What cyber security and privacy concerns of users regarding the use of MaaS systems have been reported in past research?
RQ3	What is the current state of research on technical considerations and solutions, as identified in prior investigations, for improving the cyber security and privacy of MaaS ecosystems?
RQ4	How have researchers addressed legal issues regarding the privacy of personal data processed by MaaS systems, e.g., which regulations and what kind of policies have been considered on regulating MaaS systems?

This SLR unveiled 87 peer-reviewed articles that specifically discussed cyber security and privacy risks related to MaaS according to the exclusion and inclusion criteria explained in Section 2. Compared with existing reviews on this topic, our SLR makes many new contributions because of our larger coverage of related research papers and a more in-depth

analysis of the included papers. First, we prioritize security and privacy issues as our main focus, providing a comprehensive overview of all the discussions in this area. Second, we consider both the security risks identified by MaaS researchers and the concerns of users, offering two different perspectives and categorizing discussions in the research literature accordingly—a dimension often overlooked in other literature reviews. This approach allows us to recognize the gap between the two perspectives, highlighting the lack of awareness of MaaS users in this regard. Finally, we approach this review from a legal perspective, providing an in-depth and precise representation of the literature in this area. This approach is beneficial for policymakers, service providers, and end users, offering insights into their legal rights and obligations.

The rest of the paper is organized as follows: Section 2 explains the methodology used in this study, followed by presenting the main results in Section 3. Section 4 concludes this paper with further discussion and a set of recommended research directions.

2. Materials and Methods

This SLR was conducted to examine peer-reviewed research work in the literature from 2017 to April 2025. There are two reasons to review articles published within this period: (1) It is a common practice for SLRs to focus on more recent research [21]; (2) the interest for MaaS has considerably increased from 2017 since the successful trial of the Whim app in Helsinki, Finland in 2016 [6], resulting in more publications on MaaS. While conducting this SLR, we followed the recommendations and guidelines of the Preferred Reporting Items for Systematic Review and Meta-Analysis (PRISMA) [22]. As illustrated in Figure 1, the PRISMA procedure for identifying eligible papers for an SLR process consists of the following three main stages:

1. **Identification** of relevant records and removal of duplicate records and non-English records;
2. **Screening** the identified records based on the inclusion and exclusion criteria and conducting further eligibility assessment;
3. **Final selection** of eligible records to be included in the final study.

The rest of this section presents more details on the SLR methodology in terms of the selection of scientific databases, keywords, exclusion criteria, inclusion criteria, and the methodology for the analysis.

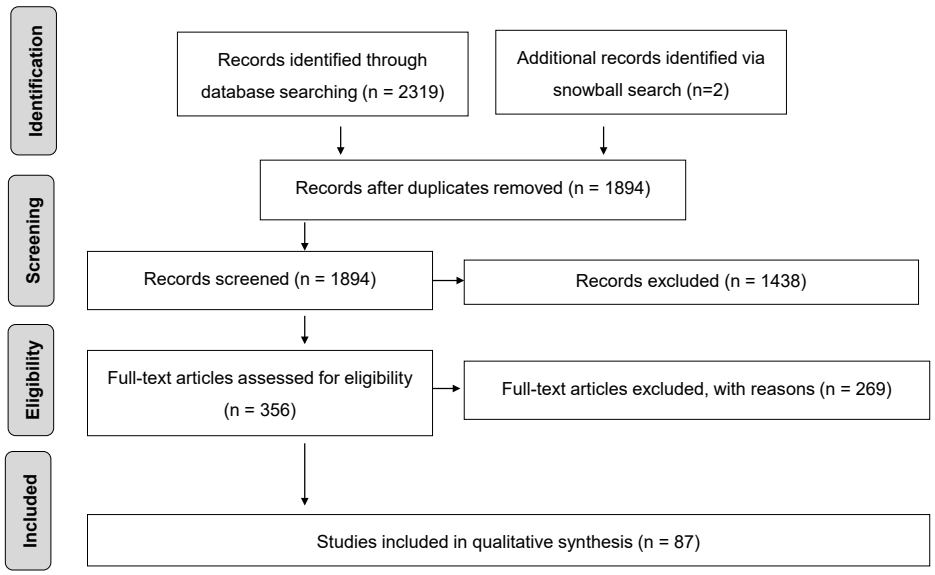

Figure 1. Illustration of the PRISMA procedure used for this SLR.

2.1. Databases

The search was conducted on 17 April 2025 using two large scientific databases: Scopus and Google Scholar. Scopus was selected because it is considered as a scientific database with a comprehensive coverage of interdisciplinary research [23]. In addition, it is worth noting that research papers published by all the main publishers, such as IEEE, ACM, Elsevier, Springer, and John Wiley & Sons, Inc. are well-covered and substantially indexed by Scopus. We also decided to use Google Scholar as an additional database to support this study. Although researchers have suggested that Google Scholar should not be used alone for SLR searches, it has been considered by researchers as a powerful addition to traditional search approaches [24]. In a more recent study on utilizing Google Scholar in SLRs, Yasin et al. [25] discovered that Google Scholar was able to retrieve 96% of the primary studies of selected software-engineering-related SLRs, and most of the primary studies that were not identified using Google Scholar were gray literature.

2.2. Keywords

The following search query was used for Scopus:

```
"mobility as a service" OR "MaaS" OR "mobility service" OR "mobility-as-a-service"
  OR "mobility integration" OR "transport as a service" OR "transportation as a
                                    service"
```

We chose not to include specific keywords related to cyber security or privacy in our search string. This decision was intentional, as preliminary searches showed that including such terms did not significantly improve the relevance of the results and, in some cases, narrowed the scope unnecessarily. By omitting these keywords, we were able to cast a wider net and capture a broader range of studies, which we then filtered using carefully defined inclusion and exclusion criteria to ensure relevance to cyber security and privacy. This approach enhanced the scope of our review while maintaining control over the relevance of the final selection.

Additionally, we limited our search to titles only rather than searching across metadata fields, such as abstracts and keywords. Searching the full metadata returned over 11,600 documents, which was unmanageable given the resources and scope of the study. Titles typically reflect the core focus of a study, so restricting the search to titles helped to ensure that the results were directly aligned with our research questions while keeping the screening process feasible.

We acknowledge that this strategy may have resulted in missing some relevant studies that refer to key concepts only in abstracts or keywords. However, we consider that this tradeoff is acceptable, as it allowed us to maintain a practical and rigorous review process without compromising the quality of the synthesis. Overall, the combination of a broad search strategy and targeted screening enabled us to balance comprehensiveness with manageability.

For Google Scholar, we used the following search query:

```
"mobility as a service" OR "mobility service" OR "mobility-as-a-service" OR
"mobility integration" OR "transport as a service" OR "transportation as a service"
```

We removed “MaaS” because adding this keyword drastically increased the number of returned documents to the level of above 80 k, which would lead to a screening process that is prohibitively time-consuming.

2.3. Inclusion and Exclusion Criteria

To make the search results more relevant, a study was excluded if it met the exclusion criteria, as depicted in Table 2. Then, the further selection of relevant studies was performed to include studies that met at least one of the inclusion criteria, as depicted in Table 2.

Table 2. Inclusion and exclusion criteria.

Exclusion Criteria
→ Published before 2017. → Were not properly or sufficiently peer reviewed, including pre-prints, book chapters, white papers, technical reports, and other forms of gray literature. → Published in languages other than English. → Discussing ride sharing (private, like Uber or Lyft, or public, like bus sharing) when ride sharing is not intended as an integrated part of a MaaS System. → Focusing on automated vehicles when automated vehicles are not integrated with a MaaS System. → Discussing one or more transport systems that involve only one mode of transport.
Inclusion Criteria
→ Have at least brief discussions on the roles played by cyber security and/or privacy risks in the development of MaaS. → Have cyber security and/or privacy discussions on MaaS (which is considered as a system with shared mobility/ticketing and multimodal travel options). A multimodal travel option involves at least one transfer between more than or equal to two transport modes per single trip. → Have considerable discussions on the policy governance of privacy and data sharing/protection and security.

2.4. Final Paper Selection

As shown in Figure 1, 318 articles were retained after the identification and screening stages of the PRISMA procedure. The screening process was conducted by reading titles and abstracts to exclude irrelevant papers. Then, we reviewed the full texts of the remaining articles to make the final paper selection.

2.5. Encoding Data Items

Upon gathering the relevant papers, the first author used a thematic approach for qualitative analysis to develop an encoding scheme. NVivo (https://www.qsrinternational.com/nvivo-qualitative-data-analysis-software/, accessed on 20 April 2025), a popular software tool for qualitative analysis, facilitated the encoding process. The first author identified discussions related to the research questions from the SLR, defining and refining codes incrementally. These codes were regularly reviewed and adjusted as needed. The encoding scheme underwent validation by the second, third, and fourth authors. They also validated the coding of a random subset (25%) of the papers. Their feedback was incorporated by the first author to finalize the encoding scheme and make necessary adjustments. The last author contributed to general discussions about the encoding scheme, performed the final read and edits, and approved the final version of the encoding scheme and encoding results.

3. Results

The publication dates for the 87 articles included in this review clearly show that interest in MaaS among researchers has rapidly grown since 2017, as illustrated in Figure 2.

3.1. Description of Main Themes and Subthemes

As shown in Table 3, we conducted a thematic analysis of all eighty-seven selected papers and classified them into three main topical themes. Papers that explicitly identified and/or reviewed specific cyber security and/or privacy risks of MaaS systems from both technical and non-technical (including human behavioral and social) perspectives were categorized under *Theme 1*. To delve deeper into this theme, we further categorized the papers within theme 1 into the following three subthemes: (1) *privacy risks*, which refer

to specific risks, such as profiling and data sharing, mentioned in the existing literature; (2) *cyber security risks*, which encompass cyber security risks and threats from both technical and non-technical perspectives; and (3) *existing solutions*, which involve existing and potential solutions identified and discussed in the literature to mitigate cyber security and/or privacy risks.

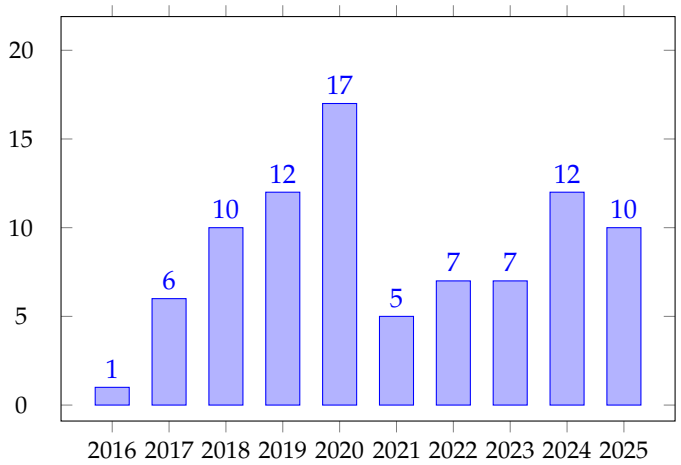

Figure 2. Number of publications per year.

Papers that explicitly looked at the cyber security and/or privacy concerns of users and their impacts on willingness to adopt MaaS systems were categorized under *Theme 2*. Finally, papers that were related to policy and regulations were grouped under *Theme 3*. Although papers considering the GDPR as a governing regulation for MaaS systems dominate the literature, we identified some other laws and reported them as another subtheme. We have also covered studies regarding the implications of privacy laws and regulations on MaaS systems under *Theme 3*. Another subtheme, 'organizational policies', was also identified, encompassing studies about the organizational standpoint regarding the existence/absence and implementation of related policies to ensure cyber security and privacy from users' perspectives.

Table 3. Three identified topical themes and papers in each theme.

Theme	Papers
Theme 1: Cyber security and/or privacy risks of MaaS systems and proposed solutions	$n = 44$: [2,18,26–67]
Theme 2: Impacts of cyber security and/or privacy concerns/risks on the adoption of MaaS systems	$n = 27$: [7,28,47,57,68–86]
Theme 3: Policies and regulations	$n = 25$: [5,10,18,26,28,33,37,54,57,62,71,79,87–98]

3.2. Cyber Security and/or Privacy Risks of MaaS Systems

Risks and concerns regarding cyber security and/or privacy that MaaS may encounter are two of the main themes that emerged in our study. Sections 3.2.1 and 3.2.2 present relevant work on identified cyber security and/or privacy risks recognized and considered for MaaS systems, aiming to answer **RQ1** and **RQ2**, respectively. To answer **RQ3**, Section 3.2.3 delves into related work on existing and cyber solutions to address cyber security and/or privacy risks.

3.2.1. Privacy Risks

Privacy risks related to MaaS have been addressed and discussed from various perspectives in the papers covered by this SLR. We categorize the papers into two categories, corresponding to two subthemes, as outlined in Table 4. The first subtheme, *profiling and inference*, includes articles that discuss how personal data, such as GPS tracking, usage logs, and payment information, collected by MaaS systems can be used to profile and infer human behaviors and mobility patterns. The second subtheme, *third-party access and data sharing*, includes articles that discuss privacy risks related to third-party access of personal data collected by MaaS providers and the sharing of personal data among multiple parties. The rest of this section provides more detailed insights into these themes.

Table 4. Identified different categories of privacy risks.

Subtheme	Description	Papers
Subtheme 1: Profiling and inference	Users' behavior and mobility patterns can be profiled and inferred based on the personal data collected by MaaS applications/systems	[18,26–32,62,63]
Subtheme 2: Third-party access and data sharing	Third-party access to personal data collected by MaaS, data sharing between stakeholders/mobility providers, data sharing to open platforms, and data sharing to government bodies	[2,26,33–38,64,65]

Subtheme 1: **Profiling and inference**

MaaS empowers users to access comprehensive trip services, including planning, booking, ticketing, payment, and real-time information, all consolidated within a unified digital platform, eliminating the need for separate ticketing and payment operations. To accomplish those tasks, MaaS systems collect and process a substantial amount of personal information. For instance, efficient MaaS provision requires the combined time- and location-specific travel behavior data of an individual. On the other hand, users must link their financial information when scheduling payments through MaaS services, adding an additional layer of data to their profiles. These instances collectively contribute to the creation of a detailed individual profile, which may raise issues related to user data and privacy concerns.

