UNIVERSITY OF TARTU
Faculty of Science and Technology
Institute of Computer Science
Innovation and Technology Management Curriculum

Ijeoma Faustina Ekeh

A Recommendation Model for Security Risk Management in Car-Sharing Scenarios

Master's Thesis (20 ECTS)

Supervisor: Raimundas Matulevičius, PhD

Tartu 2024

A Recommendation Model for Security Risk Management in Car-Sharing Scenarios

Abstract:
The sharing economy has become more common today, and car-sharing has grown globally as a transportation alternative. While this is an intelligent concept to reduce traffic congestion as countries transition towards smarter cities and more shared mobility, several researchers have raised concerns about users' data privacy when their information is shared to access this service and the security risks of sharing such information between systems. In this thesis, we used the research method of a systematic literature review to understand the state-of-the-art and context of the car-sharing system. The research result identified the existing context and scenarios of car-sharing. Furthermore, the thesis follows the Information System Security Risk Management (ISSRM) methodology for implementing Security Risk Management (SRM). Based on this, we identify assets, the security risks that present the threats and vulnerabilities associated with car-sharing scenarios, and mitigation strategies by utilising the results retrieved from the SLR carried out. We present the threat modelling approach, STRIDE; thus, the risk analysis was pivotal in understanding the scope of each threat based on the literature. Finally, the thesis proposed a security risk recommendation model for reducing car-sharing scenario risks. To achieve this, the model depicts the protected assets and the control measures. The instantiated model shows the proof of concept for implementing the recommendation model into car-sharing business processes.

Keywords:
Car-sharing, Security Risk Management (SRM), Security Risks, Recommendation Model, Scenarios, ISSRM

CERCS: T120 - Systems engineering, computer technology

Soovitusmudel turvariskide juhtimiseks autojagamise stsenaariumides

Lühikokkuvõte:

Jagamismajandus on tänapäeval muutunud levinumaks ning autode jagamine on transpordialternatiivina globaalselt kasvanud. Kuigi see on intelligentne kontseptsioon liiklusummikute vähendamiseks, kui riigid liiguvad nutikamate linnade ja jagatud mobiilsuse poole, on mitmed teadlased väljendanud muret kasutajate andmete privaatsuse pärast, kui nende teavet jagatakse sellele teenusele juurdepääsuks, ja turvariskide pärast, mis tulenevad sellise teabe jagamisest süsteemide vahel.

Käesolevas lõputöös kasutasime süstemaatilise kirjanduse ülevaate uurimismeetodit, et mõista autojagamissüsteemi tipptasemel ja konteksti. Uurimistulemused tuvastasid autojagamise olemasoleva konteksti ja stsenaariumid. Lisaks järgib lõputöö infosüsteemi turberiski juhtimise (ISSRM) metoodikat turvariskide juhtimise (SRM) juurutamiseks. Selle põhjal tuvastame varad, turvariskid, mis kujutavad endast autojagamise stsenaariumitega seotud ohte ja haavatavust, ning leevendusstrateegiad, kasutades läbiviidud peegelkaamerast saadud tulemusi. Tutvustame ohtude modelleerimise lähenemisviisi STRIDE; seega oli riskianalüüs iga ohu ulatuse mõistmisel kirjanduse põhjal otsustava tähtsusega. Lõpuks pakuti lõputöös välja turvariskide soovitusmudel autojagamise stsenaariumiriskide vähendamiseks. Selle saavutamiseks on mudelil kujutatud kaitstavaid varasid ja kontrollimeetmeid. Instantseeritud mudel näitab kontseptsiooni tõestust soovitusmudeli rakendamiseks autode jagamise äriprotsessides.

Võtmesõnad:

Autojagamine, turvariskide juhtimine (SRM), turvarisk, soovitusmudel, Stsenaariumid, ISSRM

CERCS: T120 - Süsteemitehnoloogia, arvutitehnoloogia

Acknowledgements

I want to thank my family: my mother, Mrs. Caroline Ngozi Eke, for her consistent love and support, and my siblings, Moses and Vivian, for constantly checking up to see that I am well throughout my studies. I especially thank my dearest cousin (*Nnam*), Rev. Fr. Dr Nathaniel Eke, CMF, for his prayers, support, love, and advice and for taking the time to proofread my thesis. They are the reasons I have become successful today. I would also like to thank my guardian, Mrs. Carole Kieran-Oris, and other relatives for always listening to and caring for me during my studies and while writing this thesis.

I am most grateful to my supervisor, Prof. Raimundas Matulevičius, who supported me throughout my thesis with good feedback and insightful discussions. His contributions to this thesis, which applied the results in the CHESS pilot research, are significant to me. Also, to Dr. Abasi-Amefo Affia, who gave me a guide during the thesis, I say thank you.

I want to thank my friends Simon, Dave, Vee, Asem, Mimi, Tolu, Frank, Tham and Racheal for reading through my thesis and for their support and joy throughout my studies. Finally, thank you to my father and guardian, the Late Mr Longinus Obiesi Eke and the Late Engr—Kieran Orisakwe, both blessed memories.

This work is part of the Cyber-security Excellence Hub in Estonia and South Moravia (CHESS) project funded by the European Union under Grant Agreement No. 101087529. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Research Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

Faustina Ekeh
Tartu, 2024

Contents

List of Tables

List of Figures

1 Introduction

Unlike traditional car rentals or ownership, car-sharing services allow individuals to use a vehicle when needed without the burdens of maintenance, parking, or long-term commitments[29]. By utilising technology and a network of shared vehicles strategically placed throughout urban areas, car-sharing companies have revolutionised how people move from one place to another. The car-sharing market has grown continuously in the last few years as people are moving towards not owning private cars and adopting car-sharing models [29]. To move towards a more sharing and circular economy, private car owners now rent cars by using a mobile application to order a ride and make payments through the payment channels provided rather than handle their daily outings with their cars. The proposed solution has reduced traffic congestion, especially in modern and urban cities with smart infrastructure. The business models of car-sharing are business-to-consumer (B2C) and Peer-to-Peer (P2P) [13]. These car leasing companies include Citybee, whose market is stationed in Estonia and other Baltic states, BoltDrive, Car2Go, Getaround [29], and many more worldwide. Researchers have observed the evolution of car-sharing terminology, discussing its progression towards a sustainable future and economy in various papers. However, they also highlight the need for further research on the security framework of the system. Therefore, we believe that one challenge this car-sharing system may face is the security of information shared, as users share lots of information in the cause of using the service.

1.1 Scope

The adoption of car-sharing has become the norm in the sharing economy era. Different companies utilise the service to ease urban traffic in big cities. Car-sharing services are rapidly evolving, and some researchers describe them as the new era of transportation. However, more research on the ideology is focused on its user behaviour and business models as companies apply the idea in different models such as peer-to-peer (P2P), Business-to-Customer (B2C) and Business-to-Business (B2B). The most commonly used is B2C, where the service provider leases the car for a short period in exchange for a fee for that particular trip [21]. With these concepts, the information shared in the service is subject to possible risks, which makes it prone to attacks. The scope of the research focuses on the various scenarios of the B2C car-sharing services to understand the flow of information in the different scenarios, identify the sensitive private data shared, and implement security risk management to mitigate the risks. The thesis did not apply further computational costs of the recommended control measures. The thesis does not explicitly describe privacy-enhancing technologies for mitigating risk but focuses more on the various methods selected from the literature.

1.2 Objective of Research

This research explores the state of the art of car-sharing. Firstly, we aim to identify the concepts of car-sharing, understand the main processes of the system, and analyse the security framework of car-sharing by identifying potential threats and vulnerabilities to the system. Hence, to achieve this, we shall conduct a systematic literature review to understand the level of security implementations already addressed in different research works. Secondly, we shall analyse security risks using the Security Risk Management approach (SRM) by first identifying the assets that need to be protected, the risks that exist within the system, and ways to mitigate those identified risks based on the literature reviewed. Finally, we aim to propose recommendations to reduce the existing risks. The findings of this research will provide valuable insights for stakeholders in the car-sharing sector on how such risks can be mitigated to forestall misuse of the system and how they can also be used to inform policy decisions and promote sustainable and secured transportation solutions.

1.3 Research Questions

In this section, we define our main research questions and break them down into smaller research questions to refine our main objectives for this thesis. **MRQ: How to manage security risks in car-sharing scenarios?** The main thesis question breaks down into the following:

- **RQ 1:** What is the context of the car-sharing system?
- **RQ 2:** What are the protected assets in car-sharing scenarios?
- **RQ 3:** What are security risks and their reduction approaches in car-sharing scenarios?

1.4 Research Method

We employed a systematic literature review using Kitchenham *et al.* [14] approach to conduct this thesis. The first task was to use the SLR to synthesise the results of the state-of-the-art car-sharing system by using available literature sources and performing search queries using specific keywords. The SLR also involves using inclusion and exclusion criteria in selecting the papers and extracting information about the architecture and security of the car-sharing systems. We used the Information System Security Risk Management (ISSRM) method to extract and present the results from the systematic literature review. Finally, we proposed a recommendation model based on the SLR conducted on how the system can mitigate security risks.

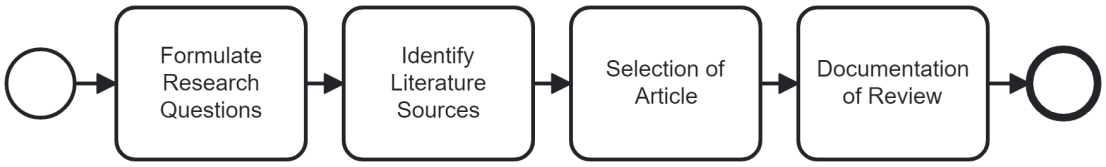

Figure 1. Systematic Literature Review Process

1.5 Thesis Contribution

The following contribution shall be made with the results of this thesis:

- The thesis presents a systematic literature review of the processes and risk analysis to understand the threats, vulnerabilities, and impacts to each asset in the car-sharing scenario and how they are mitigated based on the literature. The results would guide security risk analysts in understanding the existing security framework of the car-sharing system.
- The thesis proposes a recommendation model to mitigate the risks in the car-sharing system, thereby contributing to the sector. The results of this recommendation would give stakeholders ease of understanding the risk in each function carried out in the system and enable them to mitigate the risk following our recommendations.

1.6 Thesis Structure

The rest of the thesis is as follows: Chapter 2 presents the systematic literature review approach used in the work, which follows the Kitchenham *et al.* [14] framework of a systematic protocol. The SLR processes include formulating the research question, identifying the literature sources from the various databases, selecting the paper based on the inclusion and exclusion criteria, quality assessment, data extraction, results presentation, and discussion. In Chapter 3, we describe the different scenarios of car-sharing by capturing them in business process models. We also defined the various terms associated with car-sharing based on the literature. Chapters 4 and 5 focus on security risk management (SRM), which follows the ISSRM model. The chapter contains the protected asset identification, which describes the business and IS assets of the car-sharing system, and the risk identification, which demonstrates the risk analysis of the car-sharing system by identifying threats that affect the assets in the car-sharing model and risk reduction. In Chapter 6, we would propose a recommendation model that would validate the mitigation of the risks associated with car-sharing, and the final chapter of the thesis presents its limitations, answers to the research question, and future work.

2 Systematic Review Literature

In this section, we implemented the systematic literature review method of the security of car-sharing. We reviewed the literature following Kitchenham *et al*. [14] stages of SLR. This systematic literature review (SLR) will study the existing literature on the context, security risks, and reduction strategies of car sharing scenarios.

2.1 Literature Sources

For the Literature sources, we primarily searched using electronic databases to find relevant academic papers in Scopus, IEEE, Springer Link, Science Direct, ACM Digital Library, and Web of Science. We also included References to pertinent works as extra sources. These papers include journal articles, conference proceedings, book chapters, and the Internet.

2.2 Search Query

To search for relevant papers, we utilised the following search queries and terms as presented in Table 1 for each database: *Car-Sharing, Identity Management, Data-Sharing, System Security, Privacy, Data Breaches, Security Risks, Ride-Sharing, and Threats*. The querying operators AND and OR were used to carry out the queries. We used the Synonym identity management to get papers describing scenarios for managing user data. We ran a combination of these keywords in the different databases to give us a robust search of literature covering security in car-sharing. However, some word phrases were only partially relevant to the study's case. For example, consider the term "carpooling," which some literature considered relevant for explaining car-sharing but omitted. Due to the research limitations on "car sharing," the phrase "ride sharing." was also used to broaden the search category.

2.3 Inclusion and Exclusion Criteria

Table 2 depicts the inclusion and exclusion criteria to search for the relevant papers. The process lets us focus on which paper to select, aiding the research.

Table 1. Query Table

Q1: Scopus	**Q2: IEEE Xplore**	**Q3: Web of Science**	**Q4: ACM/-Science Direct**	**Q5:SpringerLink**
"Car-sharing" AND "Data breaches"	"Car" AND "Sharing"	"Security threats" or "Security Risks" AND "Car-sharing"	"Data sharing" AND "Security" OR Car	"car sharing" AND "Identity" AND "Management"
"car sharing" AND "Identity Management"	"car AND "sharing" AND "system" AND "Privacy"	"Car sharing" AND "Privacy"	"Identity AND Management"	"car sharing"
"Data breaches" AND "Identity" AND "Ride" OR "car" AND "Sharing"	"car sharing"	"Car sharing"	"Ridesharing" AND "Car sharing"	-

Table 2. Inclusion and Exclusion Criteria

Inclusion	**Exclusion**
The paper's scope is associated with the research question	The paper does not clearly express their thoughts on Car-sharing
The paper is written in English.	The paper was not written in English
The paper proposes security architecture models for car-sharing	Paper that discuss models for carpooling and ride-sharing.
Papers with duplicates	Papers without duplicates
The paper addresses the narrowed scope of the research	The paper covers a broader range of research (Internet of Vehicles, Vehicle Sharing, Blockchain Security).
Papers with open access and availability using the university's network	Papers with closed access

2.4 Paper Selection

The selection of papers started with searching for keywords using the search queries (see Section 2.2). Searching digital libraries and databases described in Section 2.1 yielded 81 papers. The search queries cover car-sharing and have limited our results to papers covering car-sharing systems' security. The papers were analysed manually by reading the title, abstract, and introduction to the documents representing our research's scope. The first paper selection used the inclusion and exclusion criteria, as shown in Table 2 above. During the screening, we removed seven papers as duplicates.

Furthermore, the authors removed 20 papers contributing to ride-sharing while reading each abstract, though the application of ride-sharing was a keyword during the primary search. This removal happened because the papers described ride-sharing as having two or more people share a ride, which means the ride-sharing results had different scopes from what car-sharing means, although some papers may relate them. We also removed documents focusing on the Internet of Vehicles and car sharing because they covered a broader scope. There was also the removal of four without access rights or needing payment using the exclusion analysis. (See Table 2). The 51 papers used for further analysis were papers for which the university's digital library granted access to the authors. Analysing the papers resulted in 5 additional papers obtained from snowballing. The addition of the grey literature found due to snowballing made the total number of papers 86.

We implemented two filters to get the final papers, which proceeded to quality assessment (see Section 2.5). The first approach was a general filter, as stated above, and the second filter was more synthesised by using inclusion and exclusion criteria and the quality assessments of documents that passed the selection criteria (see Section 2.5). We resolved the final papers that were the most relevant for the research, which were 12 papers. The reason is that most papers were out of the scope of the study because we have narrowed our research down to the security of car-sharing while most papers discussed a range of topics for the business models of car-sharing, cloud computing in the era of the sharing economy, ride-sharing and car-pooling, the Internet of vehicles and, the behaviour of users while using the car-sharing service. These papers did not focus on the security concepts of car-sharing, and as such, they were redundant to our research. However, four extra papers described the concepts and terminologies related to car-sharing and were used to answer our research question (*SRQ1*). Second, the research area of security in car-sharing was minimal.

2.5 Quality Assessment

The final selection phase is to scrutinise the papers further to see how they answered the research questions and to avoid possible bias in the selection of documents. The documents that do not answer the following questions were subject to removal. The

paper quality assessment focuses on the following questions:

1. Does the paper describe the architecture of the car-sharing system?
2. Are there security suggestions the paper gives to address security risks or privacy concerns?
3. Does the paper cover relevant studies on an information system's use case and vulnerabilities?

The quality evaluation used were *Yes, Partially, No*. Yes = 5 (answers all of the questions mentioned) Partially = 3 (responds to two-thirds of the questions asked) No = 1 (the article is entirely outside the subject of the research). The selection process included reading the papers to determine the researcher's perspective and whether they addressed the extent of the design, security concerns, and mitigation employed for the car-sharing system. Papers with at least a 3.5 score would be included in the research and then scrutinised. After the quality check, we had 16 papers after applying the final filter. We, however, removed four papers from the snowballing as the papers' discussion was irrelevant to the research. At the end of this scrutiny, 12 papers were eligible for further study and analysis. They covered the concepts, processes, and risk models for the car-sharing system extensively, while four papers captured the ideas.

Table 3. Paper Selection

Sources	**Scopus**	**ACM/ Science Direct**	**IEEE Xplore**	**Web of Science**	**Springer**	**Snowball (X)**	**Total**
Returned	45	9	19	6	2	5	86
First Filter	23	4	14	3	2	5	51
Second Filter	16	3	9	2	2	4	36
Final	8	2	4	-	1	1	16

2.6 Information Extraction

The extraction of Information will aid our research, extract relevant data covering car-sharing architecture, and answer our research questions. In the first extraction, we have summarised the papers to understand the concepts, processes, and risks described in the papers. In the second part of the extraction, we elicited the critical processes of car-sharing from the papers (see Table 5). These main processes were further broken down

into sub-processes to understand the concept of each activity carried out in car-sharing by mapping each sub-process to a particular paper and describing how each author termed the process (see Appendix 3). Furthermore, we presented these sub-processes using BPMN to expand the process into different tasks, from which we will understand the various assets that are to be protected. In the third part of the extraction, we aimed to extract information about the threats and vulnerabilities that affect the car-sharing assets as depicted in the BPMN process and the impact of these threats and vulnerabilities on the car-sharing system.