To better represent the scope of the personal information processed by MaaS systems, Cottrill analyzed the personal data collected using a MaaS app, namely, the Whim app, which was launched in Birmingham, in the West Midlands area of England in April of 2018 [26]. The review of the privacy policy of the Whim application revealed two main categories or types of personal data collected. The first category includes data collected directly from consumers, such as basic personal details (telephone numbers as account IDs), additional personal details (name, e-mail address, street address, device information, home country, language, credit card, and other payment details), and verification data (personal identity number, photo, or driver's license details for car bookings). The second category includes data collected through app usage, such as transaction information (records of purchases, downloads, user-provided content, requests, agreements, services, and delivery details), positioning and location data, travel data (trip start and end points and times, travel method, cost, and favorite locations), and non-personal data (IP address, access time, browsing habits, and other metadata).

Although this list is not comprehensive and is derived from a single app, it highlights the extensive scale of the data collection and the intricate privacy risks and concerns as-

sociated with MaaS apps. In a recent study, the assets—referring to personal information collected by MaaS systems—were categorized into five broad types to support the risk assessment: (1) User Information (personal and device data), (2) Geographic Data (geolocation), (3) Financial Data (payment and purchase records), (4) Social Network Data (social media single sign-ins), and (5) Verification Data (identity documents, such as driver's licenses, and legal age information for cross-border compliance) [62]. Those studies explicitly showed the personally identifiable information (PII) processed by MaaS systems. As highlighted by Garoussi et al., the processing of PII in MaaS systems is vulnerable and can lead to identity theft, financial fraud, and other forms of cyber crime in the event of a data breach [18]. In their survey study, Garoussi et al. also considered travel history and user preference data, such as preferred modes of transport or payment methods, as PII, which could be recorded to facilitate ease of use and personalized recommendations provided to users. Finally, biometric data, such as facial recognition or fingerprint information, used for identity verification and access control, were also recognized in that study as PII processed by MaaS systems. It was noted that these data could be sensitive, as they could be used for surveillance or other forms of privacy intrusion [18].

Risks associated with personal data collection, as recognized in the literature, extend beyond the processing of PII. One notable concern related to the personal data collected by MaaS applications and systems is the risk of *profiling and inferring*. A study on the utilization of MaaS for urban mobility digitization, by Barreto et al. noted that as a user registers for a MaaS service, the MaaS authorization (i.e., smart city) can analyze the personal data collected and learn about the user's behavior and mobility patterns, including the user's needs, interests, and possible route choices [27]. Similarly, a study conducted by Constantini et al. suggested that it is possible to infer information related to certain illnesses by exploring the patterns extracted from MaaS users' movement data [28]. They also addressed that the exploration of location data can potentially reveal more information and, hence, create vulnerabilities, especially when the user's destination is a cult temple or the office of a syndicate, a political party, a civil organization, or a children's school, as this would introduce legal concerns because of the sensitivity of the destination. Moreover, Cooper et al. highlighted another important risk related to location data [29]. They argued that location data contextualized with the time-of-use information can be valuable, especially to companies in the retail and leisure sector, where the monetization of such sensitive data can introduce wider privacy and ethical considerations, and this should not be overlooked.

With similar concerns, in their survey study, Garroussi et al. emphasized the importance of implementing appropriate safeguards and users' consent mechanisms to ensure the responsible use of location data in MaaS services [18]. Their review uncovered findings similar to ours, highlighting that location data have the potential to disclose sensitive information about users, including their movements, habits, and routines, thereby increasing the risk of stalking, harassment, or other malicious activities. Additionally, their review indicated that location data could expose health-related information, such as medical conditions, medication regimes, and mobility limitations, which could be exploited for purposes like discrimination, targeted advertising, or other harmful activities [18]. To address those privacy concerns, they identified the following techniques in the literature: anonymization, cryptography, differential privacy, distributed learning methods, and blockchains.

Profiling and inference have been examined extensively in a recent literature review concerning AI-driven MaaS systems [63]. The review addressed AI-enabled privacy threats—including profiling, inference attacks, and third-party data misuse—as well as adversarial AI attacks, such as evasion, model extraction, and system manipulation, highlighting their detrimental impacts on the integrity and trustworthiness of MaaS ecosystems.

Their review emphasizes that membership inference attacks (MIAs) and model extraction attacks (MEAs) pose significant security threats to AI-driven MaaS systems, particularly within federated learning (FL) architectures. MIAs can reveal whether specific user data or travel patterns were used in training, while MEAs may replicate proprietary models, undermining competitive advantages. Despite FL's privacy-enhancing design—keeping data on client devices and aggregating local models—its server–client communication structure introduces vulnerabilities such as man-in-the-middle (MitM) attacks. Studies reviewed in their work have demonstrated high inference accuracy for MIAs by both malicious clients and servers, while MEAs exploit model query interfaces to reconstruct models at low cost. It was argued that these attacks not only breach privacy and intellectual property but also serve as entry points for further adversarial actions, like evasion attacks. Therefore, understanding how adversarial vulnerabilities can propagate within the MaaS business ecosystem and identifying which actions by specific stakeholders can contribute to more secure outcomes across the system were reported as critical areas for future research [63]. It was also noted that adversarial attacks are anticipated to evolve toward multimodal tasks, where models process diverse input types, such as texts, images, audio, and videos. Addressing the challenges posed by these attacks—including evasion, extraction, inference, and gamification—will remain crucial to ensuring the reliability and robustness of AI-enabled systems. Their study further emphasizes that these risks are exacerbated by the convergence of emerging attack methods (e.g., inverse learning) with conventional cyber threats (e.g., man-in-the-middle attacks), posing significant obstacles to broader stakeholder engagement and threatening the sustainability of innovative business models within the MaaS domain [63].

Although the privacy risks of profiling and inferring MaaS customers' personal data have been discussed extensively, only a few studies have investigated privacy risks caused by profiling and inferring MaaS service providers' data. Belletti and Bayen indicated that drivers' schedule information is sensitive and should be processed properly to avoid any privacy violations [31]. Hence, they proposed a framework based on a constrained integer quadratic program, which does not need the personal availability constraints of drivers to be shared in their system.

In addition, it was highlighted in the literature that sensitive information about drivers and customers can also be extracted from drivers' GPS positioning [32]. More recent work conducted by Kong et al. argued that the performance records of drivers can lead to violations of identity and location privacy [30]. They proposed a blockchain-based solution, aiming to preserve the privacy of the driver's performance record that will be shared across MaaS operators.

Subtheme 2: **Third-party access and data sharing**

As previously explained, data exchange plays a pivotal role in MaaS systems where various stakeholders require access to diverse data types for seamless operation. Consequently, privacy risks and concerns related to third-party access to personal data collected by MaaS systems and the sharing of such data among multiple parties have been frequently studied in the literature.

For instance, in their study on analyzing the privacy policy of a MaaS app, Cottrill highlighted the complexity of privacy considerations in MaaS applications, particularly concerning the third-party processors (e.g., payment processors and hosting providers) [26]. In their review, Oberoi highlighted that the policies typically cover only the responsibilities of MaaS providers, neglecting third-party server operators who are ultimately responsible for data security—thereby limiting the effectiveness and scope of current privacy protections [64]. Pitera and Marinelli highlighted the importance of understanding which types

of personal data were necessary for which operations and which were not actually needed but still requested by the stakeholders [33]. He and Chow stated that there should be a certain level of privacy control when sharing data on open-data platforms to help public agencies better measure and evaluate the market [34]. Hence, their recommendation was to have a consensus on the type of the data and the format of the data that can be shared to best facilitate mobility platform operations. In a systematic literature review of barriers and risks that prevent MaaS adoption, Butler et al. outlined several privacy concerns, including access to personal data by nefarious sources and breach of intellectual property, potentially resulting in businesses losing competitive advantages [2].

Despite all these concerns and risks, Araghi et al. explored the possibility of utilizing MaaS data for innovative business ideas in transport, which would have a reinforcing effect on MaaS in return [37]. However, this was stated by the researchers under the assumption that all the privacy issues were taken into consideration. On the other hand, it is worth noting that the Finnish government forced all transport service providers to open their data, which was reported as one of the keys to the success of MaaS projects in Finland [38]. The sharing of travel data, including real-time data by the main mobility operators, was identified as a cornerstone for the implementation of MaaS systems in urban areas [38]. Importantly, the Finnish government specifically emphasized the need for sharing regulations and management policies during the implementation of the MaaS projects.

Our review also identified a less-explored but significant theme in the literature: data ownership. Merkert et al. emphasized the importance of understanding operator and transport agency preferences for data ownership and their implications for integration. On the other hand [35], Mukhtar-Landgren and Smith viewed MaaS operators as controllers of the information processed in connection with their service, essentially designating them as the owners of the data [36]. As with data ownership, the issue of algorithm ownership has received limited attention in the existing literature. Peralta et al. conducted a comprehensive study that combined a literature review with insights from a UK-based expert workshop to assess cyber security risks in MaaS development [65]. Their study introduced a MaaS development matrix to evaluate how well various cyber security dimensions are addressed, validated identified risks through expert input, and outlined a future research agenda. The key themes that emerged from the workshop included (i) the growing cyber security risks associated with increased data sharing, (ii) unresolved challenges around the cost and ownership of algorithms, and (iii) the need for well-defined data-sharing and privacy principles. Their study highlights that although data sharing is essential for value creation in MaaS, it simultaneously exposes the ecosystem to new and evolving vulnerabilities [65].

3.2.2. Security Risks

This section presents the security risks associated with MaaS that have been identified in the existing literature. According to the results of our SLR, we can summarize them into two subthemes, as outlined in Table 5. The subtheme *technical security risks* pertains to existing and potential cyber attacks on MaaS systems, while the subtheme *non-technical security risks* summarizes the risks caused by, or linked to, the actions of MaaS stakeholders. The remaining part of this section provides more details.

Subtheme 1: **Technical security threats/risks**

A literature review conducted by Utriainen and Pöllänen suggested denial-of-service (DoS) attacks as one particular type of cyber attack that should be considered in any MaaS system [39]. Thai et al. [40] and Vaidya and Mouftah [41] also reached a similar conclusion in their studies, where the former studied DoS attacks in the general context of MaaS, and the latter considered DoS attacks as a potential attack type for shared electric and

automated mobility. Furthermore, Thai explained that the popularity of MaaS systems could make them increasingly vulnerable to DoS attacks, in which attackers attempt to disrupt the system to make it unavailable to customers [40]. To mitigate this, researchers have proposed a theoretical framework that formulates a stochastic control problem to maximize the passenger loss in the network in a steady state while also having the capability to analyze the financial impacts of DoS attacks on MaaS systems. Apart from DoS attacks, several other attack types, including eavesdropping, spoofing attacks, jamming attacks, hijacking attacks, man-in-the-middle (MitM) attacks, replay attacks, relay attacks, remote exploitable attacks, and ransomware attacks, were also identified by Vaidya and Mouftah as threats to MaaS systems [41].

Table 5. Identified different categories of security concerns/risks.

Theme	Description	Papers
Subtheme 1: Technical security risks	Technical security risks or potential cyber attacks (e.g., denial-of-service (DoS) attacks, eavesdropping, ransomware attacks, and fault injection) to MaaS systems	[39–41,43,66]
Subtheme 2: Non-technical security risks	Security risks are related to the behaviors of end users and stakeholders of MaaS	[27,32,33,38,41,46,47,62]

Another study conducted by Chu and Guo highlighted that smart MaaS coordinators, which personalize transport services based on user profiles, are vulnerable to passenger-spoofing attacks—a novel reinforcement-learning-based threat where attackers impersonate priority passengers using falsified data [66]. Their study shows that such attacks can significantly reduce MaaS platform profitability (by up to 70%) and passenger satisfaction (by 50%), especially when coordinated through multi-agent reinforcement learning [66].

On the other hand, Callegati et al. considered insider attacks as one of the most prominent threats that can have an impact on all tiers [43]. They illustrated that various types of attacks can be associated with insider threats, such as fake data injection, MitM attacks, insider impersonation, data manipulation, and DoS attacks to different tiers of the MaaS stack.

Subtheme 2: **Non-technical security threats/risks**

In addition to the threats and risks given above, there are also some non-technical threats covered in the literature. Adopting a SWOT (strength–weakness–opportunity threat) analysis for a MaaS used in Lisbon, a number of social issues were identified by Cruz and Sarmento as potential security threats, which include: (1) the reluctance of players to have control over their own apps, (2) conflicting objectives between privately and publicly owned companies, and (3) unclear regulatory framework and data privacy issues [46]. Similarly, unawareness and unintervenability that occur when data subjects are not properly involved, informed, and empowered in the processing of their personal data were reported as privacy threat for MaaS systems [62]. The same study also reported five additional privacy threats—namely, non-transparent policies and terms, insufficient data breach responses, lack of user access/modification rights, over-reliance on consent, and unnecessary data collection beyond users' consent [62].

In addition, overpayment and wrong charges were some of the concerns articulated by the MaaS users in another study [47]. On the other hand, Vaidya and Mouftah recognized that the agents, including dishonest individuals, hackers, criminal groups, and dishonest

organizations, can pose potential security threats to MaaS systems [41]. Their findings revealed that dishonest individuals are primarily motivated by financial gain, theft, and/or unauthorized access, which can lead to potential harms, such as identity theft, vehicle theft, and financial loss, for both individuals and organizations. On the other hand, criminal groups were identified as being motivated by a desire to cause service or business disruptions, which can also significantly harm individuals and organizations. Finally, consumer profiling, sabotaging competitors, and/or industrial espionage were considered as the main motives for dishonest organizations to sabotage MaaS systems [41].

Moreover, the illegal and unethical uses of personal data by MaaS operators were other concerns considered by some studies [32,38]. Callegati et al. argued that MaaS operators could undertake many malicious activities, such as passing relevant information to their competitors and the extraction of sensitive information from aggregating anonymized data, which can be considered as potential security threats for MaaS [32]. In addition, it was suggested that the action of disabling the GPS device on drivers' vehicles can be considered as an insider threat that compromises the reliability of the GPS positioning system and that of the other services depending on it.

Furthermore, a set of challenges to ensure the security of MaaS systems has been identified. The availability and consistency of data were reported as two of the main challenges for MaaS systems [33]. It was highlighted that the integration of booking systems from multiple MaaS providers would require data sharing and strong cooperation and agreement among partners. However, achieving compatibility across Europe with different public transport providers/approaches was highlighted as a major challenge for MaaS systems [33]. Ensuring both the integrity and the availability of the applications and systems, regarding the integration of mobility technology platforms, was also seen as an important challenge in another study [27]. From a policy perspective, the study also identified the challenge of managing personal data in a way that ensures protection, confidentiality, and privacy, while maintaining the system's operational efficiency [27].

3.2.3. Existing Cyber Security Solutions for MaaS Systems

Although the majority of the reviewed studies have primarily aimed to identify cyber security and/or privacy risks associated with MaaS systems, some have also outlined the potential solutions or guidance to mitigate these risks. For instance, ensuring secure payment options, providing reliable and real-time information, and assuring data privacy were some of the guidelines considered as crucial in the literature [57]. Adopting a similar approach, Vaidya et al. [41] formulated a set of guidelines to mitigate potential vulnerabilities, e.g., access to the centralized back-end system, distributed authentication and authorization, secure association of the communication between the participating entities, and employing credential service authority (CSA) that issues enrollment and security credentials in car-sharing systems in smart cities. These guidelines cover cryptographic algorithms and protocols, communication security for end-to-end protection, and access control authorization methods.

Although the guidelines proposed by Polydoropoulou [57] and those by Vaidya and Mouftah [41] may seem to be different, they share some similarities, where both studies address issues related to data privacy, access control/authentication, and communication security, albeit to varying degrees.

In addition to those generic guidelines, our review also identified some specific solutions proposed in the literature, using a variety of techniques. Blockchain technology was the most frequently cited technology used to develop countermeasures for various types of threats. Nevertheless, other non-blockchain approaches also exist in the literature. Thus, the remaining section is divided into two parts: The first part mainly reviews blockchain-based

solutions, while the second part focuses on non-blockchain-based solutions. As shown in Table 6, many blockchain-based solutions were developed to allow MaaS systems to handle the secure payment and exchange of services of MaaS as well as to offer privacy preservation at the same time. On the other hand, among the non-blockchain-based solutions, some prioritize privacy preservation, while others emphasize developing secure solutions for data security and access control. The remaining section provides more in-depth details on these solutions.

Table 6. Cyber security solutions for MaaS.

Mitigation Solutions	Brief Description	Papers
Blockchain-based solutions	Secure ways for the payment and exchange of services and privacy preservation	[18,28,30,46,48,49,49–52,61,67]
Non-blockchain based solutions	Data security and access control	[18,26,41,44,45,53–60,63,64,99]

Blockchain-Based Solutions

Blockchain technology has often been considered as a solution to handle cyber security issues for MaaS systems [28,30,46,48–52,61,67]. Among all the studies utilizing blockchains to enhance security and privacy in MaaS systems, several objectives were reported. In their literature review, Kulla et al. categorized those objectives as follows: improving cyber security and/or privacy for passengers' identity management, enhancing transport services' trust and reliability, the separation of services into multiple MaaS operators, data synchronization, and providing secure ways for payments [52]. Similarly, in their survey study, Garroussi et al. listed the advantages of using blockchains as follows: securely and transparently storing and tracking data related to mobility services, such as vehicle usage, payment information, and trip history [18]. It was noted that blockchain technology enables the more streamlined and efficient management of mobility services, fostering enhanced trust and accountability among the involved parties. As the decentralized nature of blockchains offers the potential to eliminate intermediaries, lower transaction costs, and expedite transactions, this technology was argued to facilitate easier and more cost-effective access to a variety of mobility services, including car sharing, ride hailing, and public transport. Additionally, the incorporation of smart contracts was stated to automate various processes in MaaS, such as payments, scheduling, and route planning, thereby improving the overall efficiency, reliability, and user satisfaction of mobility services [18].

Similarly, Constantini et al. also suggested the deployment of smart contracts on the blockchain to make the payment and exchange of other services in MaaS systems faster and more convenient while ensuring customer privacy when sharing data [28]. On the other hand, Cruz and Sarmento recommended utilizing smart contracts to allow more effective contract management and compliance in addition to decrease the existing complexity of monitoring traditional "paper-based" contracts [46]. More specifically, Nguyen et al. pointed out that smart contracts need to be enforced in the blockchain-based MaaS to specify the contractual terms and statement, which can be achieved by applying cryptographic zero-knowledge argument schemes (SNARKs) to demonstrate that the terms can be satisfied and agreed with, without disclosing the private information related to the passengers named in the contract [48].

In another study, Bothos et al. pointed out that blockchain tokens allow real-time transactions, which make it possible to have micropayments with fewer transaction fees and additional security and trust [50]. The authors also added that the possibility of having conditional transactions by encrypting the data with selective access rights, using the blockchain, can lead to increased security and privacy for personal

information. They suggested that the solution could be the self-sovereign identity, which can give users complete control over their personal data via a distributed-ledger-based foundation approach supported by Hyperledger Indy (distributed ledger software: https://www.hyperledger.org/projects/hyperledger-indy, accessed on 1 May 2025). Similarly, Miron et al. developed a blockchain-powered MaaS platform using Hyperledger Fabric (https://hyperledger-fabric.readthedocs.io/, accessed on 1 May 2025) to enhance security, transparency, and efficiency [61]. The authors highlighted several key blockchain-based features, including identity management, modular architecture, scalability, privacy and confidential transactions, and data management, allowing the proposed system to be integrated with urban the transport ecosystem to potentially enhance stakeholder collaboration and trust with end users in the context of a smart city.

Putting those ideas into practice, Chinaei et al. developed an exchange smart contract platform to guarantee a secure, privacy-preserved, and hassle-free service exchange for customers [49]. The identities of the users were known by the service providers; however, they were not revealed to the other customers and peers of the blockchain network. In addition, with the proposed solution, it was possible to eliminate the dependency on third parties, as the proposed smart contract allowed commuters to exchange and trade their cryptotickets in a privacy-preserving manner without the need to trust the other party. Furthermore, Nguyen et al. conceptualized a blockchain-based MaaS system to improve trust and transparency for stakeholders by distributing computational resources to different transport providers at the edge of the network [48]. They suggested that further research on static analysis needs to be conducted to address security issues caused by smart contract builders.

In addition to the blockchain-based smart contract approach, other blockchain-based techniques have been proposed in the literature to offer privacy preservation and enhanced security to MaaS end users. In Kong et al.'s study, the authors studied drivers' performance record data, which are highly related to location and can be used to infer individuals' behaviors and characteristics [30]. In MaaS, drivers may not want to share such sensitive sensory data with MaaS operators. However, driver performance data are crucial for MaaS providers to develop and deliver personalized services. Thus, Kong et al. proposed a privacy-preserving and verifiable data aggregation scheme, using blockchain technology, which adopts (1) a modified Paillier cryptosystem and an identity-based signature scheme to aggregate and authenticate users' performance history in a secured manner, and (2) a permissioned blockchain with the proof-of-stake (PoS) consensus for immutable performance record sharing.

Non-Blockchain-Based Solutions for Privacy Preservation

As mentioned above, apart from the blockchain-based approaches, researchers have explored several technologies to achieve cyber security and privacy in MaaS systems. For instance, Campolo et al. used digital twin (DT) technology to facilitate data transmission to various stakeholders [55]. In their proposed solution, each DT could share data with authorized applications, using properly configured protocols to ensure the security and privacy of the sensitive information regarding commuter mobility and public transport vehicles in MaaS. On the other hand, Christiaanse emphasized the need for trust and privacy in MaaS and proposed extending the contract net protocol (CNP) (modeled in the canonical form with a dimensioned Petri net) to include secure privacy-preserving communication flows [56]. This approach was followed to ensure a balance between the data quality and privacy. In addition, to address data security issues and provide better security practices, Cottrill recommended using industry-standard security mechanisms for MaaS systems, including (1) storing collected personal data in protected databases

located behind a firewall, with both physical and software-based access controls provided by their hosting provider; (2) having PCI-DSS-Level-1 certified payment providers; (3) applying pseudonymization and encryption to the personal data; and (4) having a process for regularly testing to assess and evaluate the effectiveness of all those measures [26]. Encryption mechanisms were also used to transfer and store the data securely.

In a study of shared electric and automated mobility services, Vaidya and Mouftah suggested utilizing the novel technique of conjugated authentication and authorization (CAA), which comprises the entity authentication of the participating entities and authenticated prior binding (APB) [41]. This was proposed as a security solution to ensure that the identity of another party was the same as that stated and was actually participating in the authentication process. On the other hand, their study also proposed using an APB scheme, a technique combining a cryptographic hash function and an encryption scheme, to cryptographically bind the participating entities and their data together so that this binding could be easily verified by a third party [41]. Even though the details were not covered extensively, Breuer et al. also reported conducting encryption mechanisms in their proposed solution to transfer and store the data securely in MaaS systems [59]. Cloud computing is another technology utilized in MaaS systems for the sake of security [58]. However, the details regarding how the proposed solution helped to secure the system were not given in their study either.

The interoperability of the data within MaaS systems is another issue discussed in the literature. As mentioned before, MaaS serves as a platform to integrate different transport services, aiming to be accessible to commuters on demand. The data collection and processing from different sources are important to analyze and provide trip options to match users' needs and preferences. One of the challenges in this context is to ensure interoperability in such a heterogeneous environment. To address this issue, Mouhibbi et al. proposed a MaaS architecture consisting of four different components, including a task receiver component (TRC), a task sorter component (TSC), a task persister component (TPC), and a task orchestrator component (TOC) [44]. Particularly in the TRC, the levels of security between the different components were strengthened using modularity, and every connection was checked to ensure the rejection of all the unauthenticated requests.

Seamless MaaS provision is one emerging research topic, Hoess et al. identified the 'user privacy protection' as one of the key requirements for ensuring data protection in the development of seamless MaaS solutions. The authors also addressed that a well-designed digital wallet could play a crucial role in preserving user privacy by preventing tracking through routing service providers [60].

Addressing a related concern, cross-border mobility, Katsaros et al. highlighted the challenge of configuring security features locally within a recognized 'trust domain' when multiple network operators or countries are involved [54]. They advocated for employing a service-layer security approach, utilizing message queue telemetry transport (MQTT), mobile/multi-access edge computing (MEC), and transport layer security (TLS) connections to ensure secure data exchange across diverse domains. They stressed the necessity of international agreements, potentially at the European level, to address co-existence issues and ensure the implementation of privacy preservation mechanisms.

In a manner similar to that of Katsaros et al. [54], to address the interoperability challenge, Campolo et al. also suggested utilizing MEC and argued that the use of standardized protocols cannot ensure interoperability on the application layer [53]. Instead, the open mobile alliance (OMA) lightweight machine-to-machine (LwM2M) protocol was suggested to be explored for a number of benefits that included device management, information reporting, multi-data format, multi-security protocol support, and access control. MEC

was also recommended in a recent review; however, it was also noted that MEC comes with its own challenges, such as optimized resource allocation and transparency [64].

In their literature review, Garroussi et al. categorized data privacy methods for MaaS systems into anonymization, cryptography, differential privacy, distributed learning methods, and blockchains [18]. Anonymization practices included sending approximate rather than precise location data and anonymizing passenger identities. Examples of the cryptographic techniques given included homomorphic encryption and secure multiparty computation, but they were noted to potentially slow the processing time and complicate data sharing. Differential privacy, which adds random noise to protect users' data while maintaining service quality, was stated to reduce the risk of privacy breaches. Federated learning and split learning were identified as distributed learning techniques, preserving data privacy by training models without transmitting raw data to central servers. A similar approach was also recommended by Carvalho et al. where machine-learning methods were proposed to be applied in edge servers to help to detect these EOC-related attacks and security breaches in MaaS systems [45]. The same technique was also employed in another study, which combined federated learning with deep reinforcement learning and privacy-preserving techniques [99]. To address the privacy risks in centralized deep reinforcement learning (DRL) for MaaS, their study proposed a privacy-preserving federated deep deterministic policy gradient (FDDPG) approach. This method enables local training on user devices and shares only gradients using secure aggregation protocols, thus protecting against information leakage and inference attacks. Tested on real-world and synthetic NYC data, FDDPG improved the MaaS platform's profit by 90% and passenger satisfaction by 15% while maintaining robustness against agent dropout—enhancing both utility and user trust in data-driven MaaS systems. The effectiveness of the DRL has also been validated in a recent literature review focused on AI-driven MaaS systems [63].

3.3. Users' Cyber Security and Privacy Concerns and Their Impacts on the Willingness to Adopt MaaS

In this section, we represent the users' cyber security and privacy concerns identified in the literature and delve into their impacts on the willingness to embrace MaaS systems.