Table 4. Information Extraction Form

Information	**Extraction**
Authors	Name of Authors
Title	Title of Paper or Article
DOI	ID of Paper
Main Processes	Main Processes of the Car-sharing system
Sub-Processes	Sub-process of each key process in the Car-sharing system
Concepts	Various terms used by authors to describe the main process in the Car-sharing system
Information Type	Type of data used to describe the Car-sharing system
Vulnerabilities	weakness of the Car-sharing system
Threats	Threats described within the Car-sharing system
Impact	Impact of Attacks on the Car-sharing System
Mitigation Strategies	Methods used to reduce the risks found within the Car-sharing system

2.7 Overview and Summary of Selected Articles

Car-sharing is a relatively new research area, especially in papers focused on implementing privacy and security in the system. More research focuses on the behaviour of car-sharing users and owners during and after the ride and the different car-sharing models, such as P2P sharing and Free float sharing. However, few papers describe the security components and security requirements of car-sharing. Some others described how the infrastructure of car-sharing could be protected from attacks by adversaries, focusing on one use case, for instance, the authentication of users. Fig. 2 depicts the

number of papers used for this research from the libraries. Scopus provides more academic papers with relevant research on the security and privacy of car sharing. There were also repeated papers in the various digital libraries, so we removed them from the initial screening of papers (see Section 2.4), hence, the size of the papers used for this research. In Fig. 3, we show the distribution by year of publication to understand the time range for the papers selected. The chart shows that more articles addressing the security risks of car sharing and its mitigation measures were published between 2017 and 2023.

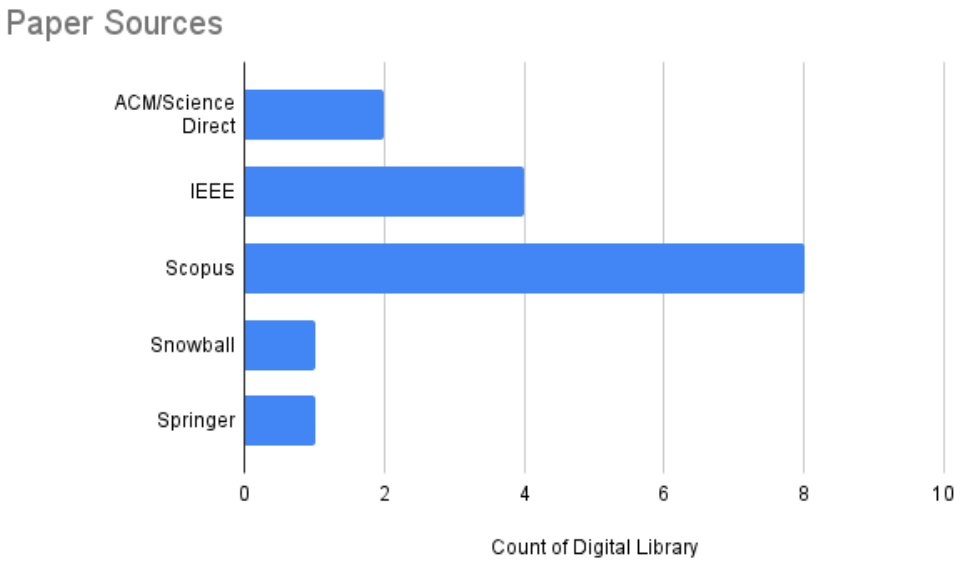

Figure 2. Count of Digital Library

Arm *et al.* [1] describe a system that consists of an embedded device for accessing a car, a back-end server, and a mobile app and describe the flow of the car-sharing process. They also illustrated the various actors and stakeholders involved in the car-sharing process. The paper also addressed issues concerning security, safety, and privacy. Auer *et al.* [2] explored a conceptual design on how to use blockchain and IoT technologies to increase the shared mobility process, and they proposed that a blockchain-IoT-based platform will promote and streamline the car-sharing process. In their proposed framework, all stakeholders in the leasing platform come together, and the workflows are streamlined to increase the user experience.

Cao *et al.* [5] propose a novel identity authentication key-exchange protocol that uses biometrics and passwords as authentication methods because combining both features could strengthen and increase data protection and security performance. The security

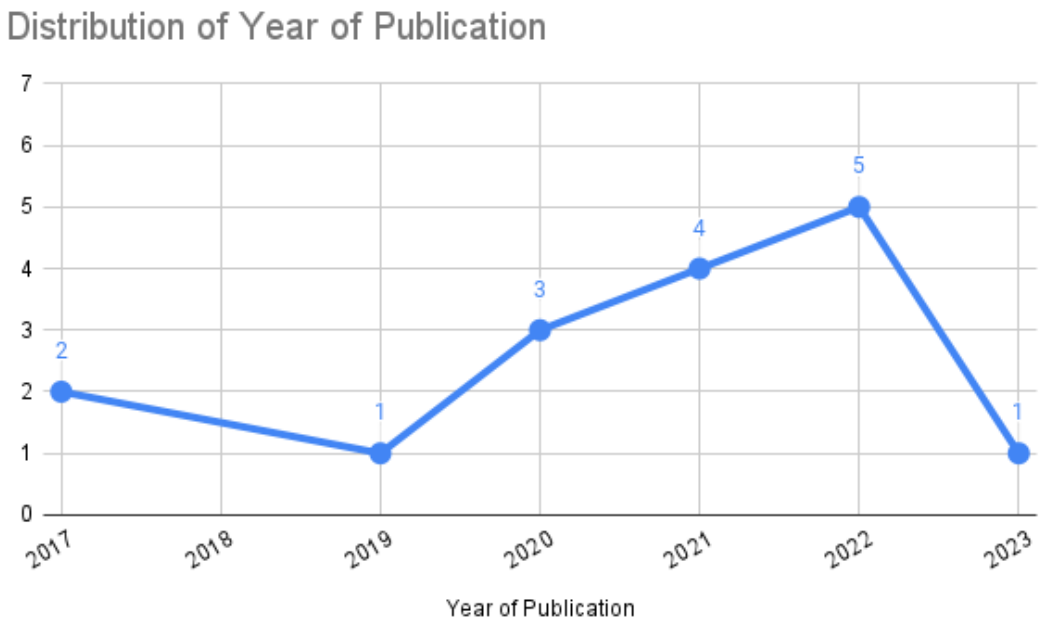

Figure 3. Research Year Distribution

requirements for this protocol were tested, and it was found that the scheme has no security vulnerabilities and protects the user's privacy throughout their service usage.

Dzurenda *et al.* [8] present a novel system where users of the car-sharing service can access the car without the need for sharing physical keys between the owners of the vehicle and the user, with an emphasis on security, privacy, and low computational demands. The system was designed more for smaller fleets and not a more extensive fleet of cars. They analysed already existing car-sharing scenarios, addressing such platforms' privacy and security aspects.

Kim *et al.* [13] propose, similar to [32], a decentralised car-sharing system that could reduce the single point entry attacks that centralised car-sharing system. They used blockchain to ensure the integrity of the data shared by the user with the system. They proposed a secure authentication scheme for the car-sharing system to withstand different threats and vulnerabilities that the system may face, thereby granting privacy-preserving access to the cars. They validated the system using AVISPA to analyse the mitigation performance of threats, such as man-in-the-middle attacks.

Ma *et al.* [16] propose the MobiDIV architecture that addresses the verification of the users to curb the potential privacy and security issues that arise when a user decides to rent a car. They proposed that users can access all their data locally using their smartphones without the companies saving their details on the cloud. The process involves using

a real-time verification process for the user. They proposed that MobiDiv verify the driver's identity and detect if an unknown driver is using the car. The framework consists of two parts, which deal first with the verification of the driver in real-time and also with an anomaly operation detection module that monitors the driver's and the car's behaviour throughout the driving cycle.

Pollicino *et al.* [23] propose a novel architecture that enables people to share their cars with prospective users through intermediate brokers. These brokers manage the expected requirements of the users as authorisation services. They opined that their framework tackles security concerns, increases the accountability protocol of the owners of the shared cars, and increases users' trust in the system.

Cheng *et al.* [7] investigate the influence of perceived risks and how the trade-off between perceived risks and benefits affects people's information privacy choices in IT-enabled ride-sharing. The concept can also be applied to car-sharing as users share information across different entities; thus, privacy awareness and online security findings are of utmost importance. They used a mixed-methods approach, such as privacy calculus theory and rapid gratification. Their interview findings show that privacy awareness, previous online privacy violations, mobile payment security, and unfavourable media exposure influence perceived risks of information sharing and that perceived risks and benefits are strongly tied to rapid gratification. In contrast to developing a risk analysis framework solution for car-sharing, Safdar *et al.* [24] study the perception of people's acceptance of the car-sharing systems, iterating concerns on how users perceive the data being collected during this service. The study described how security and privacy factors could influence shared mobility users.

In increasing trust in car-sharing, Moreno *et al.* [19] stated that for users to gain trust in how information is shared within a system, the identity management system relied heavily on centralised methods of probing and mitigating the risks of identity spoofing and loss of identity information. Car-sharing uses information such as the driver's licences of the user, and this kind of information needs to be protected from breaches and theft. In this scenario, the users should have a level of trust in the Identity Providers managing their data in the system. In their work, the authors proposed the OLYMPUS architecture, which is decentralised and attributes a limitation of roles to the Identity Providers, thereby enhancing trust in managing user identities. However, in their work, Bossauer *et al.* [3] looked towards creating trust for users in P2P car-sharing and explored the need to protect users' information to increase trust in the system. The authors approached the problem by explaining the need for car owners and renters to understand the need for information shared during the process, that is, before, during, and after the ride. They opined that connected technologies can help increase trust in information sharing and reduce the risk of information disclosure.

Liu *et al.* [15] proposed in their work a personal information protection scheme called "Login SoEasy" to increase the protection of user's details during authentication. In this

case, the security of the user's personal information does not affect the websites or apps, as they are not allowed to store any copy of the user's data. For instance, when users log into the car-sharing app, the information shared is not stored on the app; instead, they get the verification result, allowing them to continue using the service. The PIPSL is the trusted user agent who, in this case, stores one copy of the user's identity details and manages the information between the entities.

Symeonidis *et al.* [28] describe their protocol, SEPCAR, where users can use the shared cars without disclosing their private data to the companies. The protocol allows users to share generated access tokens, but it is assumed that the driver and the company agree on booking details. The protocol is based on four steps: session key generation and data distribution, access token generation, token distribution and verification, and car access. With these steps, the user can access the car, and the user's data is not disclosed. They stated offline authentication should be placed in the protocol to enable authentication with a car off the network coverage.

Valastin *et al.* [29] proposed that peer-to-peer short-term car-sharing applications should be based on blockchain and smart contracts, thereby improving data transparency in the car-sharing process. The authors described how to use non-fungible tokens to unlock a car. In this scenario, the car owner would be given complete control over how their personal information is accessed.

We *et al.* [31] proposed a secure key-sharing system known as hierarchical identity-based signature key sharing (HIBSKSharing). The HIBSKSharing consists of essential generation, critical transmission, and key management in protecting the car, how users can access the car based on their identity, and the distribution of these keys generated to the car users through their smartphones.

Zhou *et al.* [32] proposed a decentralised control scheme based on Smart Contract to reduce several threats the car-sharing system poses due to a centralised architecture. They also contributed more to security and privacy by establishing a secured, credible, and tamper-proof platform among the system stakeholders, thereby increasing efficiency and trust.

2.8 Security Risk Management

Security Risk Management (SRM) in [17] is a systematic approach to identifying assets, their associated risks, and mitigating risks that could exist within the system. According to [17], SRM is an "analytical procedure that helps us identify system valuable assets, stakeholders, and operations. It also provides logic and guidance to find and implement appropriate solutions and mitigation strategies." The findings in [12] *s*how that the ISSRM and ISMS-CORAS are proficient methods for managing security risk. The author applied the Plan, Do, Check, Act PDCA approach to determine the best method or framework for managing security risks. In the results, the ISSRM method covered the Plan, Do and Check as to the ISMS-CORAS. To manage confidentiality, integrity, and

availability within the car-sharing system, we applied the Information Systems Security Risk Model (ISSRM). The method provides a systematic approach to determining and managing the security risks of car-sharing scenarios within the organisation's system. The ISSRM domain model consists of three (3) key concepts, namely: *assets-related concepts*, *risk-related concepts*, and *risk treatment-related* concepts.(see Figure 4). According to [17]," *Asset-related concepts* are the organisation's assets that are important to protect. This asset could be anything that plays a valuable role in accomplishing an organisation's goal." These assets are divided into two parts: the business asset and the IS/System asset. Business assets are the core value of an organisation's mission; thus, they are immaterial [17]. The IS assets are those components that support the business assets; thus, they are part of the information system, or they can also be a person or a facility that plays a role in supporting the business assets.

The *Risk-related concepts* describe the risks associated with the IS asset. It categorises the threats and vulnerabilities a system faces and the impact that negates the security criteria of the business assets.

The *Risk-Treatment Related Concepts* describes how risks can be mitigated and treated. From the ISSRM model (see Figure 4), risk treatment decides to treat the associated risks by refining the security requirements and implementing different control measures for risk reduction.

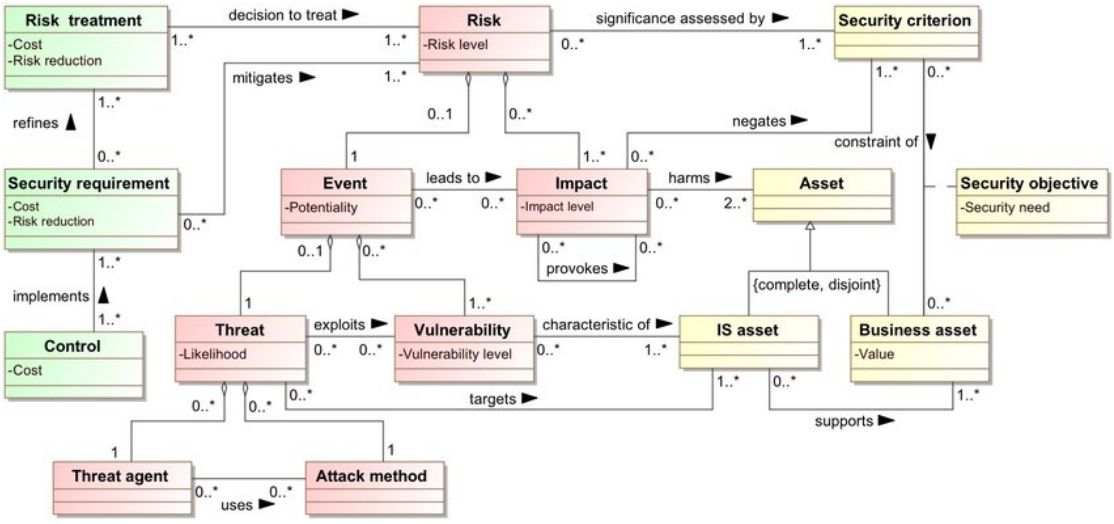

Figure 4. The ISSRM Domain Model adapted from [17]

2.9 Summary

In this chapter, we have conducted a systematic literature review following the Kitchenham *et al.* protocol by first performing a search on digital libraries using keywords from our queries, which returned 86 papers. Secondly, we apply the inclusion and exclusion

criteria to scrutinise the papers selected for the SLR. Afterwards, we synthesised the paper using further quality assessments, which resulted in 16 papers. Based on our information extraction form, a summary of the selected articles was described in the thesis. The ISSRM domain approach in managing security risk applies to the results of the SLR by extracting information from the literature to answer our research questions in the following chapters.

3 Context of Car-Sharing

In this section, we will address the research question, ***RQ 1: What is the context of the car-sharing system?*** To answer the question, we divided the research question into sub-questions based on first understanding 1. What are the main processes of the car-sharing system? 2. What are the concepts and terms used in describing the architecture of the car-sharing system? 3. How can the processes of car-sharing be used to identify the assets of the system? In providing the answers to these questions, we understand the context of the system.

3.1 Main Processes

The thesis describes the main processes as the underlying operations, which are critical to the success and user adoption of the sharing economy trend. Through a rigorous review of the existing literature, we have extracted six core processes, which are as follows: *User Registration, Verification of User, Booking of the Car, Car Access, User Behaviour process, and Payment Process*. These core processes are not isolated; instead, the processes form a cohesive scenario of the car-sharing system, addressing user interaction from the initial start to the end of service usage. In Section 3.3, we expanded this process using business process models to understand the flow of information between actors and the broader context of the scenarios **(see Models M1–M6)**.

From the presented information in Table 5, we depict the six main processes of car-sharing. However, we understood from the SLR that some processes did not appear in the literature. A detailed explanation of the process is as follows:

Process 1: User Registration refers to the process whereby the user registers into the car-sharing app to use its service.

Process 2: Verification of User refers to the process where a second party verifies the user; an identity provider would validate the information given by the user to gain access to the sharing service.

Process 3: Booking refers to the process where the user makes a reservation or booking for the car to use for a trip.

Process 4: Car Access refers to the process whereby the user can unlock a car from its locked state. To gain access to the car, the car-sharing company must approve the user.

Process 5: User Behaviour refers to the process where the behavioural information of the user and car is collected and used to monitor them throughout the service.

Process 6: Payment refers to the process of making payments for the service provided by the car-sharing company.

Table 5. Main Processes of Car-sharing

Author	**User Registration**	**Verification of User**	**Booking of Car Sharing service**	**Car Access**	**User Behaviour**	**Payment**
Cao *et al.*	✓	✓	✗	✗	✗	✗
Ma *et al.*	✓	✓	✗	✓	✓	✓
Auer *et al.*	✗	✓	✓	✓	✗	✓
Valaštín *et al.*	✗	✗	✓	✓	✗	✓
Pollicino *et al.*	✗	✓	✓	✓	✓	✓
Safdar *et al.*	✗	✗	✓	✓	✗	✗
Symeonidis *et al.*	✓	✗	✓	✓	✗	✗
Wei *et al.*	✓	✓	✓	✓	✗	✗
Dzurenda *et al.*	✓	✓	✓	✓	✗	✗
Arm *et al.*	✓	✓	✓	✓	✗	✗
Zhou *et al.*	✓	✓	✓	✓	✓	✓
Kim *et al.*	✓	✓	✗	✓	✗	✗

Sub-Processes of the Car-sharing System: The sub-processes depict the main activities within each process. ***(See Appendix 2)*** In Fig. 19, the key activities of user registration begin when prospective users install the car-sharing application and enter their personal information. This stage is crucial for establishing the user's identification in the system and verifying that the user meets eligibility requirements. It serves as the first set of user activities to allow a seamless service operation. (see Fig. 19).