3.3.1. Users' Cyber Security and Privacy Concerns

Although the majority of studies addressing cyber security and/or privacy concerns in MaaS systems primarily concentrate on the potential risks within the realm of researchers, there are also some studies that shift their focus toward the users' perspectives, aiming to pinpoint their specific concerns. For example, in a survey study enriched by workshops with stakeholders and focus groups with end users, Polydoropoulou et al. uncovered that the privacy issues of end users primarily stem from the exchange of tracking and credit card data and significantly influence their decisions regarding MaaS utilization [57]. On the other hand, Schwinger and Krempels argued that calendar data and user preferences are the data types that MaaS users are not willing to share with external service providers [68].

To better investigate those concerns, Lopez-Carreiro et al. conducted a survey involving 1000 respondents in the metropolitan area of Madrid, evaluating privacy concerns through statements such as 'I agree to share my profile, opinions, etc. with other users when using apps', 'I agree to share my personal information with companies when using apps', and 'I agree to my personal information being checked to receive personalized recommendations'. Their results supported the hypothesis, revealing that privacy concerns, the need for control, and environmental awareness each had a positive indirect effect on MaaS adoption, mediated by users' expectations of the service. In contrast, technophilia exhibited both direct and indirect effects on adoption [69]. A similar study was carried out by Lopez-Carreiro et al. in Randstad, the Netherlands in 2024 [82]. The results further

confirmed that privacy issues, among other factors, have a determining influence on the intention to uptake MaaS. Similarly, after collecting over 29,000 online reviews and applying a series of text-mining and unsupervised machine-learning techniques on them, Aman and Smith-Colin revealed that information privacy was one of the users' complaints, together with technical errors and app crashes [70].

Similar concerns were reported by Alyavina et al. in their study where they conducted semi-structured interviews in three different UK cities, namely, London, Birmingham, and Huddersfield [47]. The participants expressed concerns regarding potential cyber security threats, emphasizing that the infiltration of MaaS systems by hackers or terrorists could pose significant risks to lives in various ways.

Risks around third-party access were recognized and articulated by some of the participants in another study where access to location information was specifically given as a privacy concern [71]. This was confirmed in a recent study, in which it was highlighted that data privacy concerns, especially related to third-party data sharing, significantly affect user acceptance of MaaS services [85]. In addition, discussions regarding data ownership were another issue articulated by MaaS users in the literature. The identification of the owner of the data processed using MaaS is essential, as data ownership assigns property rights to the data. In the workshop conducted by Sochor et al., data ownership was identified as an important aspect from users' perspectives [7]. It is noteworthy that these two concerns were reported in only one study.

The level of trust in service providers' abilities to securely handle their personal information is another issue handled in only one study in the literature [71]. Although reporting a significant level of trust overall, distinctions were noted among user groups. Tesla owners and shared-car users exhibited lower trust levels compared to bus users. Trust levels also declined with age, with the highest levels observed among those aged 20–29 and diminishing in older age groups. Male respondents aged 50–59 expressed concerns about data breaches, unclear data usage purposes, and information aggregation [71].

From a slightly different angle, Wu et al. [79] looked at the barriers in developing MaaS systems from the perspective of multimodal freight transport. The authors identified obstacles in multimodal freight transport that could inform MaaS development by reviewing and comparing the past literature from both domains. They argued that the risk of ineffective information sharing among stakeholders would be a significant challenge for MaaS system development and suggested that MaaS operators should pay attention to the tradeoff between information sharing and robust privacy protections to prevent potential user data misuse.

3.3.2. Impacts of Privacy/Security Concerns on MaaS Adoption

Numerous studies have explored the key variables that could affect users' acceptance of MaaS adoption, yet only a limited subset has acknowledged "privacy/security risks and concerns" as a pertinent factor. The existing literature lacks consensus on the impacts of these concerns on the acceptance and adoption of MaaS, with some studies reporting a negative influence while others indicate no discernible relationship between the two. In Table 7, we provide a comprehensive list of the relevant papers included in this SLR, denoting instances where 'NO' signifies no impact and 'NE' denotes a negative impact. Additionally, the table incorporates details such as the publication year, research methods, number of participants, and study location for a comprehensive overview.

As shown in Table 7, more than half of these studies were conducted in Europe, one study was based in Asia, and three studies were conducted in the UK. Among these studies, the use of a survey is the most frequently used methodology. The privacy/security concerns considered in these studies are not very comprehensive, where only one or two aspects of

privacy/security concerns were considered per study. In addition, mixed results about the impacts have been reported. The rest of this section presents more details regarding those discussions in the literature.

Table 7. Studies that consider security and privacy concerns as factors that affect MaaS acceptance and adoption.

Year	Research Method(s)	Study Location(s)	Paper	Impact(s)
2020	Survey (1067 participants)	Germany	[73]	NO
2020	Questionnaire (1078 participants)	Amsterdam and Eindhoven areas (Netherlands)	[75]	NO
2020	Survey (600 participants)	Shanghai (China)	[77]	NE
2020	Workshops (90 participants), focus group (40 participants), survey (106 participants)	Budapest (Hungary) and Manchester (UK)	[57]	NE and NO
2020	Interactive workshop 1 (9 participants aged 8–13), Interactive workshop 2 (8 participants aged 14–17), and Interactive workshop 3 (3 participants aged 16–18)	North East of the Newcastle region (UK)	[76]	NE and NO
2021	Survey (1000 participants)	Madrid (Spain)	[69]	NE
2020	Workshop (20 participants, 8–18 years old)	North East England (UK)	[76]	NO
2020	Semi-structured interview (40 participants)	London, Birmingham, and Huddersfield (UK)	[47]	NE
2020	App trial, survey, and focus group (124 participants)	Brussels (Belgium), Edinburgh (Scotland), Canton Ticino (Switzerland), and Ljubljana (Slovenia)	[74]	NO
2022	Semi-structured interviews (47 participants), survey (23 participants), and survey (187 participants)	Norway	[71]	NO
2024	Online survey (700 participants)	Budapest University of Technology and Economics	[86]	NO
2025	Face-to-face survey (402 participants)	Beijing, China	[81]	NO
2025	Survey (697 participants)	Budapest University of Technology and Economics	[80]	NO
2025	Survey (1015 participants)	Qatar	[83]	NE
2025	Survey (1260 participants)	Beijing, China	[84]	NE
2025	Survey (107 participants)	the Netherlands	[85]	NE and NO

'NO' and 'NE' represent no impact and negative impact, respectively.

Negative Impacts on MaaS Adoption

The research reviewed in this section suggests that cyber security and/or privacy considerations negatively affect individuals' willingness to adopt MaaS [28,57,77,83,84]. In a study employing behavioral models to investigate the adoption of MaaS, Ye et al. analyzed the effects of several parameters, which included perceived risk [77]. The concept of perceived risk was derived from a set of four questions concerning potential negative outcomes associated with consumers' service usage. Notably, one of these questions specifically addressed concerns related to the potential leakage of personal privacy. The researchers found that among the factors included in their model, perceived risk was the only negative predictor of behavioral intention to use MaaS. Social impact was the strongest predictor, followed by individual innovation, effort expectation, performance expectation, and perceived risk. Their study, therefore, proposed a number of strategies for the promotion and application of MaaS, including strengthening the protection of users' information and enhancing the service stability of MaaS, to eliminate users' concerns.

Moreover, Alyavina et al. [47] conducted semi-structured interviews to explore the barriers and facilitators of MaaS acceptance and uptake. Trust was among the five core themes that they identified as critical determinants underpinning MaaS acceptance and success, where cyber security was considered as one part of it. In a related study, Lopez-Carreiro et al. proposed a behavioral framework to explain possible determinants and the associated power to predict MaaS adoption, driven by the theoretical constructs of the technology acceptance model (TAM) [69]. Using the behavioral framework, the

researchers conducted a survey comprising 1000 respondents in the metropolitan area of Madrid to identify attitudinal and personality factors relevant to MaaS adoption. They hypothesized that technophilia, privacy concerns, the need for control, and environmental awareness explained users' expectations of the services integrated by MaaS applications and the intention to adopt the services. In this study, privacy concerns were measured through the following items: "I agree to share my profile, opinions, etc. with other users when using apps", "I agree to share my personal information with companies when using apps", and "I agree to my personal information being checked to obtain personalized recommendations". It was one of the variables found to explain 64% of individuals' willingness to adopt MaaS, together with technophilia, the need for control, environmental awareness, and users' expectations of the services integrated by MaaS applications. More recently, Yu et al. [84] modified the TAM to explore the willingness of people in Beijing to use MaaS, where perceived risk was examined as an influencing factor. Similar to the findings in [77], perceived risk negatively affects more than 1000 participants' willingness to uptake MaaS. In particular, their participants were most worried about the misuse of private information for other purposes without formal consents.

Similarly, a study consisting of a survey, workshops with stakeholders, and focus groups with end users, revealed that privacy issues were mainly driven by the exchange of tracking and credit card data, which was a significant concern for end users, influencing their decisions to use MaaS [57]. In addition to the financial data of users, Iotzov et al. recognized the commercially sensitive fare-costing information of mobility providers as data that require the reassurance of cyber security and privacy [72]. On the other hand, the possibility of tracking users' movements and acquiring their location data have been recognized as particularly sensitive issues by Constantini et al. [28]. It has been noted that location data can indirectly reveal the sensitive data of individuals, like information regarding their health, their religious beliefs, the places they most frequently visit, as well as other information relating to individuals' private lives [28].

More recently, a survey study carried out in Qatar investigated the role of subscription sharing and nationality in MaaS adoption in Qatar. Although privacy concern was not a primary factor considered in this survey, the results from the users' feedback specifically highlighted that concerns about privacy were considered as a critical factor influencing the willingness to uptake MaaS [83].

No Impact on MaaS Adoption

In contrast to the studies discussed in the previous subsection, the research reviewed in this subsection indicates that cyber security or privacy considerations are not given precedence when contemplating MaaS adoption. Instead, individuals' willingness to adopt MaaS appears to be overwhelmingly influenced by considerations of the "ease of use" and "perceived usefulness" of the service as well as by attitudinal and personality factors. For example, conducting qualitative in-depth interviews with potential MaaS users, Schikofsky et al. reported that the adoption decision would not be significantly influenced by data privacy and data security concerns or concerns about the data usage (e.g., the tracking of mobility behavior) [73]. The majority of the participants in this study reported that they would not consider data security and privacy concerns as long as MaaS provided value for their daily mobility. This finding was confirmed in a recent study, which focused on identifying consumer preferences and segments on MaaS platforms, and data privacy was reported to rarely determine customers' decisions [85].

Similarly, in another study conducted by Huang [71], it was noted that MaaS users were not necessarily worried about data privacy. Their findings revealed that users are aware of privacy issues, but this does not necessarily affect their intention to use MaaS. In

this study, several interview participants expressed their readiness to share their mobility data to enhance the convenience of the services. Researchers have explained this with the "privacy paradox phenomenon" [78] and argued that this might be explained by the users' expectations to receive better mobility services. More recently, Tang et al. identified six key characteristics of MaaS, with "security and privacy" being one of them [81]. According to these characteristics, Tang et al. conducted a face-to-face questionnaire survey to explore the potential adoption of MaaS in Beijing, China. The results showed that only a low percentage (23.6%) of the respondents expressed concerns about "security and privacy", suggesting the potential tradeoff between privacy concerns and personalized experiences. Another study conducted with students at Budapest University also reported a lack of awareness or preparedness regarding privacy-related concerns [86]. Those findings are mostly inline with findings from earlier studies [71,78].

Similarly, user feedback collected from focus groups in a study conducted by Wright et al. revealed that users are happy to share their personal data as long as they can benefit from MaaS systems [74]. In line with this, Polydoropoulou et al. reported that some participants stated that collecting data and receiving feedback through MaaS mobile applications could help to improve the transport system [57]. This also applied to location data, with users reportedly unconcerned about GPS-based location tracking [75]. Users perceived processing GPS data as being advantageous, recognizing its utility in enhancing MaaS subscription benefits [75].

Casado et al. found that some of the participants they surveyed and interviewed seemed to accept that their movements were already being tracked by apps, such as Snapchat or public transport apps, and thereby assumed the same would be true for any MaaS apps [76]. One of the participants interviewed in the study conducted by Huang shared similar opinions and explained that she could not be bothered with evaluating data gatherings because the service providers already have a lot of her information, so it is too late to worry about it [71]. Kriswardhana et al. conducted an online survey of 687 students from Budapest about their preferences toward different aspects of MaaS. The findings suggested that the students would still prefer to use routing aspects of MaaS applications, even when being aware of potential data privacy and security risks [80]. One plausible explanation is that students' familiarity with routing features leads them to prioritize convenience over potential privacy concerns.

3.4. Policies and Regulations

To facilitate a smooth adoption of MaaS, it is vital to address legal aspects, such as policy frameworks, legislative reforms, and governance concerns, related to cyber security and/or privacy. However, notably, the development of privacy regulations and organizational policies and the implementation of privacy-sensitive and cyber-secure MaaS models are either evolving or underdeveloped. Moreover, there is a need to keep updating these policies to ensure that MaaS is secure and privacy-sensitive in the long run. This part of the SLR, therefore, focuses on the existing literature regarding *privacy regulations*, examining their presence or absence and, finally, *organizational policies* within the context of the MaaS.

3.4.1. Privacy Regulations

MaaS relies heavily on many stakeholders to operate, thereby necessitating regulations regarding information security and privacy [33]. Therefore, some studies in the MaaS literature focused on exploring data privacy regulations that could potentially be used to regulate MaaS systems. It has been noted that the lack of suitable regulations introduces vulnerabilities to MaaS systems [10], and the capacity of existing regulations to govern

MaaS systems has been discussed in these studies at varying levels of detail. Although the majority of these studies converge on applying the GDPR to MaaS systems (see the GDPR section), our review also identified other regulations considered as applicable to MaaS systems, categorized in the subsequent section (Overview of Other Privacy Laws and Regulations in MaaS). This section further explores the implications of privacy laws and regulations for MaaS services.