Verifying the user activity process begins with the user obtaining and providing their *login credentials* to access the application. Identity providers do due diligence by cross-referencing and verifying the submitted data with trusted databases. The security of personal information and its privacy are crucial within this process, as they support the overall trustworthiness of the car-sharing system. During this activity, the authenticated users use the service; thus, the integrity of the shared data strengthens against potential attack activity. (see Fig. 20).

With the user's identity authenticated, users can make bookings to use the service. The users get permission to select a vehicle from an inventory of available cars based on user preferences and availability, providing real-time updates and a streamlined booking experience. (See Fig. 21).
After successfully booking a car, the car access activity depicts the user sending a request to access the booked car. At the same time, the service provider authenticates the token keys sent to the user to access the car. The car can only be accessed when the service provider validates the access token. (See Fig. 22). The user behaviour activity involves collecting real-time information, such as facial recognition, for enhanced security, route preferences, and driving trends. (see Fig. 23). Fig. 24 shows a payment activity whereby the service provider delivers the cost of the ride, and the user enters payment information. At the same time, a third-party actor processes the payment.

3.2 Key Concepts and Terms

This section answers the sub-question *RQ 1.2: What are the concepts and terms of the car-sharing system?* We describe the various concepts of the scenarios and the various terms used in literature to name the entities of the car-sharing system.

The concepts of the car-sharing system depict how the papers reviewed describe the various scenarios, starting when a user registers to begin using the sharing service and continuing until the user makes payment for the service. In Appendix 3, The description of different processes based on the papers are depicted

In the papers, the user registration process involves installing the app on mobile devices, providing personal information by the user, and managing and storing identity details by the provider. It cites several studies and proposes techniques ranging from simple app installation and user data entry to more complex systems incorporating cloud servers, digital identity verification, and unique random number generation for user authentication. (See Table 25).

The "Verification of User Concept" analyses various approaches to user verification from various papers. It covers the steps in getting login credentials and validating a user's identification using facial characteristics and random number checks. The approaches mentioned span from server computing to cloud-based identity verification services, focusing on the security and accuracy of identity management in car-sharing systems. Each strategy uses a range of tactics, including know-your-customer (KYC) practices, establishing private passwords, and using blockchain for user identification. These protocols establish a robust verification framework that promotes the safety and dependability of car-sharing services. (see Table 26).

Several authors report on diverse models for the booking process in car-sharing systems. These models engage users from the moment they view a list of available cars to the point where they use Geo-location services to find their selected vehicle. Each author has a distinct viewpoint on this process, with some emphasising the function of smart contracts in establishing booking orders and others emphasising the relevance of the service provider in checking booking details. (see Table 27).

The car access concepts describe numerous technological mechanisms for providing car access in a sharing system. These include cloud server interactions, the creation of unique access tokens, using smartphone apps for key generation, and validating access privileges via various modes of communication, such as NFC. The papers emphasise security and user convenience, utilising new technologies like blockchain to assure safe and efficient car access. (see Tables 28). In the user behaviour and payment models, the authors present the various scenarios of ways the sharing company tracks the user behaviour and how the user can carry out the various payment procedures (see Table 29 and 30).

Furthermore, the main terms illustrate the various descriptions within the car-sharing system. The authors described the data that represented the information type in different ways. The main terms identified include the user, who engages with the system; the service provider, who orchestrates the operational framework of the sharing service; the car used for this service; the identity provider, who is the trusted authority to handle personal data of the user by verifying the user credentials and providing authentication protocols for managing the user data; the mobile application, acting as the user interface; the smartphone and cloud infrastructure, enabling connectivity into the service; the server and databases, which manages the data storage and processing; communication protocols, which ensure data transfer; and identity details, crucial for the authentication of the user.

Table 6-7 depicts the various terms about car-sharing described in the papers and how the authors represented them in their work. However, it is worth noting that most of the data used by various authors were the same, while others differed but meant or functioned the same way in the car-sharing system.

Table 6. Key Terms of Car-sharing

Type	User	Service Provider	Car	Identity Provider	Mobile App	Smartphone	Server	Communication Protocols	Identity Details
Cao et al.	User	-	-	Server	-	smartphone	database	-	Identity
Ma et al.	Driver	Company	Car	-	smartphone app	Mobile-phone	Server	Phone Sensors, Raspberry Pi	User biological information
Auer et al.	Short-term renter	Lessee	Car	OEM	-	Smartphone	IOT sever	RFID Sensor,Message Queuing Telemetry(MQTT)	Personal Information
Valastinet al.	User	Car Owner	Vehicle	-	Application	-	database server	IOT device	Personal Information
Pollicino et al	User	vehicle owner Intermediate broker	Vehicle	Authorisation Service	-	Smartphone	-	Vehicle Sensor	Identity Information
Symeonidis et al.	Consumers	Owners	car	Car Manufacturer	-	Portable Device	Database	On-board Unit(OBU), PKI Infrastructure	Unique Identity
Wei et al.	Customer (User)	Company (owner)	Car	OEM,User Management centre	Client	Smartphone	Key Management Module	Secure Communication Module,NFC	User's Identities

Table 7. Key Terms of Car-sharing (Continued)

Type	User	Service Provider	Car	Identity Provider	Mobile App	Smartphone	Server	Communication Protocols	Identity Details
Dzurenda et al.	User	Service Provider	Car	Identity Provider	-	Mobile phone	-	On-board Unit(OBU),Bluetooth Low energy interface	Identity Details
Arm et al.	User	Service Provider	-	Identity provider, OEM Identity Manager	Mobile App	Mobile Device	Identity management server Database	BLE,NFC technology, REST API	Offcial document
Safdar et al.	User	-	car	-	Mobile phone app	-	-	-	-
Zhou et al.	Tenant	Vehicle	-	Application service	Mobile phone	Cloud Server	-	-	-
Kim et al.	User	Owner	Vehicle	Trusted Authority(TA)	-	Mobile device (Smartphone)	Stations	-	Information

3.3 Expanded Car Sharing Scenarios

The section answers the sub-research question ***RQ 1.3: How can the processes of car-sharing be used to identify the assets of the system?*** This section of the thesis introduces the expanded models of our sub-processes (see Appendix 2). This model captures the processes by describing the various tasks and transfers of information from one actor to another using business process models (BPMN), starting with the user registration into the system and ending when the payment for the service is delivered. This flow of information in the BPMN presents us with the system and IS assets of car-sharing that need protection from security risks. The actors in the following models include *User, Service Provider, Car, Identity Provider, Payment Provider*. These actors illustrate the various business functions within the system.

3.3.1 User Registration Model

Figure 5 presents the first model, *the User Registration Model (M1)*, which consist of two actors, namely:

1. ***User***: The user represents a smartphone or portable device owned by the user (person) used to initiate the car-sharing processes.

2. ***Identity Provider:*** The Identity manager manages the identity information provided by the user

The scenario presented described the activities where the user registers into the car-sharing application by providing their *Identity Details (D1)*, which include the Driver's licence, Citizen's Identity ID, Biometrics, fingerprints, etc. The user's personal information is needed to achieve the objective of this process. The expanded user registration process has to include the following tasks and activities: The user enters their personal Identity details and the means of identification (see Figure 4, A1.1). The Identity Provider manages *Identity Details (D1)* and, in managing this identity information, provides the *Login Credentials (D2)* for the user (see A1.2). The Identity Provider stores *Identity Details (D1)* and *Login Credentials(D2)* in their database (see A1.3); and finally, the Identity Provider sends a message request for the login details to the User.

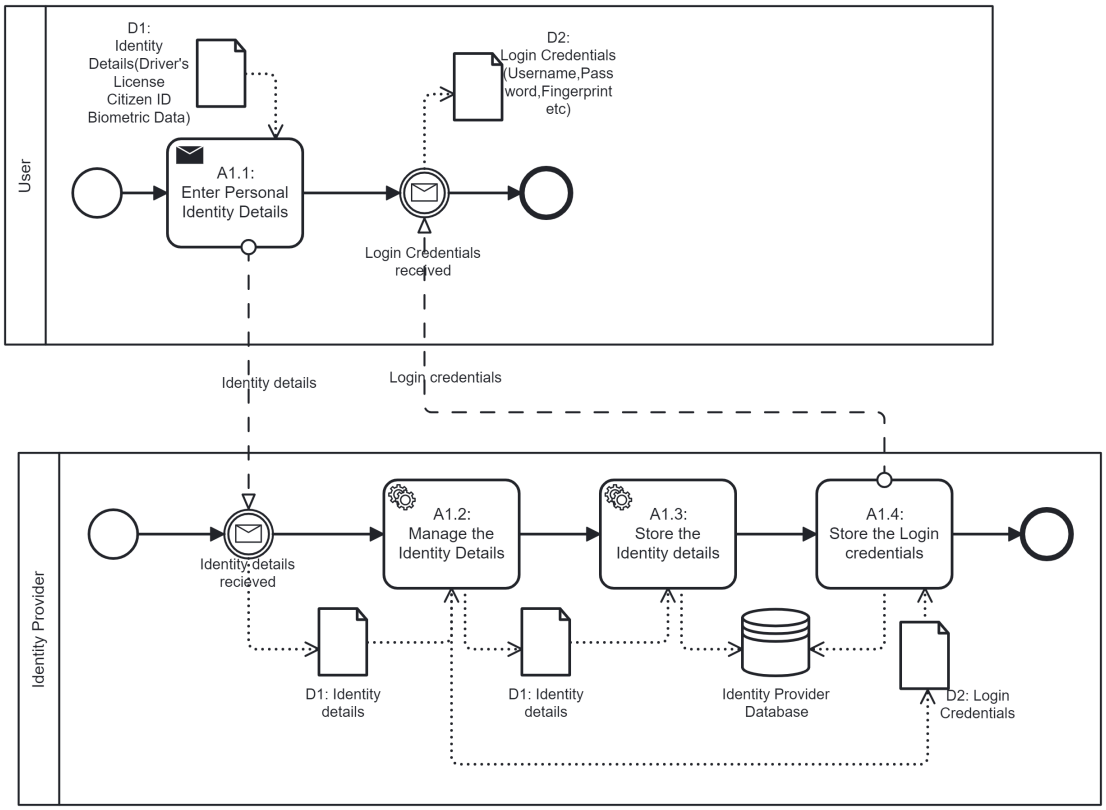

Figure 5. This Model Shows the Processes of the User Registration Scenario (**M1**)

3.3.2 User Verification Model

The second model in Figure 6 presents the user verification model (M2). This scenario depicts three (3) actors in the process. These actors include:

1. User: As described above, this is the smartphone or portable device to initiate the car-sharing processes.

2. Identity Provider: The identity provider manages the identity information provided by the user

3. Service Provider: This is the provider of the car-sharing service.

It presents how the user is verified to use the car-sharing service. From Activity (A.1.4), we understand that the Identity provider stores the *Login Credentials(D2)* of the user and sends them to the user who receives the Login Credentials. The User provides the *Login Credentials (D2)* to log into the car-sharing application (See Activity A2.1),

after which The *Identity Provider* generates the *Random number(D3)* when the user has logged into the system. (See A2.2). The *Service Provider*manages the *Random number(D3)* generated by the *Identity Provider*. The Service Provider sends the *Random number(D3)* to the User (see A2.3). The User receives the *Random number (D3)* and Enters the Random number provided (see A2.4), and the Service Provider validates the Random number (see A3.5). The Service Provider sends the *Random number(D3)* also to the Identity Provider, who validates the Random number provided by their system (see A2.6). The Service Provider accepts the Random number (see A2.7) and sends a successful Login notification to the User if the process does not fail. If the verification process is successful, the User is allowed to make a booking to use the service.

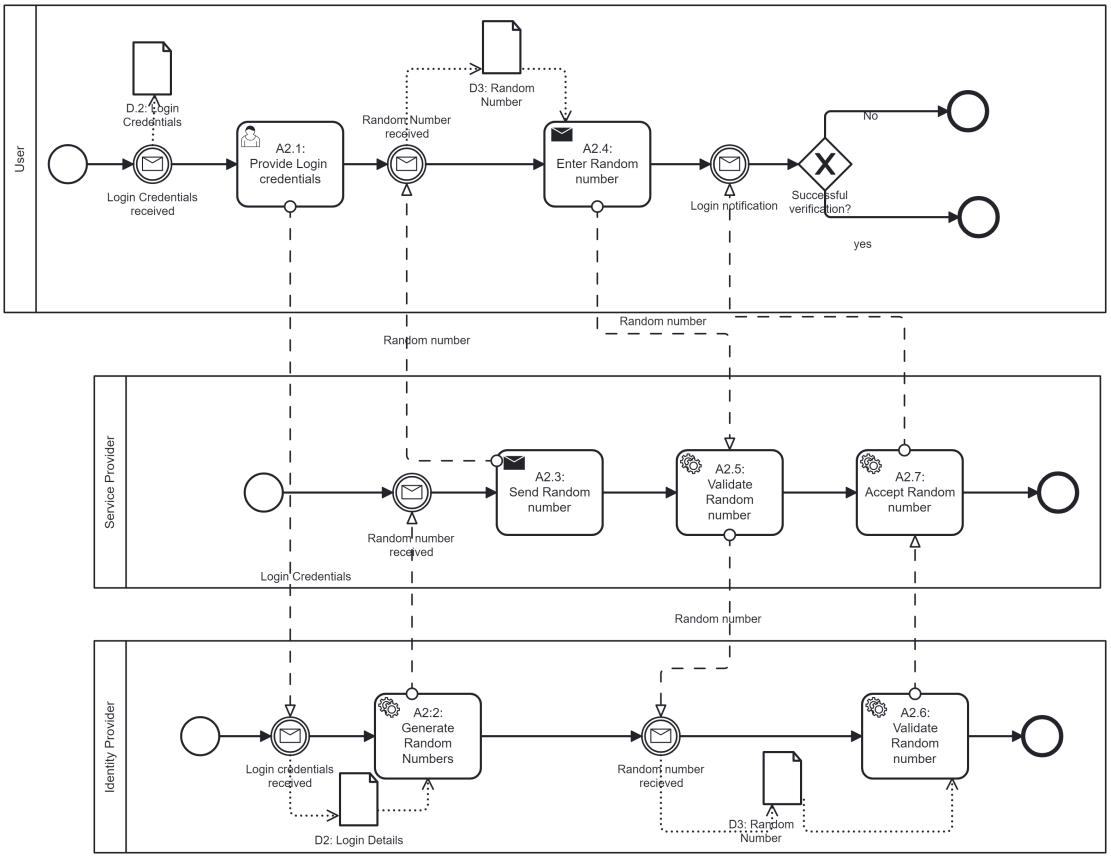

Figure 6. This Model Shows the Processes of User Verification Scenario (**M**)

3.3.3 Booking Model

The scenario of the booking model (M3) presents two actors, *User* and the *Service Provider* and depicts the different activities that take place for a user to make a booking

request successfully. In the model, the user sends a booking request to the service provider (see figure 7), who provides a list of all the available cars, and these details may include the model of the car, car type, electricity, or fuel-based consumption cars (see A3.1). The user selects a car from the list provided by the service provider (see A3.2) and enters the *Booking Details (D4)* (See A3.3), which includes User Information, Trip details, Vehicle information, etc. The Service Provider acts on the *Booking Details(D4)* of the user, validates the *Booking Details (D4)* (see A3.4), and confirms the booking (see A3.5). Furthermore, the user's booking confirmation is stored in the service provider's database, and in this model, the user gets the Geo-location of the car (see A3.6) for the ride. The *Reservation Details (D5)*, which consist of Geo-location information of the car, type of car, etc., are sent to the user to confirm that the booking is made and successful.

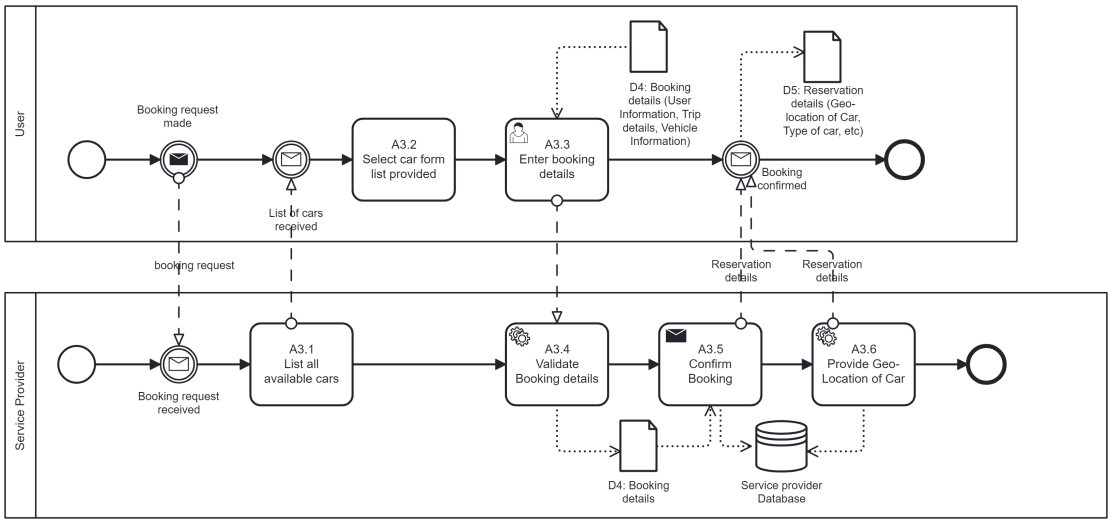

Figure 7. This Model Shows the Processes of the Booking Scenario (**M3**)

3.3.4 Car Access Model

This scenario presents the Car Access model (M4). It depicts the business processes that give the user access to the car for the service. In the model scenario, there are three core actors.

1. User: The smartphone or portable device used to initiate the car-sharing processes.
2. Service Provider: This is the provider of the car-sharing service.
3. Car: This actor comprises the communication protocols of the system, such as the sensors, OBU, BLE, and NFC communication. (see Table 7).

First, the *User* sends a request to the *Service Provider* (see A4.1) to obtain access to the *Car*. Secondly, the *Service Provider* provides a *Car Access Token (D6)* to the user (see A4.2), which communicates with the Car and unlocks it for use, after which the User sends the *Car Access token (D6)* to the *Car* (see A4.3). The car validates the *Car access token (D6)* provided by the user (see A4.4) to confirm its authenticity. If the access token passes the verification, the car sends a notification (see A4.5) to the service provider to unlock the car. The Service Provider unlocks the Car (see A4.6) and grants access for the car use.

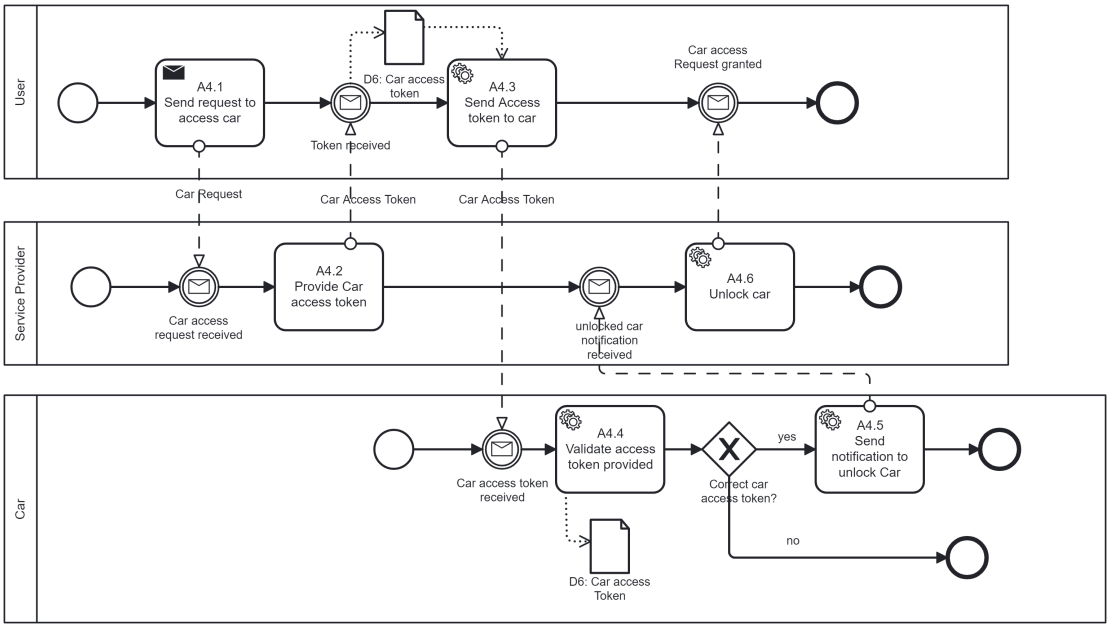

Figure 8. This Model Shows the Processes of the Car Access Scenario (**M4**)

3.3.5 User Behaviour Model

The Scenario presented the User behaviour model (M5) (see Figure 9), which describes the activities carried out by the service provider to monitor the behaviour of the car or the user of the car service. In this scenario, we present three (3) actors: the *Car*, *User* and the *Service Provider*, as explained in Section 3.3.4.

The process begins a user begins when the car-sharing service (see A5.1). The Service provider wants to know how users behave while using the sharing service. The car collects the *real-time information (D7)* details (see A5.2) of the user. It sends the *real-time information (D7)* to the service provider for them to monitor the behaviour (see A5.4). This information could include the car's location, the status of the driven car,

and the user's image being captured on camera to ascertain misbehaviour. The Service Provider revokes the car usage when it notices misbehaviour during the car-sharing service and sends the signal to the user who uses their service.

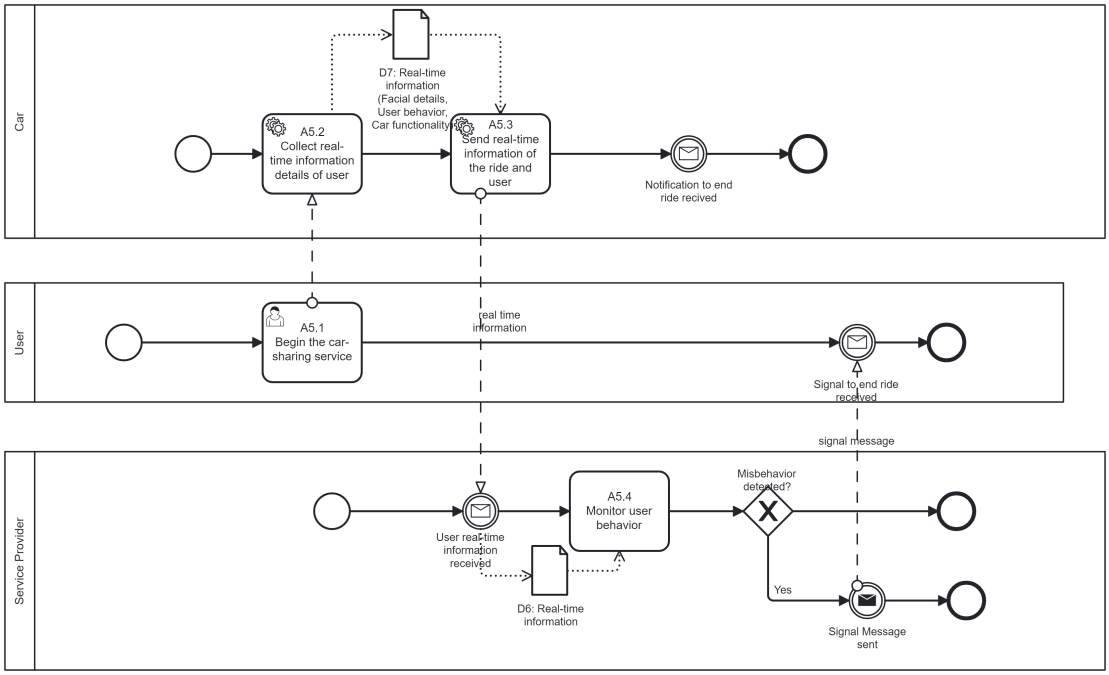

Figure 9. This Model Shows the Processes of the User Behaviour Scenario (**M5**)

3.3.6 Payment Model

Figure 10 presents the scenario of the Payment Model (M5) process, which depicts the User's processes to pay for the service after using the car-sharing service. The actors involved in this Scenario are the *Service Provider*, *User* and the *Payment Provider*. The Payment Provider is an actor who manages the payment process. The process starts when the User notifies the service provider that the ride has ended. The *Service provider* provides the price (see A6.1) for the ride to the User who in turn Enters *Payment Details (D8)* (see A6.2), such as User's information, Credit Card or Debit Card information, authorisation to proceed with payment. The Payment provider who manages the payment process validates the *Payment Details (D8)* provided by the User (see A6.3) and sends the specific payment to the Service provider. The Service provider confirms the receipt of the payment made and sends a payment confirmation (see A6.4) to the User.

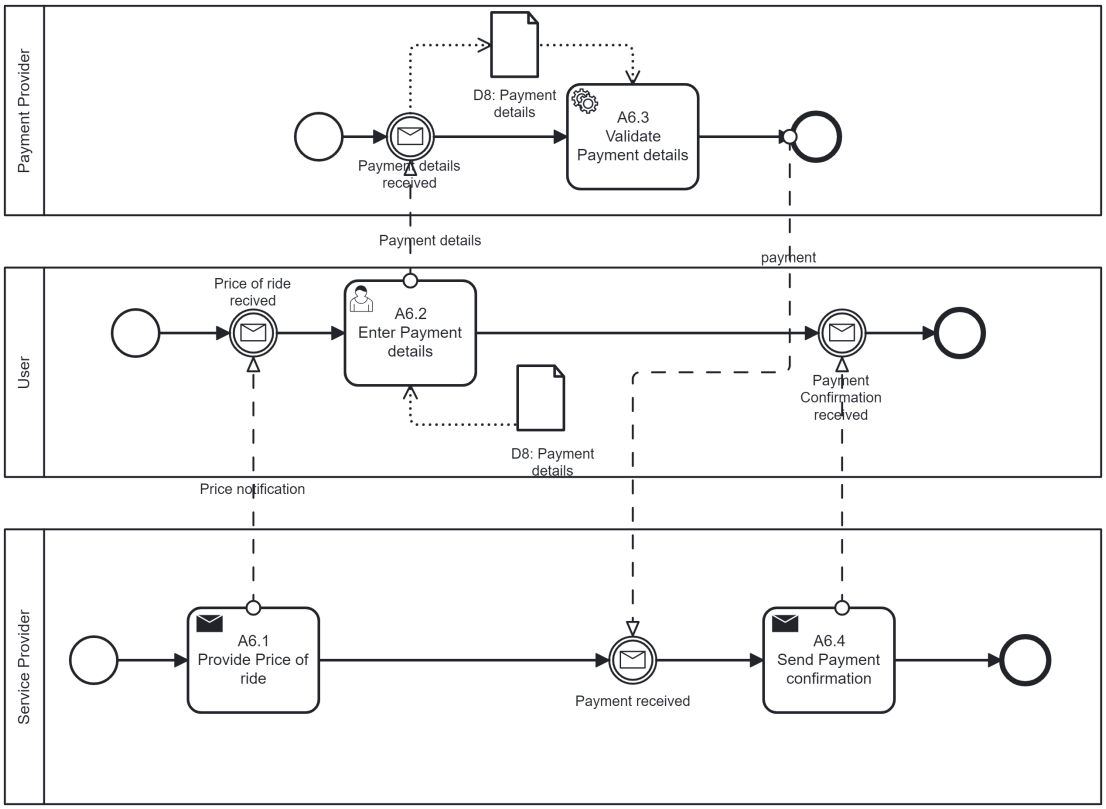

Figure 10. This Model Shows the Processes of the Payment Scenario (**M6**)

3.4 Answer to Research Questions

In this section, we intend to answer **[RQ1:] What is the context of the car-sharing system?** by providing answers to the sub-questions respectively.

RQ1.1: What are the main processes of the car-sharing system? The processes of car-sharing give insight into the main processes that make up car-sharing operations. We identified six key processes, namely, ***User registration, User verification, Booking process, Car access, User behaviour and Payment process***. User registration occurs when a person intending to use a car service provides vital information, such as their details, to sign up for the service. Users are verified to ascertain that an authorised user gains access to proceed with making a booking for the service. In booking, the service provider lists cars to select from, and the service providers receive notification of the usage intent through user requests. Upon booking, users can access the car through physical keys, mobile phones, and other related sources of communication. In most cases, during the ride, the lending company decides to monitor the user's interaction with the car, and this process is captured and sent to the lending company throughout the

renting period. Users pay for the service at the end of using the rental service.

RQ1.2: What are the concepts and terms of the car-sharing system? The concepts defined the various perspectives from which the multiple actors perceive the car-sharing process. More so, we elicited the different terminologies used to understand car-sharing concepts. For example, in this case, some papers were about the renter or driver who intended to use the service. However, the term *User*, in our case, describes the mobile phone or portable device used to carry out the operations. In some cases, the *service provider* is the vehicle owner, and in other cases, the car-sharing company is responsible for renting out their cars for a short period. In the *Server* or *Database*, all information shared within the process is stored and retrieved when needed. The *identity provider* acts as the identity manager to improve user trust in the system. They can be the trusted authority or the IDP to manage the authentication and verification process. The *car* used for the sharing service relates to various communication protocols such as BLE, NFC, On-board Unit (OBU), and sensors that facilitate communication and data exchange between the user, service provider, and the car.

RQ1.3: How can the processes of car-sharing be used to identify the assets of the system? The answer to this research question is expanded from RQ1.1. As a result, we look into ascertaining the business operations using BPMN. We identified the assets that need protection from risks to ensure secure service usage. The assets include the ***Identity details (D1)***, which cover the personal information a user sends to register with the system. The ***Login Credentials (D2)*** of the user, which enables the user to log on to perform the sharing operation. The ***Random Number (D3)*****,** which is sent by the Identity provider to authenticate a user for the service,. A user sends the booking details (D4) and receives reservation details (D5) for a successful booking. Accessing the car can only be done when the ***Car access token (D6)*** matches the available token from the service provider and the car. During the service, the ***real-time information D7*** of the user and the car is used to monitor the interaction throughout the service. Afterwards, the user provides the *payment details(D8)* to make payments using the payment provider's gateway.

4 Assets in Car sharing Scenarios

In this section, we answer our research question, ***RQ2: What are the protected assets in car-sharing scenarios?***. To address this question, we have further broken down the question into sub-questions to clarify our results. 1. What are the business assets? 2. What are the system assets? 3. What are the security needs for the assets? We will apply the Security Risk Management concept to provide a systematic approach to answering these questions. Furthermore, we present the assets that are vulnerable to risks and the security needs of the assets.

4.1 Assets-Identification

This subsection introduces the answers to the sub-research questions on what assets are vulnerable to attacks. The assets are the business and system assets, which need security for securing information. Identifying these assets is vital in the car-sharing sector, as they are critical assets that could lead to an attack on the car-sharing system.

4.1.1 Business Assets of the Car-sharing System

Business assets are valuable information that adds value to an organisation's business process to achieve its specific needs. From the car-sharing process models presented in Section 3.3, we extract the business assets ranging from essential ***Identity Details(D1)*** and ***login Credentials(D2)*** to more intricate assets such as ***Random numbers(D3)***, ***Booking Details(D4)***, ***Reservation Details (D5)***, and ***Car access tokens(D6)*** and also the information shared between actors that deals with the behaviour of the user while using the sharing service ***(Real-time Information(D7))***. To complete a payment process successfully, ***(Payment Details(D8))*** is shared by the user to make payments for the car-sharing service, as shown in Figure 10 (see A6.2 and A6.3). These assets collectively serve as the vital business assets of the car-sharing system that facilitate the information, processes, capabilities, and skills [17] essential in the car-sharing process.

4.1.2 System Assets of the Car-sharing system

In [17], Matulevicius defines system assets as a component that supports the business asset. The system assets support the business processes, the information gathered and transferred from one system to another, and how this information is stored to optimise the business processes. We followed the classification of the usage of information technologies in [17]. We classified the system assets based on their functions to support the car-sharing business assets. This function describes the *Information Processing Functions*.

The *Information processing functions* deal with how this information, in this case the business assets, are captured, transmitted, stored, retrieved, and displayed during the operations. We present in Tables 8-13 the various assets of the car-sharing system and their security needs for protecting these assets.

Table 8. Assets Identification for the Protected Assets of M1

Information Processing Functions	**System Asset**	**Business Asset**
Capturing Information	**A1.1:** User enters personal Identity details	**D1.** Identity Details (CIA)
Transmitting Information	1. From User to Identity Provider: Identity Details received 2. From Identity provider to User: Login Credentials received	I. **D1:**Identity Details (CIA) II. **D2:** Login Credentials (CIA)
Manipulating Information	**A1.2:** Identity Provider manages Identity details	**D1:** Identity Details (CIA)
Storing Information	1. **A1.3:** Identity Provider stores Identity Details 2. **A1.4:** Identity Provider stores Login Credentials	I. **D1:**Identity Details (CIA) II. **D2:** Login Credentials (CIA)

Table 8 presented in this context illustrates the system assets of a car-sharing system and their support for business assets. The mapping of these system assets against security criteria, based on the Confidentiality, Integrity, and Availability (CIA) triad, is also depicted in the table. One of the system assets, specifically in A1.1, involves the user's entry of personal *identity details*, which corresponds to business assets, including driver's licence, citizen ID, and biometric data. This system asset is primarily concerned with confidentiality within the CIA triad, as it contains sensitive personal information that needs protection from unauthorised access and disclosure.

Another system asset in A1.2 involves the management of identity details by the **Identity Provider**. This asset is critical to maintaining integrity, as it requires the proper processing and validation of user data to ensure the accuracy and consistency of the identity details stored in the system. It is worth noting that the appropriate management of identity details is essential in preventing identity theft and fraud, which can compromise the security of the car-sharing system and its users.

The Identity Provider "**Store Identity Details**" and "**Store Login credentials**" to support the associated business assets *Identity Details* (D1) and *Login Credentials* (D2), respectively, and are critical for ensuring user data integrity, availability, and confidentiality. It ensures that the information is kept correctly, without alteration, and readily available.

Table 9. Assets Identification of the Protected Assets of M2

Information Processing Functions	**System Asset**	**Business Asset**
Capturing Information	**A2.1:** User provides Login Credentials **A2.3:** Service Provider sends a Random number to the user **A2.4:** User enters Random number	**D2:** Login Credentials (CIA) **D3:** Random Number (CI)
Transmitting Information	1. From Identity Provider: Login Credentials received 2. From Identity provider to Service Provider: Random number received 3. From Service Provider to User: Random number received. 4. From Service Provider to Identity Provider: Random number received.	**D2:** Login Credentials (CIA) **D3:** Random Number (CI)
Manipulating Information	**A2.2:** Identity Provider generates Random number **A2.5:** Service Provider validates Random number **A2.6:** Identity Provider validates Random number	**D3:** Random number (CI)

Table 9 details the process through which information is captured (A2.1: *User* provides Login credentials), transmitted (A2.3: *Service provider* sends Random number to User), and manipulated (A2.5: *Service Provider* validates Random number), Each of these system assets supports business assets **D2** and **D3**, respectively. The *login credentials* should be so confidential that an attacker should have no access to the information; the information should not be altered by a third party, thereby upholding the integrity of the data; and the login credentials should be available.