GDPR

The studies reviewed in our study consistently emphasized the GDPR as a prominent regulatory framework that MaaS operators and providers could adopt to address privacy concerns associated with the processing of personal data in the MaaS context [10,33,54,57,62,89,90]. The GDPR, implemented in 2018, lays down the rules for the collection, processing, and storage of personal information, emphasizing individuals' rights and the obligation of organizations to safeguard users' data. It is essential to note that the GDPR is triggered when a system processes personal data, implying identifiable information about individuals. However, applications exclusively handling anonymous data fall outside the scope of the GDPR. This distinction was considered in the MaaS literature, and it was noted that personal travel information processed using MaaS systems, such as vehicle availability, origins, destinations, financial information, and social network data, are examples of data that could be considered as personal under the GDPR [26]. Murati emphasized the explicit mention of location data as personal data in Article 4 of the GDPR [91]. They highlighted in their study that in some cases, location data transform to sensitive information, revealing details like visits to specific locations related to medical care, religious activities, or aspects of one's private life. In such cases, they added, a higher level of protection is required by the GDPR, as outlined in its Article 9, which explicitly restricts the processing of such data unless specific conditions are met.

In their checklist prepared for MaaS operators, Pagoni et al. included being in line with the GDPR in terms of data storage and protection and collecting consent for the collection of personal information [5]. They also added that as the GDPR requires, consent must be freely given, with a clear explanation of what data are being collected, who is collecting the data, and what the data would be used for. Finally, providing the option for users to opt out from the data being collected was another data privacy practice covered in the checklist [5]. Consent management was also handled by Garroussi et al. [18]. Giving an example from a MaaS company in Germany in their study, they emphasized that this company needs to extensively revise its data collection procedures to ensure explicit users' consent [18]. In addition to consent management, Cottrill and Constantini et al. pointed out Privacy by Design (Article 25 of the GDPR) as a data privacy concern for MaaS systems, which requires privacy requirements to be considered in all the phases of the system development and appropriate measures to be fulfilled for built-in privacy [26,28].

On the other hand, delivering clear and user-friendly privacy statements was given as mandatory for MaaS providers and operators to ensure GDPR compatibility according to Constantini et al. [28]. Cottrill also referred to the territorial requirements of the GDPR [26]. Analyzing the privacy policy of a MaaS app and the statements given in it regarding the transfer of personal data across international borders, including to countries outside the European Economic Area (EEA), she concluded that the policy appeared to be in compliance with the territorial requirements of the GDPR. It was noted that such statements were beneficial not only to the service providers, who would avoid compliance issues and potential fines but also to the users, who would be able to be confident that their data were processed with adequate respect and protection [26].

Kamargianni and Goulding also mentioned the GDPR in the context of data security in MaaS systems [92]. They suggested that the open data and sharing of data for MaaS could have an impact on data security, and, hence, they reviewed the factors covered by the GDPR, like data minimization (processing the least amount of personal data necessary) and the anonymization and encryption of the data [92].

In addition to those, another GDPR element discussed in the context of MaaS is the "Data Protection Impact Assessment" (Article 35 of the GDPR). In their study, Garroussi et al. suggested the implementation of these assessments for MaaS service providers to showcase a commitment to privacy, build trust among users, and facilitate regulatory compliance [18]. This was also confirmed by Murati, who argued that MaaS providers might engage in processing sensitive data, and they must appropriately address the adoption of the "Data Protection Impact Assessment". Researchers have emphasized that failure to meet these obligations may result in fines and liabilities toward passengers (Article 82 of the GDPR) [91].

Garroussi et al. additionally argued that privacy impact assessments can play a pivotal role in guiding the design and deployment of MaaS services, fostering the integration of privacy measures from the outset [18]. It was highlighted that this proactive and preventive strategy aligns with the "privacy-by-design" approach endorsed by leading data protection frameworks, such as the GDPR [18].

Finally, GDPR compliance has also been identified as a trust issue from the users' perspectives in a survey study conducted by Huang [71]. One participant considered a MaaS service provider as trustworthy because the company is based in Norway and is obligated to adhere to the GDPR [71].

Overview of Other Privacy Laws and Regulations in MaaS

Even though the GDPR has been the most cited regulation in MaaS studies, there are some other regulations considered by MaaS researchers to have impacts on those systems. In their survey study, Garroussi et al. pointed to the California Consumer Privacy Act (CCPA), which is valid in the United States' State of California [18]. It has been noted that the CCPA imposes strict regulations on companies managing personal data, necessitating transparency in data collection, selling, and sharing practices by MaaS providers. This has prompted significant operational changes among MaaS providers, as exemplified by a major California-based provider that had to modify its data-handling practices to align with CCPA compliance. Researchers have also considered the Personal Information Protection and Electronic Documents Act (PIPEDA) of Canada and the Personal Data Protection Act (PDPA) of Singapore to manage the privacy of personal data processed using MaaS systems [18]. The CCPA was also addressed in a study by Ekpo et al., which highlighted that service providers may process personal data without a valid legal basis or violate data rights—such as the CCPA's "Do Not Sell My Data" provision—thereby potentially breaching local data protection laws [62].

Finally, Bill 25 is another regulation considered by Garroussi et al. as a regulation to govern MaaS systems [18]. It was noted that in Quebec, the Access-to-Information Commission issued a reminder in September 2021 regarding the implementation of provisions from Bill 25. This reform was reported to modernize provisions related to the protection of personal information in the private sector, promising enhanced protection of personal information, new rights for citizens, and more responsible and transparent management of personal information [18].

In another study focusing on the development of MaaS in Finland and Sweden, Mukhtar-Landgren and Smith considered the Finnish Personal Data Act [100]. They

identified MaaS operators, referred to as controllers, as responsible for complying with this regulation when sharing the data of MaaS customers [36].

Moreover, there are few studies that discuss general recommendations for strengthening policy and regulatory frameworks for MaaS. Wu et al. [79] suggested that in order to clarify the responsibilities of each MaaS stakeholder and build a framework for data sharing and privacy protection to support MaaS operations, governments and transport-planning authorities should work with researchers to develop relevant laws, policies, and regulations.

Implications of Privacy Laws and Regulations for MaaS Service Providers

Reviewing the literature in their survey study, Garroussi et al. reported several adjustments for MaaS service providers for their data-handling procedures [18]. Implementing systems to collect and manage users' consent, creating tools for data minimization, and enhancing data security architecture were some of the practices highlighted by the researchers. Furthermore, restrictions required by privacy laws and regulations were argued to have a substantial impact on the business models adopted by MaaS providers. It was noted that regulations regarding data collection and utilization compel providers to reassess their approaches to data-driven monetization. Considering the severe consequences stipulated by laws such as the GDPR, Bill C-27 in Canada, and L25 in Quebec for non-compliance, researchers have stated that business models must strike a delicate balance between the necessity of utilizing data for service improvement and the imperative to uphold user privacy [18]. Their study also delved into how these laws influence the interactions between MaaS companies and their customers. Emphasizing the transparency principle within privacy regulations, their study suggested that MaaS providers should portray themselves as responsible custodians of user data, thereby fostering stronger consumer relations [18].

In addition to the potential advantages, considerable challenges introduced by adhering to these laws were also covered in their study. It was underlined that the regulations frequently vary across jurisdictions, necessitating providers operating in multiple regions to navigate an intricate and diverse privacy regulatory landscape. Furthermore, because these laws undergo changes over time, it was added that sustaining compliance becomes an ongoing challenge that demands continuous vigilance and adaptability [18].

Ekpo et al. [62] also highlighted the potential risk of violating the data minimization principle, noting that certain services may require users to disclose excessive personal information, thereby increasing their vulnerability and the potential impacts of data breaches. In addition to data minimization, their study addressed several other key aspects of the GDPR. These include the unlawful processing of personal data by service providers, the use of invalid or inadequately understood consent mechanisms, data collection without a lawful basis, and violations of the storage limitation principle—where personal data are retained longer than necessary, heightening the risk associated with potential data breaches.

Another set of issues was identified by Araghi et al. [37,87,88], related to the implications of privacy regulations for MaaS service providers. Araghi et al. questioned to what extent the market should be left to evolve freely [37]. Underhill and Knowles argued that the participation of governments in developing regulations was important, as under-involvement from governments could lead to (1) failures in regulating the storage and monetization of data by the private sector and (2) insufficiently robust security and privacy [87]. However, the risk of over-involvement was also covered in their study where excessive regulation was argued to disincentivize private companies from entering the MaaS space. A potential increase in the way MaaS service providers care for data security and privacy was also noted in the same study. Following Underhill and Knowles's

work [87], Knowles et al. also argued that over-involvement of governments may result in excessive regulation, limited industry participation, and hindered innovation [88].

3.4.2. Organizational Policies

Although not extensively covered, certain studies in the MaaS literature have underscored the necessity for establishing a robust policy framework for data security and privacy within the MaaS environment. For instance, in their analysis of the MaaS business ecosystem, Kamargianni et al. highlighted that the MaaS ecosystem has several layers, or actors, including transport operators, data providers, technology providers, infrastructure, regulatory bodies, and research institutions [93]. Their study specifically identified the data providers within the correspondence layer as a pivotal actor, emphasizing the importance of a regulatory framework that meets the requisite policy and security standards for data warehouses. Recommending the application of advanced encryption processes as a part of a policy framework, their study advocated for a central policy, both at the national and international levels, to facilitate MaaS in achieving data interoperability. Additionally, the need for policy formulation concerning the secure usage of open data was highlighted. This aligns with findings from a recent study conducted by Nikitas et al., which noted that because of privacy concerns, open-data policies present both legal and ethical challenges for the implementation of MaaS systems [98]. The policymakers and regulation authorities were positioned as another actor within the outer layer of the proposed ecosystem, and it was added that governments needed to have clear and uncontested policies that take care of passengers' rights, privacy, and cyber security concerns of the stakeholders, market competitions, and other issues related to MaaS. Another study that handled the policy framework for data security and privacy within the MaaS environment also emphasized the need for enhancing the effective communication of data privacy policies and information [95].

In their study, Hlubi and Seftel analyzed the "MaaS reference architecture" to assess its suitability for implementation in South Africa [94]. During this examination, they identified the absence of any relevant national policy or legislation that could support the MaaS facilitation. However, their study indicated that the related governmental departments are actively working on having legislation in effect. The researchers underscored the importance of this legislation aligning with a transport policy framework that promotes open data format and convenient payment methods. Recognizing an appropriate legislative framework as a key facilitator for MaaS adoption, they suggested that it would make a fair ground for competition and cater to many concerns, including the rights of travelers and privacy and security issues [94].

Another interesting finding of our review, regarding organizational policies, can be given as the lack of discussion in the literature proposing a dedicated practical approach to assess MaaS services and indicators that could be used to assess data privacy or evaluate consumers' feedback in this area. In only one study, Gompf et al. referred to the UNEP/SETAC Guidelines and Product Social Impact Assessment (PSIA) to be utilized for this purpose [96]. According to the UNEP/SETAC Guidelines, "a social and socioeconomic Life Cycle Assessment (S-LCA) is a social impact (and a potential impact) assessment technique that aims to assess the social and socioeconomic aspects of products and their potential positive and negative impacts along their life cycle" [101]. These guidelines provide a framework on how S-LCA should be conducted, identifying impact categories and indicators for those categories. The guidelines also refer to data privacy, including the number of consumer complaints or complaints by regulatory bodies related to privacy as a quantitative indicator. Among those indicators, Gompf et al. suggested several indicators focusing on country rankings or the strength of the policies regarding privacy to be used in the context of MaaS [96].

From the perspective of governance, Mohammed et al. conducted a study of inviting key transport stakeholders in Qatar to partake in a workshop, aiming to identify key factors for establishing successful governance to implement and operate MaaS [97]. The findings indicated that data sharing and privacy are two elements that need to be further studied. In addition, Mohammed et al. specifically highlighted the impact of data sharing on MaaS governance, where at least three data-sharing strategies, including limited data sharing, data openness, and restricted data sharing, were discussed.

Much like the UNEP/SETAC guidelines, PSIA [102] helps to assess the positive and negative social impacts of products and services on four stakeholder groups: workers, local communities, small-scale entrepreneurs, and users. It offers a practical method for pinpointing social aspects relevant to those stakeholder groups, along with corresponding performance indicators. These indicators, identified by Gompf et al. as being suitable for assessing data privacy in mobility services [96], include:

- The company has a policy to protect users' data privacy;
- The company shares or sells sensitive private data without users' consent or transparency;
- The company uses and processes sensitive private data without users' consent or users' access to the data's content and purposes;
- The company's use of private data complies with local laws;
- If no regulation exists, the company does not collect, process, share, store, resell, or use sensitive data;
- The company has a PDCA process in place to exceed the minimum legal standard;
- The company has established a grievance mechanism.

4. Further Discussion

In this section, we outline and discuss our primary findings concerning our research questions, alongside acknowledging the limitations of previous research and identifying research gaps in the literature.

4.1. Cyber Security and Privacy Risks Associated with the Use of MaaS Systems and Solutions Proposed to Address Them (RQ1 and RQ3)

Our study highlighted the prominent theme of risks regarding cyber security and privacy in the context of MaaS. Regarding cyber security risks, our SLR identified both technical and non-technical risks raised by the MaaS researchers. DoS attacks were the most frequently discussed technical risks in the literature, whereas the illegal use of personal data by MaaS operators was the most common non-technical risk. In terms of privacy risks, two key themes emerged: profiling and inference, as well as third-party access and data sharing. The subtheme of profiling and inference encompasses discussions on how personal data collected by MaaS systems can be utilized to profile individuals and infer their behaviors. On the other hand, the second subtheme addresses the privacy risks associated with third-party access to personal data collected by MaaS providers and the sharing of such data among multiple entities.