Table 10 presents the information processing functions for the booking process in a car-sharing system. It explains the information capture process (A3.3: User enters booking data), which is related to the business asset booking details (D4), which emphasises that the booking details should not negate the integrity and availability (IA) of the data provided by the user. The transmission and processing of booking information include user requests, service provider receipts, and booking validation and confirmation, which are D4 and D5, with Integrity and Availability as its security criteria. Furthermore, the *Service Provider* oversees delivering the car's Geo-location and keeping reservation information, ensuring data accuracy and accessibility throughout the booking process.

Table 11 presents the system assets A4.1, where the *user* sends a request to access the car, and A4.2, where the *service provider* issues an access token (D6. Car access token). It also addresses the delivery of the access token to the user (A4.3) and the car's

Table 10. Assets Identification for the Protected Assets of M3

Information Processing Functions	**System Asset**	**Business Asset**
Capturing Information	**A3.3:** User enters booking details	**D4.**Booking details (IA)
Transmitting Information	1. From User to Service Provider: Booking request made 2. From Service Provider to User: Booking request received	
Manipulating Information	**A3.4:** Service Provider validates booking details **A3.5:** Service Provider confirms booking **A3.6:** Service Provider provides Geolocation of car	**D4:** Booking details (AI) **D5:** Reservation details (IA)
Storing Information	**A3.5:** Service Provider stores reservation details	**D5:** Reservation details (IA)

validation of this token (A4.4). Finally, it describes the car's notification to unlock (A4.5). This system asset supports granting access to the car using the *Car access token* (D6). The assets maintain the CIA criterion of the security triad. (See table 9)

Table 12 describes the different activities from Fig. 9 on how the *car* collects and sends real-time information (A5.2 and A5.3) to the *service provider*. The information is vital for monitoring the user's behaviour during the ride (A5.4) and communicating with the user, such as signalling the end of the ride (manipulating information). These activities are associated with business asset *Real-time Information* (D7) and emphasise the confidentiality and integrity (CI) of the data collected during the ride. The information collected can be shared by third parties concerning how a user's behaviour goes during the ride. In a scenario where an unknown party intercepts this asset, it could lead to data loss and mistrust from the customer perspective [16]. The negation of the confidentiality of how a user behaves should be protected by the Service Provider, especially during the transfer of the information from the Car to the Service Provider.

Table 11. Assets Identification for the Protected Assets of M4

Information Processing Functions	**System Asset**	**Business Asset**
Capturing Information	**A4.1:** User sends request to access the car **A4.3:** User sends Access token to car	- **D6** Car access Token (CIA)
Transmitting Information	1. From User to Service Provider: Car access request received 2. From Service Provider to User: Car access token received 3. From User to Service Provider: Car access token received 4. From Car to Service Provider: unlock car notification received. 4. From Service Provider to car: Car access request granted	- **D6** Car access Token (CIA)
Manipulating Information	**A4.2:** Service Provider provides Car access token **A4.4:** Car validates access token provided **A4.5:** Car sends notification to unlock car	**D6:** Car access token (CIA)

Table 12. Assets Identification for the Protected Assets of M5

Information Processing Functions	**System Asset**	**Business Asset**
Capturing Information	**A5.2:** Car collects real-time information details of user	**D7:** Real-time Information (CI)
Transmitting Information	1. From Car to Service Provider: Real-time information received 2. From Service Provider to User: Signal to end ride received	**D7:** Real-time Information (CI)
Manipulating Information	**A5.3:** Car sends real-time information of the ride and user to service Provider **A5.4:** Service Provider monitors the user behaviour	**D7:** Real-time Information (CI)

Table 13 describes how the *service provider* communicates the ride's price (A6.1) and how users provide payment details (A6.2). It also specifies the payment provider's role in confirming these payment details (A6.3) and the service provider's responsibility for delivering payment confirmations (A6.4). Each process is associated with business asset

Table 13. Assets Identification for the Protected Assets of M6

Information Processing Functions	**System Asset**	**Business Asset**
Capturing Information	**A6.1:** Service Provider provides the price of ride **A6.2:** User enters payment details	**D8:** Payment Details (CIA)
Transmitting Information	1. From Service Provider to User: Price of ride received 2. From User to Payment Provider: Payment details received 3. From Payment Provider to Service Provider: payment received 4. From Service Provider to User: Payment confirmation received	**D8:** Payment details (CIA)
Manipulating Information	**A6.3:** Payment Provider validates payment details **A6.4:** Service Provider sends payment confirmation	**D8:** Payment details (CIA)

Payment Details (D8). The information's confidentiality, integrity, and availability ensure that car-sharing transactions are secure and efficient. From the table, the supporting assets for the process to run efficiently are the *Service provider*, which provides the cost of the trip, and the *Payment Provider*, which is a third party that validates the payment details(D8) obtained from the *User*.

4.1.3 The Security Need

In answering RQ2.3, we defined the security needs, which are the security constraints that apply to the business assets. The business assets presented in Table 8 entail different security criteria needed to negate the impact of a risk of the car-sharing assets.

1. **Confidentiality**: The business assets presented in **RQ 2.1** such as the *Identity Details*, *Login credentials*, *Random number*, the *car access token*, *real-time information* and *payment details* of the user are kept private and undisclosed to third parties to prevent unauthorised access to information by an intruder or attacker. This means that information is not made available or disclosed to authorised individuals, entities, or processes [17].

2. **Integrity**: The accuracy and completeness of the business assets (D1–D9) are essential. We must ensure that no part of the information is tampered with or altered from within the process or an unauthorised source. The authenticity of

private data shared during car-sharing should be kept and maintained. Also, the car access token shared with the user is not to be updated or tampered with, as this could cause harm to the protected assets.

3. **Availability**: The assets must be available when required. For example, the *identity details* of a user should be available and usable to the service provider for them to process the registration of a user into the car-sharing app. The assets that are made available should be for only authorised entity usage. Once a protected asset is tampered with, it may disrupt the entire process of the car-sharing system.

4.2 Answer to Research Question

In this section, we provide the answer to **[RQ2:] What are the protected assets in car-sharing scenarios?** We provide the findings by answering the sub-questions.

RQ2.1: What are the business assets? The business assets are the vital information shared across the car-sharing scenario between the different entities. The results present us with eight (8) assets to be protected. These assets are needed in 24 cases within the scenario, forming a crucial part of the business operations. Hence, they need to be protected. **RQ2.2:What are the system assets?** From the results presented, the supporting assets include the User, Service Provider, Identity Provider, Car, Database, and Payment Provider. These six assets support the process by providing various information processing functions. **RQ2.3: What are the security needs for the assets?** The assets' confidentiality, integrity and availability are crucial to protecting them from attacks. The Identity Details, Login Details, Car access Token and Payment Details cover all the principles (CIA). In contrast, the Booking Details and the Reservation details cover the integrity and availability of the information. The Real-time Information captures the confidentiality and integrity of the user's behaviour.

4.3 Summary

In this section, we answer our research question **RQ2** by first identifying the protected assets of scenarios. These assets are business assets, such as the user's identity information used during the registration stage and the user's login credentials for the user verification process. The data captured, transmitted, manipulated, stored, or displayed while using the service. To identify the security risks, we understand that parts of these processes are vulnerable, as these assets form a comprehensive architecture that aids the operationality of the car-sharing service. Furthermore, we applied the security needs, which are confidentiality, integrity, and availability, to understand the part of the need that a risk could negate.

5 Security Risk and Risk Reduction

This section addresses the research question, ***RQ 3: What are security risks and their reduction approaches in car sharing scenarios?***. We divided it into two sub-questions. 1. What are the security risks? 2. What are the reduction approaches? We shall derive the threat model using the STRIDE model approach to capture the various risks in the scenarios. Furthermore, these risks are annotated into the car-sharing models to capture the places where a particular risk exists. To further understand the type of risks, we presented a security risk analysis of each risk and provided reduction methods.

5.1 Risk-Related Concepts

Risk: To understand the concept of **risk**, the risk-related concepts define risk itself and its immediate components [17]. We addressed the *risk*, which comprises of the *threat* and *vulnerabilities* that could lead to a negative *impact* on an asset; thus, a combination of threat and vulnerability constitutes the type of risk event and its impact. The *impact* associated with a risk negates the security need of the business assets presented in Sect. 4.1.3 (lack of confidentiality of the information, lack of integrity of the information, and non-availability of the information). They can harm the assets, thereby disrupting the organisation's business activities. Thus, before a *risk event* takes place, there must exist a *threat* and one or more *vulnerabilities*. A *threat* exploits the vulnerability of the system asset, and it begins with a *threat agent* who utilises different attack methods to execute the threat.

5.1.1 Threat Model for Car-sharing

Threat modelling gives a concrete guide that every asset in a system is prone to risk and is used to identify threats in a system [22]. To define the threat model, we considered first the threats within the car-sharing system by mapping the risks to each paper (see Appendix 3). We elicited the potential attacks that each paper addressed and determined in what part of the activity the attack happened. The various attacks on the system were further mapped into the scenarios (See Fig.11 – 16). Defining the threat model is one of the first steps in information security for identifying risks. Furthermore, we implemented the STRIDE approach for threat modelling. The threat model depicts 14 threats described by the various authors that an attacker can exploit during the sharing service. For this thesis, we shall further analyse eight (8) of these during the security risk analysis.

STRIDE: This approach is used to identify the threats in the system, categorised into *Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service and Elevation of Privilege*. [1]

[1]To further understand the Microsoft STRIDE modelling framework [25]

Table 14. Threat Modelling using the STRIDE Approach

	S	T	R	I	D	E
Paper						
Fengkuan cao *et al.*	**SR1: Phishing**	**TR1: Sever Leakage**	**RR1: Unauthorized Access Denial**	**IR1: Man-in-the-middle attack**	**DR1: Dos attack**	-
Yinan Ma *et al.*	**SR2: Impersonation attack**	-	-	-	-	-
Sophia Auer *et al.*	-	**TR2: Data Silos**	-	-	-	-
Viktor Valaštín *et al.*	-	-	-	-	**DR1: Dos attack**	-
Francesco Pollicino *et al.*	-	-	-	**IR2: Information Extraction**	-	-
M. Safdar *et al.*	**SR2: Impersonation attack**	-	-	-	-	-
Iraklis Symeonidis *et al.*	-**TR5: Data Tampering**	-	-	**IR1: Man-in-the-middle attack**	-	-
Zhuo Wei *et al.*	-	-	-	-	**DR1: Dos attack**	-
Petr Dzurenda *et al.*	-	**TR5: Data Tampering**	-	-	-	-
J. Arm *et al.*	-	**TR4: Replay attack**	-	**IR3: Mobile intrusion attack**	-	**ER1: Authentication Bypass**
Qihao Zhou *et al.*	-	**TR3: Illegal intrusion of servers**	-	-	-	-
Myeonghyun Kim *et al.*	-	**TR4: Replay attack**	-	**IR1: Man-in-the-middle attack**	-	-

5.1.2 Risk Scenarios

Considering the model scenarios in Section 3.3, the identified threats in the literature were mapped to the STRIDE model (see Table 14). We found a total risk in the scenarios in 33 places where each risk captures the places where the risk is potentially affecting the assets. It is also pertinent to note that, for some processes, we can identify more than one risk occurring in that process even when not captured in the literature.

The user registration process activities were mapped with the following risks;

- ◇ R1: Man-in-the-middle attack
- ◇ R2: Impersonation attack
- ◇ R3: Tampering data
- ◇ R4: Information Disclosure
- ◇ R5: Server Leakage
- ◇ R6: Phishing attack

In the Man-in-the-Middle attack (R1), the attack agent listens to the entire communication process between when the user provides *Identity details* to *Identity Provider*, thereby disclosing information to a third party. The *Identity details* is tampered with by an adversary [5]. The impersonation attack (R2) threat occurs when the attacker monitors and pretends to be the owner of the *Identity details* of the user [5]. Auer *et al.* [2] indicate in their work that when there is a single point of data in a centralised server when the *Identity Provider* sends a unique digital identity to *user*, it could result in a server leakage (R5) as there would be a lack of communication between the identity provider and the service provider. When users download the car-sharing app, they may be unaware of the information disclosed to the company. An example could be granting internet permission when installing and running the app. During this process, the adversary steals the user's information in such cases.

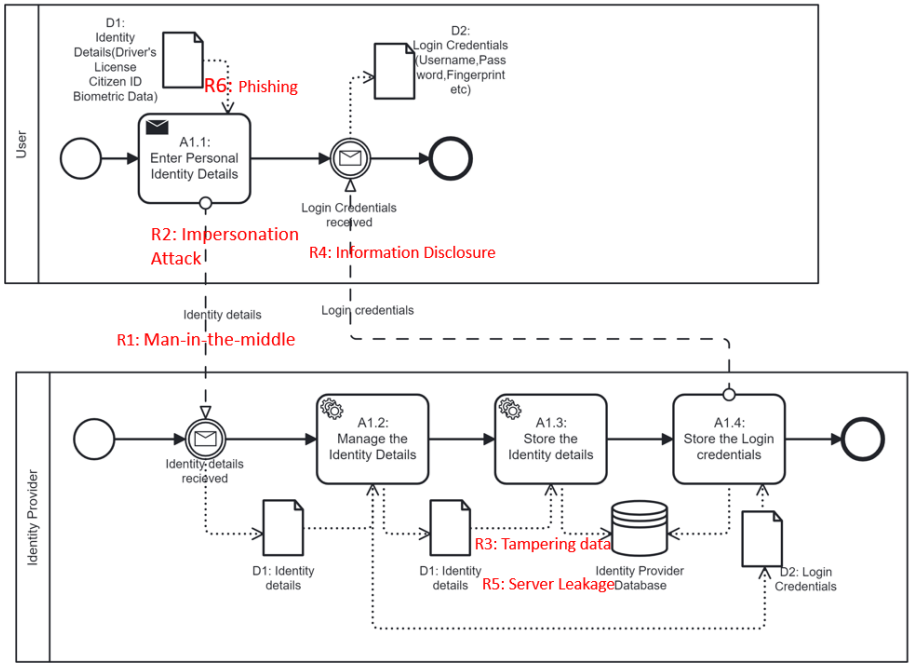

Figure 11. Risk Model of the User Registration Process

The verification of user scenarios in various papers presents the following risks:

◇ R1: Man-in-the-middle attack

◇ R2: Impersonation attack

◇ R3: Tampering data

◇ R7: Phishing attack

Zhou *et al.* [32] opined that the R1 occurs when the car owner provides the user with a digital sharing key. The attacker can obtain the session key while transferring it to the user. Cao *et al.*[5] also illustrated that a man-in-the-middle attack (R1) can take place when the server generates the *random number* and sends it to the user as the attacker listens to the entire communication process. In [13], the phishing attack (R6) can occur when the attacker acts like the service provider lures the user to provide their personal information. The user believes the message comes from the identity provider or car owner. An attacker accesses the user's credentials to access the car-sharing service.

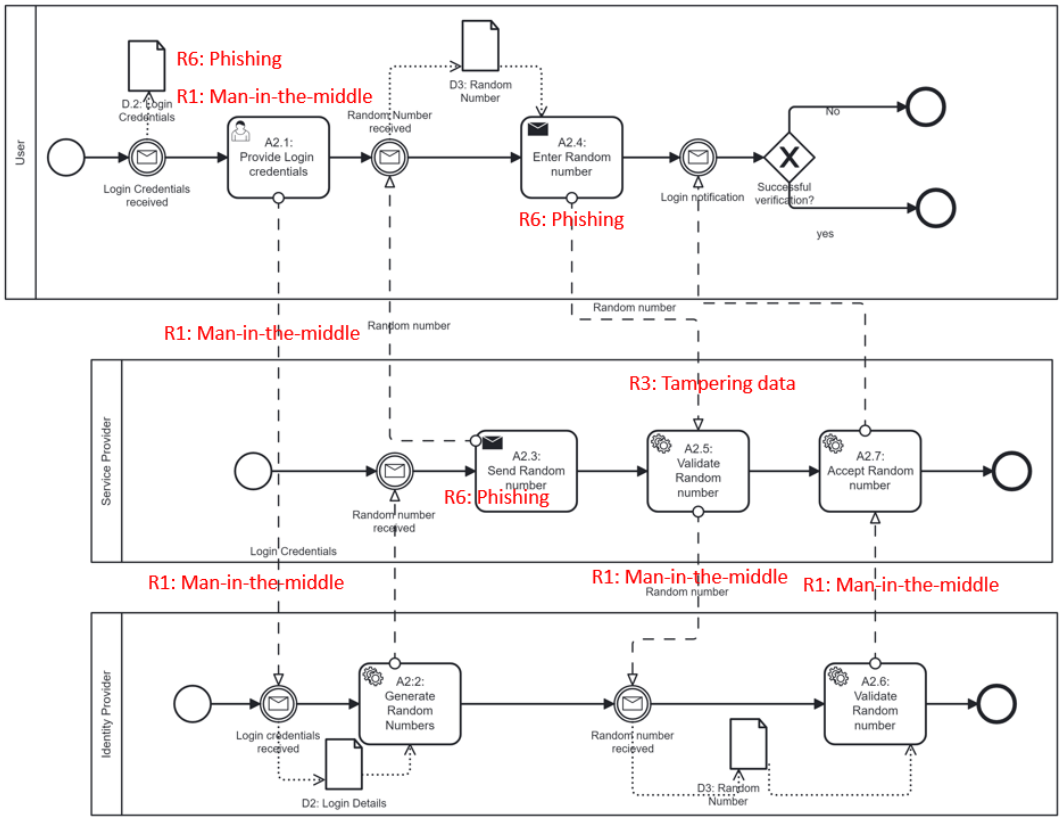

Figure 12. Risk Model of the User Verification Process

The booking process by various concepts presented the following types of risks:

- ◇ R1: Man-in-the-middle attack
- ◇ R3: Tampering data
- ◇ R5: Server Leakage
- ◇ R6: Phishing attack
- ◇ R8: Denial of Service (DOS) attack

The tampering data attack (R3) can be a result of server leakage; thus, an adversary can tamper with the user data stored in the *database* of the *service provider*, such as by modifying the booking details of the user [24]. Phishing attacks (R6), according to [1, 2, 23, 29], can occur in the process when the user submits their booking details and credentials. Due to a single entry point on a centralised server, an attack agent can perpetrate a denial of service attack (R7) such that the whole booking system service is

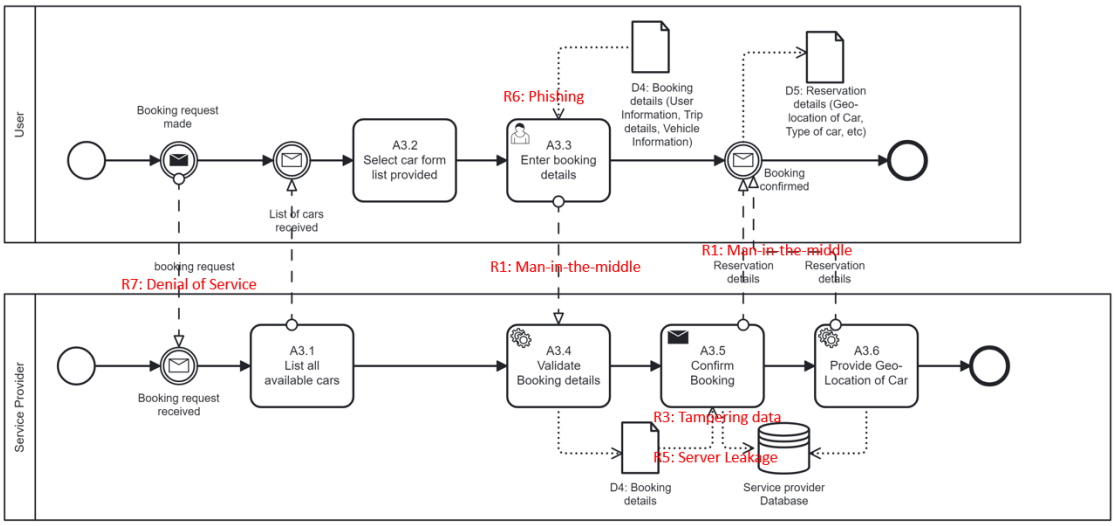

Figure 13. Risk Model of the Booking Process

unavailable, and a user cannot make a booking.

The car access activities described in Table 28 by the various authors elicit the following types of risks in the car access process.

- ◇ R1: Man-in-the-middle attack
- ◇ R2: Tampering of data
- ◇ R7: Denial of Service (DOS) attack
- ◇ R8: Unauthorised access denial

The process begins with a user request for vehicle access, which transitions into the service provider issuing a car access token. This token is pivotal for the user's authentication by the car's system. However, there exists a critical vulnerability to Man-in-the-middle attacks (R1), where an unauthorised intermediary could intercept the **car access token**(D6). Additionally, the token's integrity is at risk of being compromised through tampering data (R3) and the possibility of unauthorised modifications that could either grant access to illegitimate users or deny it to legitimate ones. The Denial of Service (R7) could hinder the system, preventing users from accessing the vehicle services. Lastly, Unauthorised access(R8) indicates the threat of access breach without proper authentication.

In Fig. 15, it is indicated that there is a potential risk associated with the disclosure of sensitive or personal real-time information collected during the car-sharing service at different points of the service. Information disclosure attack (R4) is a recurring risk in the

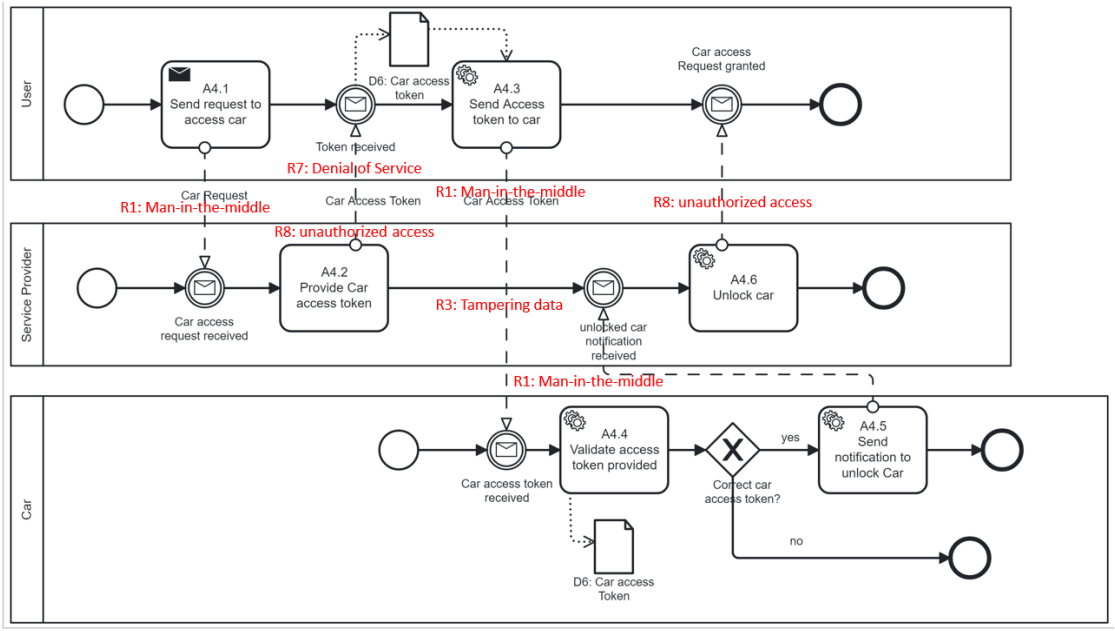

Figure 14. Risk Model of the Car Access Process

model. When the car collects the user's real-time information details (A5.2), an attacker can gain unauthorised access to this information and make alterations and manipulations to the information collected. Such attacks of disclosure of real-time information about a user's behaviour lead to a lack of protection of the user's privacy and tracking and profiling of the user by the attacker [23] an acknowledgement of the privacy concerns of the user's behaviour inherent in car-sharing services is relevant, as such systems, when faced with high vulnerabilities, may pose an attack on the disclosure of the real-time behaviour of the user concerning data protection standards.

In the Risk model shown in Fig. 16, the payment activities captured the risk of MitM. Man-in-the-middle attack(R1) pertains to the potential interception of payment details by an unauthorised entity during the transmission between the user, the service provider, and the payment processor. During the payment process, the attacker could potentially capture sensitive information, *payment details* (D8), such as credit card details and personal identification numbers. The risk occurs due to the multiple data transfer points: from the user submitting payment details to the service provider receiving and validating these details, and finally, to the payment confirmation. However, based on the literature, only this risk was ascribed to the payment process, although more risks could exist.

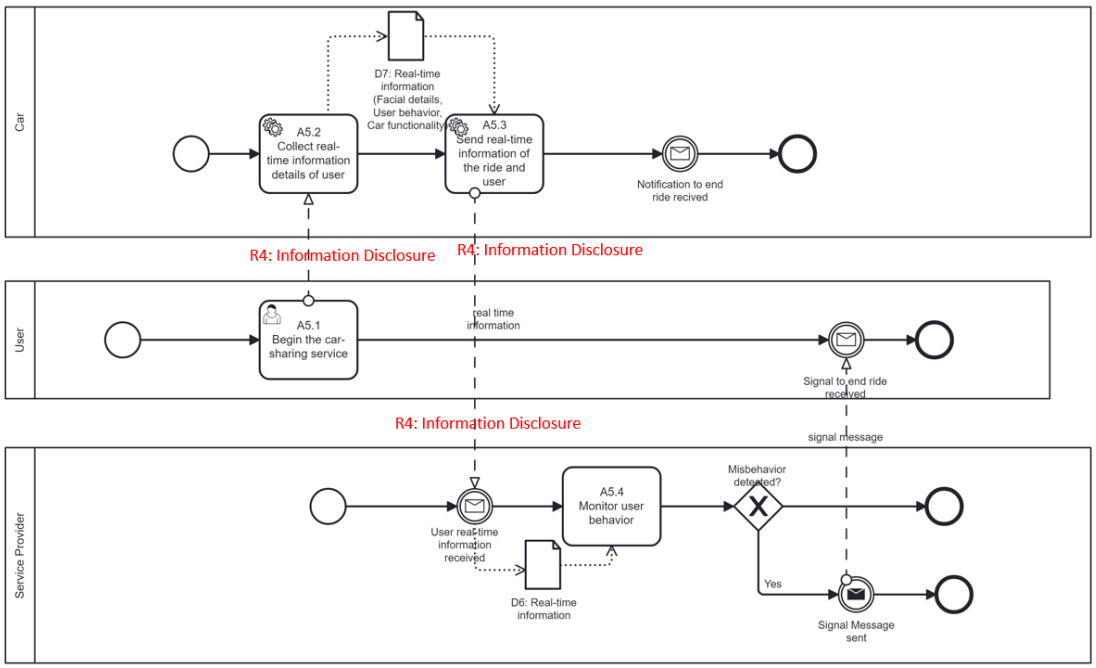

Figure 15. Risk Model Scenario of User Behaviour

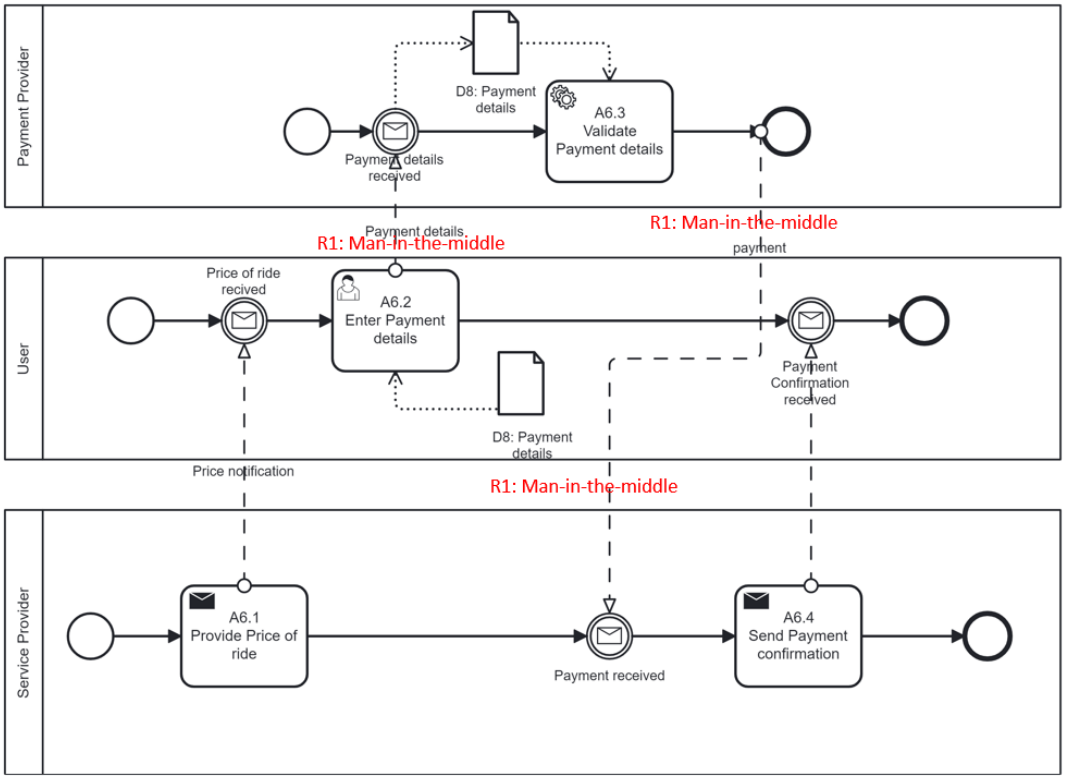

Figure 16. Risk Model Scenario of the Payment Process

5.2 Security Risk Analysis

This section will analyse the security risks these car-sharing scenarios face. Using the STRIDE approach presented in Table 14, we mapped the various threats from the previous section and identified the places where these risks exist using the scenario models. To perform the risk assessment, we examined the system asset to define which business asset the system supports, the system's vulnerability, the impact of the risks obtained on the system asset and business asset, and the security criteria negated in the business asset. In the Threat modelling (See Table 14), we identified 14 threats. These threats include threats found from literature sources and described by the authors as threats to car sharing. Among the 14 threats found, eight were modelled in the scenario targeting the business assets of the system. (See Fig. 11-16).

In the risks derived from the model, six risks were targeting the *Identity details*(D1), four risks were targeting the *Login credentials*(D2), five risks were targeting the *booking details*(D4) and *reservation details*(D5), three risks targeted the *Random number*(D3) used for verification of the user, four risks were targeting the car access token (D6) and one risk each targeting the *real-time information*(D7) and *payment details*(D8) asset. During the analysis, the **Man-in-the-Middle attack (IR1)** appeared in seven (7) positions in the risk models targeting the *Identity details*(D1), *Login credentials* (D2), *random number*(D3), *booking details*(D4), *reservation details* (D5), the car access token (D6) and the *payment details*(D8).

According to [6], in the **Man-in-the Middle (IR1)** attack, an adversary inserts himself into a discussion between a user and an application to eavesdrop on or impersonate one of the parties, thus making it appear that a regular exchange of information is taking place. For an attacker to perform this action, the attack agent needs medium-level expertise, such as understanding network and communication protocols, to penetrate the system. This risk negates the confidentiality, integrity and availability of the business assets (**D1, D2, D6 and D8**), negates the privacy and integrity of the random number (**D3**) used for the verification of user in the system and finally negates integrity and availability at **D4** and **D5**. The impact of this attack on the business asset is the compromise of the information between system assets of the car-sharing system. Furthermore, the risks were analysed, describing the vulnerabilities of assets, the threat agent, and the method of the threat. Also, describe the impact of each risk on the assets. (See Table 15-19.).

Phishing (SR6): This risk depicts how attackers can obtain user authentication information by posing as a reputable user. The threat model illustrates that in car-sharing Scenario M1 and M2, the attacker can steal the *identity details*(D1) and *Login Credentials* (D2) of the user acting as a legitimate service provider. It also addresses the negation of the confidentiality and integrity of the business assets D1 and D2.

Impersonation Attack (SR2): This risk describes how an attacker can appear to be an authorised user of an application. It illustrates how attackers might pose as legitimate users, exploiting weaknesses in authentication methods. The vulnerability of weak

Table 15. Spoofing Security Risk Analysis of the Car-Sharing System

Threat Type	**Vulnerabilities**	**Threat**		**Impact**
		Threat Agent	Attack Method	
1. **SR6: Phishing:** An attacker gets access to the information of a user by masquerading as a legitimate entity to lure user into revealing their information	Weak authentication method	**Expertise:** Attacker has the technical knowledge with authentication procedures and uses a wide variety of actions to lure user deceptively. Basic knowledge about websites: obtaining them, designing and implementing them.	An attacker can send deceptive emails to users to lure them and gain access to their identity details or Login credentials.	1. **Impact on System Asset:** Communication protocol unreliability and untrustworthiness between User. The attacker gains the Identity Provider and Service Provider privileges at **M1, M2, and M3**. 2. **Impact on Business Asset:** The user's identity details (D1) is stolen, and the attacker can impersonate the user. The User's login credentials have been stolen. 3. **Negation of Security Criteria:** Negation of C and I at **D1** and **D2**
2. **SR2: Impersonation Attack:** An attacker pretends to be the user and impersonates the legitimate user of the application	i. Weak username and password (A threat agent can easily guess login credentials) ii. Generation of Incorrect Security Tokens by Identity Provider	Capability: The attacker acquires the user identity details and can manipulate the sharing service, acting like the user.	i. The attacker attempts to impersonate a legitimate user by securing false ID information and generating an authentication message.	1. **Impact on System Asset:** In **M1** and **M2**, there is a communication protocol unreliability between **User** and **Identity Provider** as attacker can impersonate user and steal the Identity details(D1) data. 2. **Impact on Business Asset:** The **identity details (D1)** of the user is stolen, and the user can be impersonated. **Login Credentials (D2)** of User is stolen. 3. **Negation of Security Criteria:** Negation of C and I at **D1**, Negation of C and I at **D2**

authentication gives attackers the possibility of guessing login details or generating incorrect security tokens. This risk negates the confidentiality and integrity of D1 and D2.

Server Leakage (TR5): This risk illustrates the vulnerabilities related to a single point of entry in servers and centralised data management [5]. The threat agent, who knows server architecture, can breach servers to steal or manipulate sensitive user data, impacting both *identity details* (D1) and *login credentials* (D2), resulting in a lack of integrity of the user's data. This negates the confidentiality and integrity of D1 and D2 in M1 and the integrity of D4 and D5 in M3. (See Fig.11 and 13).

Unauthorised Access (RR8): When access to an asset, such as an unauthorised service user, is perpetrating the car, it leads to session hijacking. The adversary explores the authentication flaws and takes control of the user account, thereby compromising the communication session between the *Service Provider* and the *User*. This risk negates the confidentiality, integrity and availability of the *Car access token* which the Service Provider provides to the Service user. (See Table 17)

Information Disclosure (IR4): The risk describes when an adversary gains access to sensitive data, which could lead to a data breach in the car-sharing system. The inefficiency of the database or server could lead to a third party eavesdropping on the transferred data. Also, when there is a lack of data anonymisation, the adversary could read the breached data and thus misuse the information stolen. For the adversary to be able to carry out this operation, it must understand the system, architecture, and server management. It can perform SQL injection attacks on the database or exploit the server configurations. This type of attack leads to a lack of trustworthiness in the system due to a compromise of the data of the *User* Thus, it negates the confidentiality of the information captured or transferred. (see Table 18)

5.3 Security Risk Reduction

In providing a risk reduction strategy, risk reduction reduces the potential for harmful threats to affect a system. The approach reduces the adverse effects of threats and uncertainties in a system. The existing studies from SLR discuss how to mitigate security risks by exploring ways to reduce the impact of the risk on the sharing scenario. We have used the existing literature to develop the risk treatment plan. From the ISSRM domain model, we describe how to treat risk by satisfying the security requirements and implementing them as controls or countermeasures to improve the system's security. Hence, based on this, we further refined the security requirements and the control measures to reduce the risk of occurrence.