Another theme that emerged in our review is the identification of potential solutions and guidance to mitigate these risks. Blockchain technology emerged as a significant suggestion in the literature for developing countermeasures against various threats. However, alternative non-blockchain approaches, such as cryptography, digital twins, or mobile/multi-access edge computing, were also discussed as feasible options.

In the context of cyber security and privacy risks for MaaS systems, our SLR uncovered a gap in the literature. The identified studies tended to concentrate on limited facets of the MaaS landscape, resulting in fragmented insights. As summarized above, the current body of work about privacy risks and concerns predominantly revolves around the handling

of data within MaaS systems. This focus is notably directed toward two primary aspects: (1) the risks associated with profiling and inferring insights from the collected personal data and (2) the concerns and risks related to third-party access to the amassed personal data. Given the amount of data MaaS can collect and process and the multitude of parties that might be involved in such a process, we envisage that the privacy concerns and risks of MaaS could occur at different phases, including the data generation phase, data storage phase, and data-processing and data-sharing phases. Yet, existing work has failed to address this in a systematic way to provide a more in-depth and comprehensive understanding of its full scale.

Moreover, cyber security and privacy have often been intertwined and jointly discussed together in the literature. However, distinctions exist between them. Privacy is about the use and governance of individual data to ensure that the data are collected, used, and shared in appropriate ways, whereas cyber security is more about protecting and preventing data from malicious attacks and misuse (in its narrow sense) [103], suggesting that cyber security is fundamental for protecting data but might not be sufficient for ensuring privacy [104]. Taking MaaS's heterogeneity into consideration, there is a need to have an in-depth discussion on the relationship between the cyber security and privacy of MaaS systems.

Furthermore, MaaS is a complex system of different systems, where different stakeholders of MaaS have a hierarchy of needs in which optimized travel options remain crucial [105]. It is an emerging challenge to learn the holistic landscape of MaaS. A number of attempts have been made in the literature, utilizing ontology, typology, and taxonomy-based methodologies [7,105–107]. However, to the best of our knowledge, no previous work has been conducted solely from the perspectives of cyber security and privacy, which could potentially help to provide guidance and elicit cyber security and privacy requirements designed for MaaS systems, as well as help to systematically address related risks and concerns.

In brief, our study encourages more research in the following areas:

- Systematically investigating the scale and landscape of cyber security and privacy risks of MaaS systems;
- Further clarifying the relationship between cyber security and privacy in the context of MaaS;
- Establishing a more comprehensive understanding of the technical requirements for mitigating cyber security and privacy risks of MaaS systems.

4.2. Cyber Security and Privacy Concerns That Users Have Regarding the Use of MaaS Systems (RQ2)

Regarding the low number of past studies that have looked at the impacts of the cyber security and/or privacy concerns on end users' willingness to adopt MaaS systems, there is no conclusive agreement on their effects on people's intention to adopt MaaS. The fragmented depiction of users' cyber security and privacy concerns makes it difficult to reach solid conclusions regarding their impacts on MaaS acceptance and adoption. Additionally, considering that most researchers in this area do not primarily belong to the cyber security domain, the relatively narrow scope is somewhat expected. Cyber security researchers often focus on providing solutions for cyber security threats (as summarized in Section 3.2.3) without delving into the broader impacts of users' cyber security or privacy concerns impacting MaaS adoption, which is an area where we call for more research. This lack of disciplinary convergence may also explain why findings are inconsistent—some studies find privacy concerns to be a significant barrier to adoption, while others report little to no effect. These discrepancies may be because of differences in research focus,

methodologies, regional users' perceptions, or how privacy concerns are framed, further highlighting the need for more nuanced, interdisciplinary investigations.

Additionally, our SLR uncovered a significant gap in the literature concerning the awareness of MaaS end users. Our study highlights the disparities between the risks identified by MaaS researchers and those perceived by end users. For example, although third-party sharing is frequently discussed as a privacy risk by MaaS researchers, it was reported as a concern by MaaS users in only one study. Similarly, profiling was not mentioned as a concern by any participants in the reviewed studies. We speculate that the lack of awareness among MaaS users regarding data privacy could contribute to these findings. However, there is currently no dedicated study aimed at assessing or improving awareness among MaaS users, underscoring the need for further exploration in this area. This disconnect between expert-identified risks and users' perceptions may partly explain the conflicting findings in the literature regarding the role of privacy concerns in MaaS adoption. Without a clear understanding of what users actually know or worry about, it becomes difficult to interpret the extent to which privacy concerns influence adoption behavior across different studies.

Herein, we have identified the following research areas to be considered in future studies:

- Systematically defining and comparing cyber security and privacy concerns from different stakeholders' perspectives;
- Conducting privacy awareness studies among MaaS users to assess and improve their awareness;
- Investigating the impacts of cyber security and privacy concerns on MaaS adoption in a more comprehensive and nuanced approach, considering both technical and user-related aspects.

4.3. Legal Issues Regarding the Privacy of Personal Data Processed Using MaaS Systems (RQ4)

The past research primarily refers to the GDPR as a prominent regulatory framework to govern MaaS systems. Recognizing MaaS service providers as data controllers under the GDPR, several GDPR elements are discussed in the literature within the MaaS context, including data minimization, consent management, transparency, privacy by design, encryption, anonymization, and data protection impact assessments. Some have also argued that data processed using MaaS systems can easily transition to sensitive data, which are recognized as special category data under the GDPR, warranting a higher level of protection.

It is important to note that discussions on the GDPR within the context of MaaS primarily stem from the perspective of service providers, highlighting their obligations under the GDPR. However, there is a gap in the literature concerning the users' viewpoints and their rights granted by the GDPR. For instance, the "right to be informed", which grants data subjects (in this case, MaaS users) the right to be informed about the collection and use of their personal data, has not been addressed in any past studies our SLR covers. Similarly, the "right to access", which allows individuals to obtain a copy of their personal data from service providers, and the "right to be forgotten", enabling users to request the deletion of their data, have also been overlooked. We specifically highlight these rights because executing them in MaaS systems poses challenges because of the multiple stakeholders involved in data processing. Despite this, none of the studies has identified them as risks or concerns that users have.

Aligned with this observation, studies regarding a comprehensive data privacy policy exclusively tailored and implemented for MaaS operations appear to be lacking in the literature. Conducting further research in this area could significantly benefit the MaaS industry, providing much-needed guidance for service providers in formulating their

privacy protocols. Additionally, the absence of studies dedicated to proposing indicators for assessing these privacy practices is also notable. However, it is worth considering that the indicators recommended by Gompf et al. could be customized for this purpose, as they offer a solid foundation despite initially being intended for general applications [96].

It is also evident that none of the studies has established clear sharing policies that foster innovation while simultaneously ensuring the security of both service providers and users. Sharing data is not only inevitable for MaaS systems to work but also extremely useful both for users and for MaaS providers, as it allows them to improve the latter's services [38].

Therefore, after conducting a comprehensive analysis, our study encourages more research in the following areas:

- Systematically examining the GDPR compatibility of MaaS systems, considering all the elements of the GDPR, with a particular focus on data subjects' rights;
- Exploring the components essential for an organizational policy dedicated to addressing cyber security and privacy issues specific to MaaS;
- Researching sharing policies that encourage innovation while also ensuring the security of service providers and users;
- Researching indicators to be used to assess data privacy practices of MaaS service providers.

4.4. Limitations

Although our study thoroughly identified research on cyber security and privacy risks in MaaS, certain limitations exist. First of all, our review focused on research papers published from 2017 to April 2025, aligned with the surge of interest in MaaS, which followed the Whim app trial. Although we consider this as a valid criterion, earlier foundational work or very recent emerging studies may have been excluded because of this date restriction. Second, searching only titles with Google Scholar, because of its vast data and low hit rate for full-text searches, may have caused some relevant studies to be omitted. However, we mitigated this by also searching with Scopus, known for its comprehensive research coverage and support for searches of metadata. Therefore, we believe that our included papers represent past research well. Additionally, using MaaS-related keywords might have missed papers using terms like "transport" or specific transport modes (e.g., "bike sharing" or "ride hailing"). Despite this, the high volume of reviewed articles provides a strong representation of past research. Finally, we acknowledge that language and publication bias may also affect our findings, as our review focused only on peer-reviewed academic publications written in English. This may have excluded relevant work published in other languages or in the gray literature, which could offer additional perspectives on users' concerns and implementation challenges. Future reviews could expand the scope to include these dimensions.

5. Conclusions

In this study, we have undertaken a comprehensive examination of the cyber security and privacy issues intrinsic to Mobility-as-a-Service (MaaS) through a systematic literature review of 87 relevant research papers published between 2017 and April 2025. Our analysis has illuminated three primary themes prevalent in the current literature: the identification and mitigation of inherent cyber security and privacy risks in MaaS systems, the impacts of users' concerns on the adoption of MaaS, and the regulatory landscape governing these emerging transport solutions. To support actionable insights, we present a summary table highlighting the key takeaways and tailored recommendations for policymakers, developers, and researchers. (See Table 8).

Table 8. Summary of the key takeaways and recommendations for stakeholders.

Stakeholder Group	Key Takeaways	Recommendations
Policymakers	- Lack of standardized data-sharing protocols and legal frameworks - Inconsistent enforcement of data protection laws, like the GDPR	- Develop harmonized international policies and data governance models - Mandate privacy-by-design in MaaS platforms
Developers/Providers	- Privacy risks include profiling, inference attacks, and third-party data sharing - Security vulnerabilities include DoS, spoofing, and insider threats	- Implement privacy-preserving technologies (e.g., federated learning, anonymization, and encryption) - Use secure architecture standards and blockchain smart contracts for transparency
Researchers	- Limited cross-disciplinary analysis on legal, behavioral, and technical risks - Gaps between users' concerns and proposed solutions	- Focus future research on user-centric security design - Conduct longitudinal studies on risk perceptions and adoption behaviors

Our findings underscore the critical importance of addressing cyber security and privacy challenges to ensure the successful implementation and widespread acceptance of MaaS. By systematically categorizing the identified risks and evaluating the proposed solutions, we provide a clear framework that can guide MaaS service providers in enhancing their security protocols. Furthermore, understanding users' concerns and their influences on adoption highlights the need for transparent communication and robust data protection measures to build and maintain users' trust.

Additionally, our investigation into existing laws and policies reveals significant gaps and inconsistencies that need to be addressed. This underscores the necessity for policymakers and legislators to develop comprehensive regulatory frameworks that can keep pace with the rapid advancements in MaaS technologies and practices. Such regulations should aim to protect user privacy, ensure data security, and foster an environment conducive to innovation and growth in the MaaS sector.

In conclusion, our SLR led to valuable insights into the critical areas of cyber security and privacy within MaaS, offering guidance for service providers, users, and policymakers alike. By addressing these concerns, we can pave the way for a more secure, user-friendly, and sustainable future in urban mobility, thereby realizing the full potential of MaaS in transforming transport.

Author Contributions: Conceptualization, R.B.-S. and S.L.; methodology, R.B.-S.; validation, H.Y., M.S.H., R.A. and S.L.; formal analysis, R.B.-S.; investigation, R.B.-S.; resources, R.B.-S., H.Y., M.S.H. and R.A.; data curation, R.B.-S., H.Y., M.S.H. and R.A.; writing—original draft preparation, R.B.-S.; writing—review and editing, R.B.-S., H.Y., M.S.H., R.A. and S.L.; visualization, R.B.-S.; supervision, S.L.; project administration, R.B.-S. and S.L.; funding acquisition, S.L. All authors have read and agreed to the published version of the manuscript.

Funding: This research was partly supported by the research project "Mobility as a Service: Managing Cyber Security Risks Across Consumers, Organizations, and Sectors (MACRO)", funded by the Engineering and Physical Sciences Research Council (EPSRC), a part of UK Research and Innovation (UKRI) under the reference number EP/V039164/1.

Data Availability Statement: No new data were created or analyzed in this study. Data sharing is not applicable to this article.

Acknowledgments: The authors would like to thank the other members of the MACRO project, particularly Nazmiye Balta-Ozkan, Ali Alderete Peralta, Weisi Guo (Cranfield University), and Kai-Fung Chu (University of Cambridge), for their feedback on the work reported at multiple project meetings.

Conflicts of Interest: The authors declare no conflicts of interest. The funders had no role in the design of the study; in the collection, analyses, or interpretation of the data; in the writing of the manuscript; or in the decision to publish the results.