Security Requirement and Control: In defining security requirements, there are several conditions to fulfil to mitigate the risks of the protected assets of a system [17]. Security requirements ensure that users are authorised to access data in the system while protecting the system from attacks or access by unauthorised persons [17]. [9]

Table 16. Tampering Security Risk Analysis of the Car-Sharing System

Threat Type	**Vulnerabilities**	**Threat**		**Impact**
		Threat Agent	Attack Method	
1.**TR5:Server Leakage attack**	Single point of entry servers and centralised servers depending on a central node to manage data and operate the system	**Expertise:** Attacker has knowledge of server architecture and understands where sensitive data of the user is stored. ii. Attacker can intercept, modify, forge and delete data or messages transmitted in the service	i. The attacker breaches the server and attempts to steal the user's information stored in the identity provider and service provider databases. ii. Attacker uses SQL injection to bypass the application	1. **Impact on System Asset:** lack of integrity on the data stored in the server as the attacker. 2. **Impact on Business Asset:** From **M1, D1** and **D2** and from **M3, D4** and **D5** stored in the server are breached and opened to attack by the attacker as the attacker misuses the data stored. 3. **Negation of Security Criteria:** Negation of C and I at **D1, D2,** Negation of I at **D4** and **D5**
2.**TR3:Tampering Data:**	exploits the centralised point of entry into the system and the verification of the user and car	**Expertise:** Attacker understands database manipulation and has an idea about the infrastructure of the system. **Capability:** An attacker intentionally modifies the **Identity details**, **Booking details**, **car access token** and tampers with the **Random number** sent by the user to the Service provider to manipulate the authentication data.	i. The attacker modifies the data of the Identity details of the user, the booking details by creating, updating or deleting the already provided details and can also distort the integrity of the **Car access token** and **Random number** used for verification of the user and access to the car.	1. **Impact on System Asset:** compromise the data between the **Identity provider** while storing the details of the user. Disrupts the integrity of the **random number** sent between user and service provider. compromise of the **car access token** sent from **user** to the **car** to gain access to the car. 2. **Impact on Business Asset:** The **identity details** of the user and the **booking details** lacks integrity and confidentiality due to the tampered data. compromise of integrity of the **random number** and the **car access token**. 3. **Negation of Security Criteria:** Negation of CIA at D1, Negation of I at D4. Negation of CI at D3 and Negation of CIA at D6

Table 17. Repudiation Security Risk Analysis of the Car-Sharing System

Threat Type	**Vulnerabilities**	**Threat**		**Impact**
		Threat Agent	Attack Method	
RR8: Unauthorised Access Denial: An attacker accesses the car with the user's details, and the user denies the activity of accessing the car even when the service logs show the user performed that activity.	session hijacking or car access token theft can enable the adversary to take over legitimate user sessions, potentially leading to unauthorised access.	**Expertise:** An Attacker gains access through knowledge of the inherent weaknesses of an authentication mechanism or by exploiting a flaw in the authentication scheme's implementation	i. The attacker may intercept and hijack sessions when the service provider grants the user access to the car and takes control of users' accounts to perform the car access action without their knowledge.	1. **Impact on System Asset:** In **M4**, there is a compromise of the communication session between the **service provider** and the **user** in accessing the **car**. 2. **Impact on Business Asset:** The **car access token(D6)** would be hijacked and access granted to an unauthorised user. 3. **Negation of Security Criteria:** Negation of CIA of D6

Table 18. Information Disclosure Security Risk Analysis of the Car-Sharing System

Threat Type	**Vulnerabilities**	**Threat**		**Impact**
		Threat Agent	Attack Method	
1. **IR1: Man-in-the-middle attack:** Attacker inserts himself into a communication between a user and an application, either to eavesdrop or to impersonate one of the parties.	V1: Lack of strong encryption of the business assets like in **D1, D2, D3, D4, D5,D6** and **D8**. V2: Insecure Wifi-Networks between user and car. V3: Lack of secure session tokens in **M1, M2, M3, and M4** and **M6**"	**Expertise:** Attacker has an understanding of network and communication protocols within the framework of the car, the user or the service provider's network. An attacker has the skill of social engineering where he acts as the service provider to retrieve the **Identity details(D1)**, **Login credentials (D2)**, **Car access token(D6)**.	An attacker can determine the type and manner of communication between the two target components through the Interception and Decryption methods.	1. **Impact on System Asset:** From **M1,M2,M3,M4** and **M6**, there is a compromise of the confidentiality of the **User**. Users' privacy is altered, leading to identity theft and unauthorised access. 2. **Impact on Business Asset:** Lack of accuracy and injection of false information to the system. **D1,D2,D3,D4,D5,D6** and **D8** are compromised and lacks the integrity of the data. 3. **Negation of Security Criteria:** Negation of CIA at **D1,D2, D6** and **D8** Negation of CI at **D3** Negation of IA at **D4** and **D5**
2. **IR4: Information Disclosure attack:** The attacker gains unauthorised access to sensitive data, leading to a confidentiality breach.	V1: Lack of data anonymisation and data linkage to the user of their car. V2: Inefficiency in data storage such as weak database security	**Expertise:** Attacker understands the car-sharing system's cloud storage architecture and knows how to decrypt a user's data efficiently.	An attacker might exploit insufficient access controls on the data repositories. The attack could involve SQL injection attacks on databases or exploiting configurations in data storage systems to gain unauthorised access to the real-time information shared	1. **Impact on System Asset:** From **M5**, there would be a lack of trustworthiness to the system and high operational costs of understanding the breach. There is also a compromise of the user identity and car behaviour. 2. **Impact on Business Asset:** The **real time information (D7)** in **M6** will be compromised as the sensitive data is disclosed. 3. **Negation of Security Criteria:** Negation of Confidentiality in D7

Table 19. Denial of Service (DOS) Security Risk Analysis of the Car-Sharing System

Threat Type	**Vulnerabilities**	**Threat**		**Impact**
		Threat Agent	Attack Method	
1. DR7: Denial of service attack: Attacker makes resources unavailable to its users by temporarily or permanently disrupting services on a host connected to the Internet.	i: The system cannot take many car access requests and has a low service load. ii: Inadequate Resource Allocation	**Expertise:** The attacker should have an understanding of cybersecurity, networks, and system penetration techniques, as well as the ability to issue a large number of HTTP requests.	An attacker can overwhelm the service provider with numerous car access requests and booking requests, thereby overwhelming the system's capacity and preventing genuine access requests from being processed.	1. **Impact on System Asset:**From **M3**, the **user** is unable to make a booking request as the system is unavailable for usage. The server of the **service provider** handling booking requests may be overburdened, failing to process new legitimate requests. ii. From **M4**, the service provider's system for managing car access requests may be incapacitated, impeding the issuing and verifying car access tokens (A4.2, A4.4). 2. **Impact on Business Asset:** From **M3**, there would be inaccessibility of the **booking details (D4)** and interruption in the processing of the booking details ii. In **M4**, The process of issuing and validating **car access tokens (D6)** would be affected, causing delays and even producing a backlog of service requests. 3. **Negation of Security Criteria:** Negation of IA at **D3** and **D4**, Negation of CIA at **D6**

stated in their work that security requirements can be seen as constraints on the system's functionality, focusing on what to achieve.

We described in Section 5.2 the security risk analysis, where we identified the different threats and vulnerabilities posed by the system while eliciting the security criteria for each risk to an asset. To describe the solution space [17], we have identified the techniques to mitigate the risk and create a privacy-aware solution to the car-sharing system. Firesmith [10] discusses how the guidelines have proven helpful for eliciting, analysing, specifying, and maintaining security requirements. In his work, he pointed out different objectives for what security requirements entail and how these requirements ensure the mitigation of potential risks in a system. He further described the various types of security requirements that were applied in our work. Security requirements include identification, authentication, authorisation, integrity, and privacy.

Using the following guidelines, we have elicited forty-two (42) security requirements that support the implementation of security controls in car-sharing scenarios where these risks exist. (see Table 20- 24)

5.4 Answer to Research Question

In this section, we provide the findings of the SLR to answer the research question. textbf[RQ3:] What are security risks and their reduction approaches in car-sharing scenarios?

RQ3.1: What are the security risks? The STRIDE threat modelling approach was applied. The approach resulted in the identification of fourteen risks that existed within the scenarios. There are several places where these risks negate the assets' confidentiality, integrity, and availability. For instance, the **Man-in-the-Middle attack (MitM)** negates the security need for the assets as the attacker listens to the communication between the entities. Server leakage attacks, impersonation attacks, and phishing appear primarily in systems where an attacker pretends to be a legitimate user to steal the user's data. The Denial of Service (DOS) is where the attacker overwhelms the system request, such as the booking service.

RQ3.2: What are the reduction approaches? Following the ISSRM model approach, we have elicited 42 security requirements and control measures implemented in the car-sharing system to reduce the risks. In the MitM attack, secure connection protocols such as SSL-TLS should be implemented for secure data transfer between the entities. Reducing phishing attacks ensures users have an additional layer of security through different authentication channels, such as their biometrics. Advance Encryption Standard (AES) and data minimisation reduce the amount of readable data stored, lowering the risk of data exposure if a server leaks. Also, applying the approach in cases where an unauthorised user handles data reduces the risk of tampering with data.

Table 20. Security Risk Mitigation for Car-sharing System by Papers

SR6: Phishing		
Paper	**Security Requirement**	**Security Control**
Cao *et al.*	1. The system shall authenticate a user with a multi-factor authentication system. 2. The system shall Identify it is the right user of the car-sharing application. 3. The system shall randomly select the identity details used during registration. 4. The Identity details of the user should be inaccessible to adversaries	i. **Multi-factor Authentication (Biometrics and Passwords)** ii. **Random ID Selection at Registration:** The ID used in the authentication process is selected randomly during the registration stage, making it difficult for an attacker to guess the correct ID information.
	5. The system shall accept login credentials over a secured connection. 6. The system shall enable a secured communication link between actors.	**Secure Credential Transmission: TLS or HTTPS**
	7. The system shall implement a challenge-response system that incorporates user-specific biometric data. 8. The user shall be provided with the correct information for an identifier	**Challenge-response system**
	9. The system shall manage the integrity of booking details.	Pseudomisation of information
SR2: Impersonation Attack		
Kim *et al*, Ma *et al*.	**Security Requirement**	**Security Control**
	10. The system shall enforce multi-factor authentication.	**Data Minimisation**: (The adversary cannot generate the authentication message of a legitimate user because they do not possess the user's private key, random number, identity, and password [[13, 16]]
	11. The system shall cross-check messages generated to ensure user access only	Identity Protection using XOR and hash operations [[16]]

Table 21. Security Risk Mitigation for Car-sharing System by Papers (Continued)

SR3: Tampering Data		
Paper	**Security Requirement**	**Security Control**
Dzurenda *et al.*	12. The system shall secure data transfer at the communication point. 13. The system shall not allow an unauthorised user access to data.	**cryptographic algorithms:** ensure data integrity and confidentiality.
SR5: Sever Leakage		
Zhou *et al.*	14. The system shall Implement a strict access control policy for stored data 15. The system shall prevent unauthorised access to the communications.	**User Anonymity:** random numbers in the authentication process (if server data is leaked, the session keys and user anonymity are maintained)
Cao *et al.*	16. The system shall use industry-standard encryption protocol to encrypt personal data	**Data encryption of personal data and biometric information**
	17. The service provider should not store the personal data. 18. The service provider should not link the user on the communication channel	**Data Minimisation**
Sudarsa *et al.*	19. The system shall monitor and alert the service provider of a data breach within 30 minutes of the breach.	**Intrusion Detection Systems**

Table 22. Security Risk Mitigation for Car-sharing System by Papers(Continued

SR1: Man-in-the-middle attack		
paper	**Security Requirement**	**Security Control**
Cao *et al.*	20. The Identity provider shall implement a robust encryption mechanism for data in transit.	**challenge/response mechanism along with random numbers**
Kim *et al.*	21. The system shall ensure the validation of message integrity.	Un-directionality of the hash function: (Users can verify whether an intermediary falsifies the transferred message through validation between the random number and private data)
	22. The System shall use timestamps for message verification	**Timestamps Utilisation:** confirming the timeliness and authenticity through Timestamps
	23. The Identity Provider shall use random numbers for authentication processes	**Blockchain for decentralisation and integrity of data:** (BAN logic and AVISPA simulations)
	24. The system shall employ pseudo-identities in place of real user identities	**Pseudo-identities:** (User anonymity)
Arm *et al.*	25. The REST API endpoints shall have stringent input validation	Limiting and validating inputs in REST API to prevent misuse of information systems and data breaches.
	26. The identity verification processes should be robust and employ a trusted identity provider.	Utilising an identity provider to protect sensitive data and prevent identity spoofing
	27. The system shall implement secure communication protocols for all data transmissions	**Secure connection protocols**
Symeonidis *et al.*	28. The communication channels shall be secure in the system	**SSL-TLS and NFC**

Table 23. Security Risk Mitigation for Car-sharing System by Papers(Continued)

SR4:Information Disclosure		
Paper	**Security Requirement**	**Security Control**
Pollicino *et al.*	The system shall limit the monitor's access to user information. 13. The system shall focus on the car state	**Application using Pseudonym Certificates compliance with policies**
	31. The system shall ensure secure information transfer from the identity provider to the user.	**Trusted Platform Modules (TPMs)** to securely store information and detect tampering.
Symeonidis *et al.*	32. The system shall anonymise the details of the user during car-share	Hardware Security Module (HSM) that supports secure key storage and cryptographic operations such as symmetric and public-key encryption
	33. The service provider shall provide transaction details to law enforcement without violating other users' privacy	**Forensic Evidence Provision**
SR7: Denial of Service (DOS)		
Cao *et al.*	34. The system should handle high request loads	use efficient cryptographic operations, and minimise computational requirements
Valaštín *et al.*	35. The system should have a robust, decentralised network architecture	**Decentralised system: (Blockchain Methodology)**
Wei *et al.*	36. The system shall have secure communication protocols that protect the network	**HIBS-KSharing system**

Table 24. Security Risk Mitigation for Car-sharing System by Papers (Continued)

SR8: Unauthorised Access		
paper	**Security Requirement**	**Security Control**
Cao *et al.*	37. The system shall identify the user to ensure that authorised users have access.	**Incorporation of user-specific biometrics along with passwords**
Ma *et al.*	38. The system should employ user verification in real-time.	**MobiDIV** (real-time, on-device face verification, three-stream neural network for robust face feature extraction)
Symeonidis *et al.*	39. The system shall ensure that the access token is only available to the shared car. 40. The system shall ensure that the access token is only available to the authorised user. 41. The Service Provider shall request authentication access from the user.	secure multi-party computation (MPC) and encryption techniques (Confidentiality of the car access token)
	42. The system should implement independently generate keys.	Backward and Forward Secrecy of Access Code (independently generated keys for each token encryption)

5.5 Summary

The answer to the research question **RQ3** identifies the risks by first presenting a threat model using the STRIDE approach to elicit the threats based on the literature provided during SLR. We identified fourteen perceived threats to the car-sharing system and further conducted a security risk analysis of eight risks by describing their vulnerabilities, threat agents, attack method and impact of the risk on both the business and system assets. The chapter also presented the defined security requirements and their possible reduction measures. In the next chapter, recommendations on how to reduce these perceived risks are provided based on the literature.

6 Recommendation of Security Risk Reduction

This section explores the various recommendations for reducing risks based on the elicited security requirements and control measures depicted in Section 5.3. for the car-sharing scenario. We present the recommendation model for use in reducing the risks, and to further validate the thesis, we provide an instantiation of the model.

6.1 Proposed Recommendation Model

We present the recommendation model for risk mitigation in car-sharing scenarios. The model is divided into assets, risks, and security mitigation. The assets represented by the functions *capturing, transferring, storing, manipulating, retrieving, and Displaying Information* as presented in Section 4. Capturing describes the protected assets when there is an input or captured data. The transferring assets depict the assets transferred from one channel to another and are prone to attacks. Manipulating depicts the assets that perform a particular activity in the sharing service to produce results, and storing describes the storage of data on the database and how that data is retrieved and displayed as assets in the car-sharing process [17]. The recommendation model also depicts the various risks (see Section 5.1.2) and where they exist in each function. Furthermore, the model captures the control measures to mitigate the risks, as elaborated below on the mitigation strategies based on the security requirements and control measures employed to reduce the risks from occurring in the car-sharing scenarios. (See Fig. 17)

Mitigation of Man-in-the-Middle attacks: The Man-in-the-Middle (R1), as seen in the user registration risk model (Fig. 10), occurs between the **User** and the **Identity Provider**. The risk occurs when users enter their identity details (see A1.1), and the identity provider receives them. It also illustrates data transfer from the *user* to the *Identity Provider*. Moonsamy *et al.* [18] described the MitM attack as active eavesdropping. The MitM attacker can manipulate the user's identity details (in this case, a mobile phone) and place themselves between the user and the identity provider's server communication channels to achieve their goal. [18] opined that the MitM attacks target the SSL and DNS of the user (smartphone). An adversary could hijack the session and channel and act as the user, interfering with the communication protocol. Thus, it acts as the original owner of the identity details in the network. Once an adversary hijacks the session, it manipulates and breaches the confidentiality and integrity of the user's identity details. The MitM attacks pose a significant threat to communication between the system assets, which in this instance are the user and the identity provider.