Abbreviations

The following abbreviations are used in this manuscript:

MaaS	Mobility as a Service
SLR	Systematic Literature Review
ICT	Information and Communication Technology
GDPR	General Data Protection and Regulation

References

1. Newman, P.W.; Kenworthy, J.R. The land use—Transport connection: An overview. *Land Use Policy* **1996**, *13*, 1–22. [CrossRef]
2. Butler, L.; Yigitcanlar, T.; Paz, A. Barriers and risks of Mobility-as-a-Service (MaaS) adoption in cities: A systematic review of the literature. *Cities* **2021**, *109*, 103036 . [CrossRef]
3. Hietanen, S. Mobility as a Service. *New Transp. Model* **2014**, *12*, 2–4.
4. Goodall, W.; Dovey, T.; Bornstein, J.; Bonthron, B. The rise of mobility as a service. *Deloitte Rev.* **2017**, *20*, 112–129.
5. Pagoni, I.; Gatto, M.; Tsouros, I.; Tsirimpa, A.; Polydoropoulou, A.; Galli, G.; Stefanelli, T. Mobility-as-a-service: Insights to policymakers and prospective MaaS operators. *Transp. Lett.* **2022**, *14*, 356–364. [CrossRef]
6. Audouin, M.; Finger, M. The development of Mobility-as-a-Service in the Helsinki metropolitan area: A multi-level governance analysis. *Res. Transp. Bus. Manag.* **2018**, *27*, 24–35. [CrossRef]
7. Sochor, J.; Arby, H.; Karlsson, I.M.; Sarasini, S. A topological approach to Mobility as a Service: A proposed tool for understanding requirements and effects, and for aiding the integration of societal goals. *Res. Transp. Bus. Manag.* **2018**, *27*, 3–14. [CrossRef]
8. Pham, H.D.; Shimizu, T.; Nguyen, T.V. A Literature Review on Interactions Between Stakeholders Through Accessibility Indicators Under Mobility as a Service Context. *Int. J. Intell. Transp. Syst. Res.* **2021**, *19*, 468–476. [CrossRef]
9. Arias-Molinares, D.; García-Palomares, J.C. The Ws of MaaS: Understanding mobility as a service from a literature review. *J. Int. Assoc. Traffic Saf. Sci. (IATSS)* **2020**, *44*, 253–263. [CrossRef]
10. Jittrapirom, P.; Marchau, V.; van der Heijden, R.; Meurs, H. Dynamic adaptive policymaking for implementing Mobility-as-a Service (MaaS). *Res. Transp. Bus. Manag.* **2018**, *27*, 46–55. [CrossRef]
11. Mulley, C.; Kronsell, A. Workshop 7 report: The "uberisation" of public transport and mobility as a service (MaaS): Implications for future mainstream public transport. *Res. Transp. Econ.* **2018**, *69*, 568–572. [CrossRef]
12. Kayikci, Y.; Kabadurmus, O. Barriers to the adoption of the mobility-as-a-service concept: The case of Istanbul, a large emerging metropolis. *Transp. Policy* **2022**, *129*, 219–236. [CrossRef]
13. Gebhart, J.; Schlick, S.; Marvell, A. Analysing Barriers in the Business Ecosystem of European MaaS Providers: An Actor-Network Approach. *EPiC Ser. Comput.* **2023**, *93*, 68–81. [CrossRef]
14. Maas, B. Literature Review of Mobility as a Service. *Sustainability* **2022**, *14*, 8962. [CrossRef]
15. Zhang, Y.; Kamargianni, M. A review on the factors influencing the adoption of new mobility technologies and services: Autonomous vehicle, drone, micromobility and mobility as a service. *Transp. Rev.* **2023**, *43*, 407–429. [CrossRef]
16. Natvig, M.K.; Stav, E.; Vennesland, A. Systematic mapping of scientific publications on maas. *Manag. Rev. Q.* **2025**, *75*, 83–118. [CrossRef]
17. Anthony, B.; Sarshar, S. Enhancing data sovereignty to improve intelligent mobility services in smart cities. *Urban Gov.* **2025**, *5*, 20–31. [CrossRef]
18. Garroussi, Z.; Legrain, A.; Gambs, S.; Gautrais, V.; Sansò, B. Data privacy for Mobility as a Service. *arXiv* **2023**. [CrossRef]
19. Garroussi, Z.; Legrain, A.; Gambs, S.; Gautrais, V.; Sansò, B. A systematic review of data privacy in Mobility as a Service (MaaS). *Transp. Res. Interdiscip. Perspect.* **2025**, *31*, 101254. [CrossRef]
20. Ekpo, O.; Casola, V.; De Benedictis, A. Security and Privacy Issues in Mobility-as-a-Service (MaaS): A Systematic Review. In Proceedings of the 2024 19th Annual System of Systems Engineering Conference (SoSE), Tacoma, WA, USA, 23–26 June 2024 ; pp. 300–307.
21. Kaur, H.; Pannu, H.S.; Malhi, A.K. A Systematic Review on Imbalanced Data Challenges in Machine Learning: Applications and Solutions. *ACM Comput. Surv.* **2019**, *52*, 1–36. [CrossRef]
22. Page, M.J.; McKenzie, J.E.; Bossuyt, P.M.; Boutron, I.; Hoffmann, T.C.; Mulrow, C.D.; Shamseer, L.; Tetzlaff, J.M.; Akl, E.A.; Brennan, S.E.; et al. The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. *Syst. Rev.* **2021**, *10*, 1–11. [CrossRef] [PubMed]

23. Bar-Ilan, J. Tale of three databases: The implication of coverage demonstrated for a sample query. *Front. Res. Metrics Anal.* **2018**, *3*, 6. [CrossRef]
24. Haddaway, N.R.; Collins, A.M.; Coughlin, D.; Kirk, S. The Role of Google Scholar in Evidence Reviews and its Applicability to Grey Literature Searching. *PLoS ONE* **2015**, *10*, e0138237. [CrossRef]
25. Yasin, A.; Fatima, R.; Wen, L.; Afzal, W.; Azhar, M.; Torkar, R. On Using Grey Literature and Google Scholar in Systematic Literature Reviews in Software Engineering. *IEEE Access* **2020**, *8*, 36226–36243. [CrossRef]
26. Cottrill, C.D. MaaS surveillance: Privacy considerations in mobility as a service. *Transp. Res. Part A Policy Pract.* **2020**, *131*, 50–57. [CrossRef]
27. Barreto, L.; Amaral, A.; Baltazar, S. Urban Mobility Digitalization: Towards Mobility as a Service (MaaS). In Proceedings of the 2018 International Conference on Intelligent Systems, Madeira, Portugal, 25–27 September 2018; pp. 850–855. [CrossRef]
28. Costantini, F.; Archetti, E.; Di Ciommo, F.; Ferencz, B. IoT, Intelligent Transport Systems and MaaS (Mobility as a Service). Jusletter IT 21. 2019. Available online: https://cambiamo.net/wp-content/uploads/2019/07/Costantini-et-al.-2019-IoT-intelligent-transport-systems-and-MaaS-mobility-as-a-service.pdf (accessed on 5 June 2025).
29. Cooper, P.; Tryfonas, T.; Crick, T.; Marsh, A. Electric vehicle mobility-as-a-service: Exploring the "Tri-Opt" of novel private transport business models. *J. Urban Technol.* **2019**, *26*, 35–56. [CrossRef]
30. Kong, Q.; Lu, R.; Yin, F.; Cui, S. Blockchain-based Privacy-preserving Driver Monitoring for MaaS in the Vehicular IoT. *IEEE Trans. Veh. Technol.* **2021**, *70*, 3788–3799. [CrossRef]
31. Belletti, F.; Bayen, A.M. Privacy-preserving MaaS fleet management. *Transp. Res. Procedia* **2017**, *23*, 1000–1024. [CrossRef]
32. Callegati, F.; Giallorenzo, S.; Melis, A.; Prandini, M. Cloud-of-Things meets Mobility-as-a-Service: An insider threat perspective. *Comput. Secur.* **2018**, *74*, 277–295. [CrossRef]
33. Pitera, K.; Marinelli, G. *Autonomous E-Mobility as a Service-Final Report*; Technical Report Report 3/2017 NTNU IBM; NTNU: Trondheim, Norway, 2017 .
34. He, B.Y.; Chow, J.Y.J. Gravity Model of Passenger and Mobility Fleet Origin–Destination Patterns with Partially Observed Service Data. *Transp. Res. Rec.* **2021**, *2675*, 235–253. [CrossRef]
35. Merkert, R.; Bushell, J.; Beck, M.J. Collaboration as a service (CaaS) to fully integrate public transportation–Lessons from long distance travel to reimagine mobility as a service. *Transp. Res. Part A Policy Pract.* **2020**, *131*, 267–282. [CrossRef]
36. Mukhtar-Landgren, D.; Smith, G. Perceived action spaces for public actors in the development of Mobility as a Service. *Eur. Transp. Res. Rev.* **2019**, *11*, 32. [CrossRef]
37. Araghi, Y.; Larco, N.; Bouma, G.; Doll, C.; Vonk Noordegraaf, D.; Krauß, K. Drivers and Barriers of Mobility-as-a-Service in urban areas. In Proceedings of the 8th Transport Research Arena Conference (TRA) 2020, Helsinki, Finland, 27–30 April 2020. [CrossRef]
38. Zhang, Z.; Zhang, N. A Novel Development Scheme of Mobility as a Service: Can It Provide a Sustainable Environment for China? *Sustainability* **2021**, *13*, 4233. [CrossRef]
39. Utriainen, R.; Pöllänen, M. Review on mobility as a service in scientific publications. *Res. Transp. Bus. Manag.* **2018**, *27*, 15–23. [CrossRef]
40. Thai, J.; Yuan, C.; Bayen, A.M. Resiliency of Mobility-as-a-Service Systems to Denial-of-Service attacks. *IEEE Trans. Control Netw. Syst.* **2018**, *5*, 370–382. [CrossRef]
41. Vaidya, B.; Mouftah, H.T. Security for Shared Electric and Automated Mobility Services in Smart Cities. *IEEE Secur. Priv.* **2020**, *19*, 24–33. [CrossRef]
42. Callegati, F.; Delnevo, G.; Melis, A.; Mirri, S.; Prandini, M.; Salomoni, P. I want to ride my bicycle: A microservice-based use case for a MaaS architecture. In Proceedings of the 2017 IEEE Symposium on Computers and Communications, Heraklion, Greece, 3–6 July 2017; pp. 18–22. [CrossRef]
43. Callegati, F.; Giallorenzo, S.; Melis, A.; Prandini, M. Insider Threats in Emerging Mobility-as-a-Service Scenarios. In Proceedings of the 50th Hawaii International Conference on System Science, Waikoloa, HI, USA, 4–7 January 2017; University of Hawaii: Manoa, HI, USA , 2017.
44. Mouhibbi, L.; Elhozmari, M.; Ettalbi, A. Sorting and persisting REST and SOAP client for MaaS based architecture. In Proceedings of the 2018 6th International Conference on Multimedia Computing and Systems, Rabat, Morocco, 10–12 May 2018. [CrossRef]
45. Carvalho, G.; Cabral, B.; Pereira, V.; Bernardino, J. A Case for Machine Learning in Edge-Oriented Computing to Enhance Mobility as a Service. In Proceedings of the 2019 15th International Conference on Distributed Computing in Sensor Systems, Santorini Island, Greece, 29–31 May 2019; pp. 530–537. [CrossRef]
46. Cruz, C.O.; Sarmento, J.M. "Mobility as a service" Platforms: A Critical Path towards Increasing the Sustainability of Transportation Systems. *Sustainability* **2020**, *12*, 6368. [CrossRef]
47. Alyavina, E.; Nikitas, A.; Njoya, E.T. Mobility as a service and sustainable travel behaviour: A thematic analysis study. *Transp. Res. Part F Traffic Psychol. Behav.* **2020**, *73*, 362–381. [CrossRef]
48. Nguyen, T.H.; Partala, J.; Pirttikangas, S. Blockchain-Based Mobility-as-a-Service. In Proceedings of the 2019 28th International Conference on Computer Communication and Networks, Valencia, Spain, 29 July–1 August 2019. [CrossRef]

49. Chinaei, M.H.; Hossein Rashidi, T.; Waller, T. Digitally transferable ownership of mobility-as-a-service systems using blockchain and smart contracts. *Transp. Lett.* **2022**, *20*, 54–61. [CrossRef]
50. Bothos, E.; Magoutas, B.; Arnaoutaki, K.; Mentzas, G. Leveraging Blockchain for Open Mobility-as-a-Service Ecosystems. In Proceedings of the 2019 IEEE/WIC/ACM International Conference on Web Intelligence—Companion Volume, Thessaloniki, Greece, 14–17 October 2019; pp. 292–296. [CrossRef]
51. Casady, C.B. Customer-led mobility: A research agenda for Mobility-as-a-Service (MaaS) enablement. *Case Stud. Transp. Policy* **2020**, *8*, 1451–1457. [CrossRef]
52. Kulla, E.; Barolli, L.; Matsuo, K.; Ikeda, M. Blockchain Applications for Mobility-as-a-Service Ecosystem: A Survey. In Proceedings of the Advances in Internet, Data & Web Technologies: The 11th International Conference on Emerging Internet, Data & Web Technologies (EIDWT-2023), Semarang, Indonesia, 23–25 February 2023; Springer: Berlin/Heidelberg, Germany, 2023; pp. 129–140. [CrossRef]
53. Campolo, C.; Cuzzocrea, D.; Genovese, G.; Iera, A.; Molinaro, A. An OMA Lightweight M2M-compliant MEC Framework to Track Multi-modal Commuters for MaaS Applications. In Proceedings of the 2019 IEEE/ACM 23rd International Symposium on Distributed Simulation and Real Time Applications, Cosenza, Italy, 7–9 October 2019. [CrossRef]
54. Katsaros, K.V.; Amditis, A.J.; Trichias, K.; Shagdar, O.; Soua, A.; Requena, J.C.; Santa, J.; Kakes, G.; Almeida, J.; Sousa, E.; et al. Connected and Automated Mobility Services in 5G Cross-Border Environments: Challenges and Prospects. *IEEE Intell. Transp. Syst. Mag.* **2023**, *15*, 145–157. [CrossRef]
55. Campolo, C.; Genovese, G.; Molinaro, A.; Pizzimenti, B. Digital Twins at the Edge to Track Mobility for MaaS Applications. In Proceedings of the 2020 IEEE/ACM 24th International Symposium on Distributed Simulation and Real Time Applications, Prague, Czech Republic, 14–16 September 2020. [CrossRef]
56. Christiaanse, R. Mobility as a Service. In Proceedings of the Companion Proceedings of the 2019 World Wide Web Conference, San Francisco, CA, USA, 13–17 May 2019; pp. 83–92. [CrossRef]
57. Polydoropoulou, A.; Pagoni, I.; Tsirimpa, A. Ready for Mobility as a Service? Insights from stakeholders and end-users. *Travel Behav. Soc.* **2020**, *21*, 295–306. [CrossRef]
58. Callegati, F.; Gabbrielli, M.; Giallorenzo, S.; Melis, A.; Prandini, M. Smart mobility for all: A global federated market for mobility-as-a-service operators. In Proceedings of the 2017 IEEE 20th International Conference on Intelligent Transportation Systems, Yokohama, Japan, 16–19 October 2017. [CrossRef]
59. Breuer, D.; Spichartz, P.; Sourkounis, C. Concept of interlinking mobility services for urban transport towards intermodal mobility including private and shared electromobility. In Proceedings of the 2019 14th International Conference on Ecological Vehicles and Renewable Energies, Monte-Carlo, Monaco, 8–10 May 2019. [CrossRef]
60. Hoess, A.; Lautenschlager, J.; Sedlmeir, J.; Fridgen, G.; Schlatt, V.; Urbach, N. Toward seamless mobility-as-a-service: Providing multimodal mobility through digital wallets. *Bus. Inf. Syst. Eng.* **2024**, *67*, 149–170. [CrossRef]
61. Miron, R.; Hulea, M.; Muresan, V.; Clitan, I.; Rusu, A. Integrating Blockchain Technology into Mobility-as-a-Service Platforms for Smart Cities. *Smart Cities* **2025**, *8*, 9. [CrossRef]
62. Ekpo, O.; Casola, V.; De Benedictis, A. Towards a Privacy Resilient Mobility-as-a-Service (MaaS): A Threat-driven Approach. In Proceedings of the 2024 International Conference on Smart Systems and Technologies (SST), Osijek, Croatia, 16–18 October 2024; pp. 271–224.
63. Chu, K.F.; Yuan, H.; Yuan, J.; Guo, W.; Balta-Ozkan, N.; Li, S. A Survey of Artificial Intelligence-Related Cybersecurity Risks and Countermeasures in Mobility-as-a-Service. *IEEE Intell. Transp. Syst. Mag.* **2024**, *16*, 37–55. [CrossRef]
64. Oberoi, K.S. Personalisation in Mobility-as-a-Service: Where We Are and How to Move Forward. In Proceedings of the 10th International Conference on Vehicle Technology and Intelligent Transport Systems (VEHITS 2024), Angers, France, 2–4 May 2024; pp. 352–360.
65. Peralta, A.A.; Balta-Ozkan, N.; Li, S. The road not taken yet: A review of cyber security risks in mobility-as-a-service (MaaS) ecosystems and a research agenda. *Res. Transp. Bus. Manag.* **2024**, *56*, 101162.
66. Chu, K.F.; Guo, W. Multi-agent reinforcement learning-based passenger spoofing attack on mobility-as-a-service. *IEEE Trans. Dependable Secur. Comput.* **2024**, *21*, 5565–5581. [CrossRef]
67. Kummetha, V.C.; Concas, S.; Staes, L.; Godfrey, J. Mobility on demand in the United States–Current state of integration and policy considerations for improved interoperability. *Travel Behav. Soc.* **2024**, *37*, 100867. [CrossRef]
68. Schwinger, F.; Krempels, K.H. Mobility-oriented Agenda Planning as a Value-adding Feature for Mobility as a Service. In Proceedings of the 11th International Conference on Agents and Artificial Intelligence, Prague, Czech Republic, 19–21 February 2019; pp. 288–294. [CrossRef]
69. Lopez-Carreiro, I.; Monzon, A.; Lois, D.; Lopez-Lambas, M.E. Are travellers willing to adopt MaaS? Exploring attitudinal and personality factors in the case of Madrid, Spain. *Travel Behav. Soc.* **2021**, *25*, 246–261. [CrossRef]
70. Aman, J.J.C.; Smith-Colin, J. Application of crowdsourced data to infer user satisfaction with Mobility as a Service (MaaS). *Transp. Res. Interdiscip. Perspect.* **2022**, *15*, 100672. [CrossRef]

71. Huang, S. Listening to users' personal privacy concerns. The implication of trust and privacy concerns on the user's adoption of a MaaS-pilot. *Case Stud. Transp. Policy* **2022**, *10*, 2153–2164. [CrossRef]
72. Iotzov, V.; Cartolano, F.; Ciccarelli, G.; Durant, T.; Rizzoli, A.E. Integration vs fragmentation: Alternative tactics of local mobility businesses in response to a global wave of market disruptions. In Proceedings of the 7th Transport Research Arena TRA 2018, Vienna, Austria, 16–19 April 2018.
73. Schikofsky, J.; Dannewald, T.; Kowald, M. Exploring motivational mechanisms behind the intention to adopt mobility as a service (MaaS): Insights from Germany. *Transp. Res. Part A Policy Pract.* **2020**, *131*, 296–312. [CrossRef]
74. Wright, S.; Nelson, J.D.; Cottrill, C.D. MaaS for the suburban market: Incorporating carpooling in the mix. *Transp. Res. Part A Policy Pract.* **2020**, *131*, 206–218. [CrossRef]
75. Caiati, V.; Rasouli, S.; Timmermans, H. Bundling, pricing schemes and extra features preferences for mobility as a service: Sequential portfolio choice experiment. *Transp. Res. Part A Policy Pract.* **2020**, *131*, 123–148. [CrossRef]
76. Casadó, R.G.; Golightly, D.; Laing, K.; Palacin, R.; Todd, L. Children, Young people and Mobility as a Service: Opportunities and barriers for future mobility. *Transp. Res. Interdiscip. Perspect.* **2020**, *4*, 100107. [CrossRef]
77. Ye, J.; Zheng, J.; Yi, F. A study on users' willingness to accept mobility as a service based on UTAUT model. *Technol. Forecast. Soc. Change* **2020**, *157*, 120066. [CrossRef]
78. Kokolakis, S. Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Comput. Secur.* **2017**, *64*, 122–134. [CrossRef]
79. Wu, C.; Vine, S.L.; Sivakumar, A. Assessment of the barriers in establishing passenger mobility-as-a-service (MaaS) systems: An analogy with multimodal freight transport. *Case Stud. Transp. Policy* **2025**, *20*, 101433. [CrossRef]
80. Kriswardhana, W.; Esztergár-Kiss, D. Examining university students' preferences toward MaaS aspects. *Transp. Res. Interdiscip. Perspect.* **2025**, *30*, 101348. [CrossRef]
81. Tang, J.H.C.G.; Liu, J.; Chen, A.; Wang, B.; Zhuge, C.; Yang, X. Exploring the potential adoption of Mobility-as-a-Service in Beijing: A spatial agent-based model. *Transp. Res. Part A Policy Pract.* **2025**, *194*, 104430. [CrossRef]
82. Lopez-Carreiro, I.; Monzon, A.; Lopez, E. Assessing the intention to uptake MaaS: The case of Randstad. *Eur. Transp. Res. Rev.* **2024**, *16*, 2. [CrossRef]
83. Tsirimpa, A.; Karakikes, I.; Tsouros, I.; Mohammed, A.; Tahmasseby, S.; Salam, S.; Alhajyaseen, W.; Polydoropoulou, A. The role of subscription sharing and nationality in MaaS uptake in Qatar. *Case Stud. Transp. Policy* **2025**, *19*, 101364. [CrossRef]
84. Yu, S.; Li, B.; Wang, H.; Liu, Y.; Hu, S. Applying a Modified Technology Acceptance Model to Explore Individuals' Willingness to Use Mobility as a Service (MaaS): A Case Study of Beijing, China. *Systems* **2024**, *12*, 511. [CrossRef]
85. Tunn, V.; Van Opstal, W.; Athanasopoulou, A. Unlocking Sustainable Mobility: Consumer Preferences and Segments on Mobility-as-A-Service Platforms. Available online: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5168626 (accessed on 5 June 2025).
86. Kriswardhana, W.; Esztergár-Kiss, D. University students' adoption of mobility as a service with respect to user preferences and group differences. *J. Public Transp.* **2024**, *26*, 100079. [CrossRef]
87. Underhill, B.; Knowles, A. Governance Participation Strategies for Mobility as a Service. In Proceedings of the Transportation Association of Canada 2020 Conference and Exhibition-The Journey to Safer Roads, Toronto, ON, Canada, 21 September–8 October 2020.
88. Knowles, A.; Underhill, B.; Wong, R.; Lightsone, A. Mobility as a Service: Governance Strategies for Impending Disruptions. In Proceedings of the 2019 Canadian Transportation Research Forum 54th Annual Conference-Change, Vancouver, BC, Canada, 26–29 May 2019.
89. Bevis, K.; Sozcu, O.; Fenner, R. Mobility as a Service. Presented at EEVConvention: Policies and Best Practice, Oslo, Norway, 25 September 2018.
90. Mitropoulos, L.; Kortsari, A.; Mizaras, V.; Ayfantopoulou, G. Mobility as a Service (MaaS) Planning and Implementation: Challenges and Lessons Learned. *Future Transp.* **2023**, *3*, 498–518. [CrossRef]
91. Murati, E. Mobility-as-a-service (MaaS) digital marketplace impact on EU passengers' rights. *Eur. Transp. Res. Rev.* **2020**, *12*, 62. [CrossRef]
92. Kamargianni, M.; Goulding, R. The Mobility as a Service Maturity Index: Preparing the Cities for the Mobility as a Service Era. In Proceedings of the 7th Transport Research Arena TRA 2018, Vienna, Austria, 16–19 April 2018. [CrossRef]
93. Kamargianni, M.; Li, W.; Matyas, M.; Schäfer, A. A Critical Review of New Mobility Services for Urban Transport. *Transp. Res. Procedia* **2016**, *14*, 3294–3303. [CrossRef]
94. Hlubi, N.; Seftel, L. Could Mobility as a Service (MaaS) Have a Role in an Integrated Public Transport Network in South African Cities? In Proceedings of the 38th Annual Southern African Transport Conference 2019, Pretoria, South Africa, 8–11 July 2019.
95. Bandeira, J.M.; Macedo, E.; Teixeira, J.; Cicarelli, G.; Niculescu, M.; Fischer, N.; Gather, M. Multidimensional indicator of MaaS systems performance. *Transp. Res. Procedia* **2022**, *62*, 491–500. [CrossRef]

96. Gompf, K.; Traverso, M.; Hetterich, J. Towards social life cycle assessment of mobility services: Systematic literature review and the way forward. *Int. J. Life Cycle Assess.* **2020**, *25*, 1883–1909. [CrossRef]
97. Mohammed, A.; Salam, S.; Tahmasseby, S.; Alhajyaseen, W. Governance as Success Factor for Implementing MaaS in Countries with High Share of Expatriates: Qatar's Case Study. *Transp. Res. Procedia* **2025**, *82*, 547–562. [CrossRef]
98. Nikitas, A.; Cotet, C.; Vitel, A.E.; Nikitas, N.; Prato, C. Transport stakeholders' perceptions of Mobility-as-a-Service: A Q-study of cultural shift proponents, policy advocates and technology supporters. *Transp. Res. Part Policy Pract.* **2024**, *181*, 103964. [CrossRef]
99. Chu, K.F.; Guo, W. Privacy-preserving federated deep reinforcement learning for mobility-as-a-service. *IEEE Trans. Intell. Transp. Syst.* **2023**, *25*, 1882–1896. [CrossRef]
100. Finnish Ministry of Justice. Personal Data Act (1999). Finnish law, Finlex 523/1999 Available online: https://natlex.ilo.org/dyn/natlex2/r/natlex/fe/details?p3_isn=73914 (accessed on 1 May 2025).
101. Andrews, E.S.; Barthel, L.P.; Tabea, B.; Benoît, C.; Ciroth, A.; Cucuzzella, C.; Gensch, C.O.; Hébert, J.; Lesage, P.; Manhart, A.; et al. *Guidelines for Social Life Cycle Assessment of Products*; Technical Report; United Nations Environment Programme: Nairobi, Kenya, 2022.
102. Goedkoop, M.J.; de Beer, I.M.; Harmens, R.; Saling, P.; Morris, D.; Florea, A.; Hettinger, A.L.; Indrane, D.; Visser, D.; Morao, A.; et al. Product Social Impact Assessment Handbook. 2020. Available online: https://ciraig.org/index.php/project/product-social-impact-assessment-handbook/ (accessed on 1 May 2025).
103. Jing, Q.; Vasilakos, A.V.; Wan, J.; Lu, J.; Qiu, D. Security of the Internet of Things: Perspectives and challenges. *Wirel. Netw.* **2014**, *20*, 2481–2501. [CrossRef]
104. Jain, P.; Gyanchandani, M.; Khare, N. Big data privacy: A technological perspective and review. *J. Big Data* **2016**, *3*, 25. [CrossRef]
105. Lyons, G.; Hammond, P.; Mackay, K. The importance of user perspective in the evolution of MaaS. *Transp. Res. Part A Policy Pract.* **2019**, *121*, 22–36. [CrossRef]
106. Landolfi, G.; Bami, A.; Izzo, G.; Montini, E.; Bettoni, A.; Vujasinovic, M.; Gugliotta, A.; Soares, A.L.; Diogo Silva, H. An Ontology Based Semantic Data Model Supporting A Maas Digital Platform. In Proceedings of the 2018 International Conference on Intelligent Systems, Funchal, Portugal , 25–27 September 2018; pp. 896–904. [CrossRef]
107. Yazdizadeh, A.; Farooq, B. Smart Mobility Ontology: Current Trends and Future Directions. In *Handbook of Smart Cities*; Springer: Berlin/Heidelberg, Germany, 2021; pp. 803–838. [CrossRef]