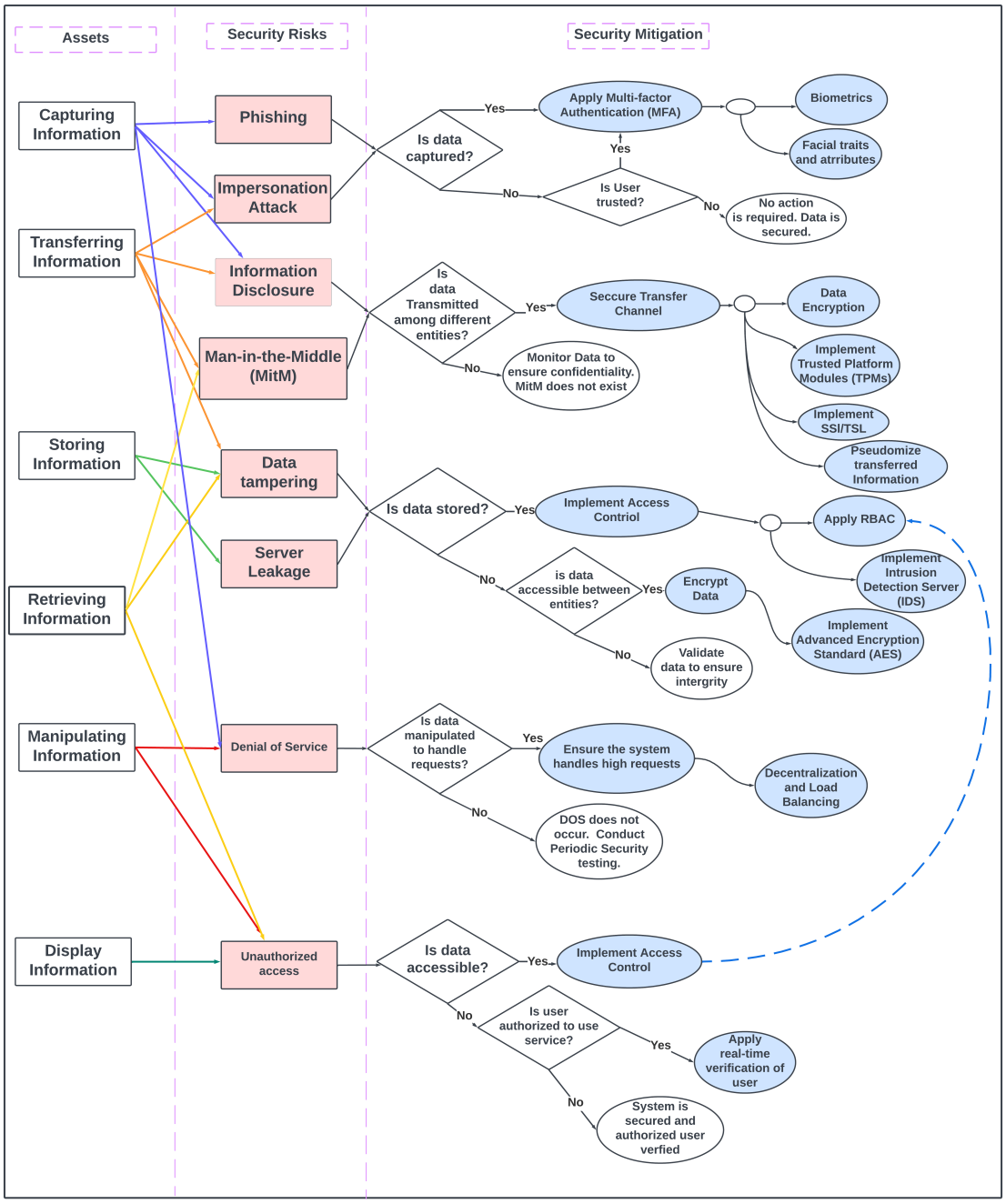

Figure 17. Recommendation Model for Mitigation of Security Risk in Car-sharing

RECOMMENDATION: The proposed security requirement of the MitM attack in the user registration car-sharing process is to secure the communication channels between the user and the service provider. From the security requirements outlined in Table 20, we choose two requirements that solve the MitM attack between the user and the identity provider during registration.

- SR24: The system shall employ pseudo-identities instead of real user identities.
- SR28: The communication channels shall be secure in the system.

When a user sends their identity details, such as a driver's licence and other information, an adversary can act as the user when they gain access. The weak channels of communication between both entities could cause this attack.

SSL/TLS: To mitigate such a scenario, we recommend using SSL/TLS protocols. The Secure Sockets Layer (SSL) and the Transport Layer Security (TLS) provide a secure communication channel between the user and the identity provider. These protocols employ encryption and protection of the identity details sent by the user. This protocol would help prevent the Man-in-the-Middle attack by building a solid connection between the User and the Identity provider. Transport Layer Security (TLS) is an essential tool for protecting internet communication, assuming that the user registers using the internet. The solution would help to keep sensitive information safe [4]. The connection with TLS ensures that this data, in the scenario case, the **Identity details** are encrypted for transmission over the network. [4, 28], and it thus keeps the confidentiality and integrity of the **Identity details** of the user intact.

Pseudo identity: An adversary intercepts the transmitted information between the User and the identity provider, thereby breaching the user's privacy stored in the smartphone [13]. Kim *et al.* [13] suggested in their work that protecting the user's anonymity can be done by the pseudonym of the user's real identity. In the scenario of the risk model for registration, the identity details are protected using random numbers and hash operations.

Mitigation of Impersonation Attack In the risk model (see Fig. 10), as earlier described, when an adversary intercepts the user's identity details, they can act as a proxy for the legitimate user of the car-sharing service. The adversary can also conduct the attack physically if the sharing service user loses their mobile phone or portable device. The loss could also give an adversary access to the information of the legitimate user to register for the service. We suggest the identification requirement, which signifies the extent to which the service would identify a legitimate user of the service, [10] should employ more ways to authenticate and identify a user during registration.

RECOMMENDATION: Our recommendation advocates incorporating multiple identification methods, encompassing traditional means and advanced techniques such as biometrics and facial identification.

- SR10: The system shall enforce multi-factor authentication.

In this user registration scenario, the adversary will have less access to impersonation as identification factors such as biometrics are unique. **Biometrics**, as one of the recommended identification factors, offers a unique and difficult-to-duplicate layer of security. Unlike conventional identity information that can be intercepted or guessed, biometric data, such as fingerprints or facial features, provides a distinct and personalised aspect of identification. This uniqueness enhances the system's ability to accurately verify the legitimacy of a user, thereby reducing the likelihood of a successful impersonation attack.

Mitigation of Tampering data Data tampering in this scenario affects the system assets of the car-sharing registration models. When an adversary tampers with the *identity details*, it loses the integrity and confidentiality of the data shared by the user. Usually, an authorised person can attack with access to the server or a third party. When the adversary intercepts the data stored in the database, they could alter the data available. The identity provider does not allow unauthorised access to user data to mitigate this risk during user registration. As outlined in the existing literature, data tampering attacks pose a severe threat to intelligent systems, and similar concerns apply to the car-sharing system [27]. In the context of user registration, an adversary with access to the *identity details* can manipulate the data, jeopardising the trustworthiness of the entire system.

RECOMMENDATION: The security requirement presented in Table 21 describes how we could mitigate the tampering data attacks in the car-sharing system. To address the tampering data risk, we propose a security requirement (SR14) that focuses explicitly on preventing unauthorised access to user data within the car-sharing system. This requirement emphasises the importance of implementing measures that restrict unapproved users or agents from accessing and potentially corrupting the information provided by the user.

- SR13: The system shall not allow unauthorised user access to data.

To implement this security requirement, [8] highlights the efficacy of cryptography algorithms, explicitly endorsing the use of the Advanced Encryption Standard (AES). Encrypting the transferred data adds a layer of protection, making it significantly more challenging for unauthorised entities to tamper with or manipulate sensitive user identity details. By adopting measures to prevent tampering with data attacks, mainly through implementing advanced encryption algorithms, the car-sharing system can enhance its resilience against malicious actors seeking to compromise the integrity and confidentiality of user identity details.

Mitigation of Server Leakage Server leakage is the unauthorised disclosure or exposure of sensitive information kept on a server, which could lead to significant security breaches and jeopardise user data confidentiality and integrity. The server leakage risk in the user registration process of car-sharing systems, particularly within the domain of the *identity provider*, necessitates additional security requirements. When

enacted, the server leakage can also lead to the risk of having the user's data (*identity and login details*) tampered with. Adversaries may leverage server leaks to impersonate users, engage in fraudulent operations, or compromise the entire security and trustworthiness of the car-sharing system. Mitigating server leakage threats is critical for ensuring the confidentiality and integrity of user data in car-sharing systems.

RECOMMENDATION: To effectively address server leakage, a diverse solution that includes a variety of security controls is required. The recommended security measures seek to reduce the danger of server leakage during the car-sharing user registration procedure. We propose SR14 as an alternative to SR19 or implementing both requirements in the system.

- SR14: The system shall implement a strict access control policy for stored data.
- SR19: The system shall be monitored to alert the service provider of a data breach within 30 minutes of the breach.

We recommend that to comprehensively mitigate the server leakage risk in the Identity Provider's domain, it is advisable to integrate multiple security requirements. A robust approach would involve combining an access control policy and monitoring the database for holistic protection against unauthorised access and data exposure of both the *Identity details* and the *Login credentials* of the user. [32] stated that although these access control schemes help mitigate information leakage, existing controls are centralised. This means there is also a high chance of a single-point failure.

Access Control Policies: One standard policy that the Service Provider should implement to mitigate server leakage is Role-Based Access Control (RBAC). This policy ensures that only authorised individuals with specific roles or attributes can access sensitive user data. By implementing access control policies, the system restricts unauthorised personnel or programs from interacting with stored information, reducing the likelihood of server leakage. This policy can help the *identity provider* distribute roles among entities as to who has the authorisation to access the database or server.

Intrusion Detection Servers: The Data shared by the user with the *identity provider* must be monitored continuously to avoid leakage of such data to a third party. Continuous monitoring is vital for quickly discovering and responding to any unexpected or suspicious activity that could indicate a potential server leakage. The implementation of Intrusion Detection Systems (IDS) [11, 32] is intended to detect and respond to unusual activity of potential security events in the server environment. It analyses network and system activities to identify patterns that differ from usual behaviour. We recommended that the *identity provider* integrate and implement the IDS, as this approach empowers the *identity provider* to detect and respond to potential server leakage incidents in real time, thereby fortifying the security of user registration data.

Mitigation of Information Disclosure Risk When an *identity provider* transfers a user's *login credentials*, the data is most likely disclosed to a third party. An adversary

may intercept and steal this data, disclosing critical *login credentials* to manipulate the system.

RECOMMENDATION: For the identity provider to enhance the confidentiality and integrity of the login process, particularly when the identity provider sends *login credentials* to the user, providing a more secure environment for users is important.

- SR31: The system shall ensure secure credential transfer from the identity provider to the user.

To implement this, we recommend the implementation of Trusted Platform Modules (TPMs), which play a significant role in mitigating information disclosure attacks.

TPMs are hardware-based security modules that provide a secure enclave for storing sensitive information and performing cryptography operations [23]. They provide data and hardware protection for secret data [26]. The user's login credentials (D2) are essential to using the car-sharing service and, hence, protected from outside attacks or adversary manipulations. TPMs can secure critical data within a specialised hardware enclave. The security measure ensures that the login credentials are not readily available, even if an adversary can access the user's device. TPMs enable secure key exchange protocols, allowing the identity provider to create a trusted channel for transferring login credentials. The modules prevent man-in-the-middle attacks and ensure credentials are provided to the intended user without interception or information disclosure attack, as described in Section 3.3.2.

Mitigation of Phishing attack To access the car-sharing service, a user must provide sensitive and personal information to the service providers. There are chances of identity theft and other loss-of-information attacks that could happen within the system. In the risk process diagram (see Fig.11), the user provides their identity information to the identity provider, and hence it is prone to a phishing attack. A phishing attack occurs when a user enters their identity details (see Fig.11), and adversaries use deceptive techniques to trick individuals into divulging this sensitive information. Phishing attacks heavily rely on social engineering techniques to manipulate individuals, such as exploiting human psychology, trust, and curiosity to trick people into taking actions that may compromise their security. [5].

RECOMMENDATION: We elicited the security requirement to mitigate the risk of a phishing attack, which will help mitigate this risk from the system. Table 19 shows different ways to protect identity details from phishing attacks.

- SR1: The system shall authenticate a user by multi- factor authentication.
- SR3: The system shall randomly select the identity information used during registration.

Multi-factor Authentication (MFA): Implementing a dual-factor authentication system (SR1) strengthens the identification process, making it more difficult for adversaries

to compromise user credentials only through phishing [5]. The system adds levels of complexity that hinder adversaries from exploiting user trust during identity entry by incorporating biometrics and facial identifications as parts of the user-provided data. According to security experts, multi-factor authentication is an excellent defence against phishing attempts because it forces attackers to compromise numerous parts, increasing the difficulty of unauthorised access to the system. Contrary to Wang *et al.* [30] opined that while MFA could be the best way of tackling the phishing attack, designing this security measure has become a challenge as different schemes end up being unable to secure the data of the user.

Random ID Selection: Randomly selecting identity information during registration is a proactive measure against phishing attacks. These adversaries frequently focus on anticipating or copying user credentials, a task made difficult by the unpredictable nature of randomly chosen identifiers. Instead of users manually entering their personal identification details, the system can generate and assign randomised identifiers, enhancing the unpredictability of user credentials by the adversary.

We recommend the implementation of the MFA for mitigating phishing attacks because of its effectiveness in preventing them, as it adds an extra layer of security during user registration. As discussed earlier, it protects against unauthorised access and impersonation attacks.

Mitigation of Denial of Service attack A denial-of-service attack impairs a system's regular activity. To mitigate a DOS attack, it can either be proactive or reactive [20]. Mitigating this risk is critical for making car-sharing services available to appropriate and legitimate users, thereby safeguarding the integrity and availability of *booking details* (see Table 10). This means that an adversary can send in many requests for bookings or car access codes to cause delays and impede the operation of the service. The denial of service negates security criteria for the availability of the service when needed for the booking operation.

RECOMMENDATION: We recommend the security requirements to mitigate the denial-of-service attack and prevent such attacks in future car-sharing systems. It also prepares the system to adapt to future threats involving increased traffic or more sophisticated attack methods.

- SR34: The system should handle high request loads.

The selected security requirement directly addresses the risk of DOS attacks, wherein an adversary attempts to overwhelm the system by flooding it with excessive requests. By ensuring the system's capacity to handle high request loads, the service provider endeavours to halt potential DOS incidents. Therefore, adhering to SR34, the service provider establishes a robust defence against potential DOS attacks and enhances the system's overall performance and reliability.

Mitigation of the Unauthorised access attack for a user to access a car, they provide the user with access tokens that enable them to gain access to the car. (see Fig. 14). The

service provider unlocks the car after a user is authorised to use it. Unauthorised access could be physical security, where the user accesses the car or a driver pretending to be the original person authorised to use the car.
More so, Ma *et al*. [16], have introduced continuous verification of the driver using their proposed framework, MobiDIV, to ascertain that a suspicious person or adversary does not gain access to the car.

RECOMMENDATION: To mitigate unauthorised access to the car access scenario, we recommend that real-time user verification be consistent with current best practices in security design and supported by existing literature on securing shared mobility systems.

- SR38: The system should employ user verification in real-time.

Implementing SR38 into the security architecture of the car-sharing system not only strengthens its defences against potential harm but also aligns with legal regulations and industry norms that promote compulsory user verification methods. [16] provides further validation for the effectiveness of this security technique in preventing unauthorised access. When an adversary has subverted the authentication by gaining access to the *car access code*, they can gain access to the car when they are not the original person intending to use the car service. Therefore, this recommendation helps to prevent unauthorised access while also improving the car-sharing service's general reliability and availability because the *Service Provider* can confirm the identity of the person who gained access to the car.

6.2 Instantiation of Recommendation model

This subsection presents an example of implementing the recommendation model (see 18. The model illustrates the asset (manipulating information), capturing the scenario of car access. In the process, the service provider provides the car access token (D6)(see Fig. 8). This asset is vital for the operation of the user accessing the car. Hence, the asset needs protection from a denial-of-service attack and unauthorised access to the asset. The risks were analysed using the security risk analysis presented in Tables 17 and 19, respectively. Furthermore, a decision requesting data manipulation means that the adversary may compromise the service through a DOS attack by impeding the services of the car-access process. To reduce this risk, the service provider can handle high-volume requests for users who want to access the car by decentralising the servers and implementing active load balancing. On the other hand, the unauthorised attack occurs when the car access token is accessible to the attacker; hence, we suggest the application of role-based access control (RBAC) to reduce the chances of an unauthorised person getting access to the car access token (D6). In this case, token theft is possible, as the adversary takes over the legitimate user session, compromising communication between the service provider and the car. If, at any point, data manipulation does not occur while accessing the vehicle,

it means that this risk of unauthorised access would not exist within the process and hence make the session and data processes safe from danger. Also, the decision to treat becomes true if the user of the car-sharing service is unauthorised because there can be chances that an unauthorised user has gained access to the car; hence, we apply the real-time verification of the user throughout the sharing service. While the unauthorised access in process A2.2 of Fig. 14 does not explicitly appear in the literature, it is pertinent to say that there is a gap in the literature on identifying exact places where the risk might occur. However, it also gives us a clearer perception of the attack areas of the scenarios.

6.3 Discussion

The recommendation model for security risk management in car-sharing aims to reduce the risks to assets in different car-sharing scenarios. We made recommendations based on theoretical insights from the literature from the SLR conducted. The development of the recommendation model started with the criteria for relevant studies described in sections 2.4 and 2.5, respectively, as well as the literature covering car-sharing and security, from which we extracted the relevant information for the thesis. Furthermore, the recommendation model gives us an overview of the assets, which comprise both the business and system assets, by capturing the process that occurs in the scenario where the risks affect the processing of the information and depicting the decision to reduce the risks. We looked at the vulnerabilities of data privacy concerns, such as weak usernames and passwords for login credentials, and how the impact negates the security need for confidentiality, integrity, and availability when hijacked by an adversary.
Moreover, the proposed recommendation model captures the core concepts of the Information Systems Security Risk Management (ISSRM) approach and gives the companies a structured framework for risk mitigation in car sharing. To further provide proof of concept to the existing theoretical concept, we also provide an illustrative example that instantiated one of the assets to demonstrate the practical application and usability of the recommendation model based on the scenario provided in the business process models and security risk analysis aids in validating our work in this research. In summary, this recommendation model provides a structured, systematic approach to identifying the assets and security risks and proffering risk reduction strategies for practical implementation in car-sharing companies.

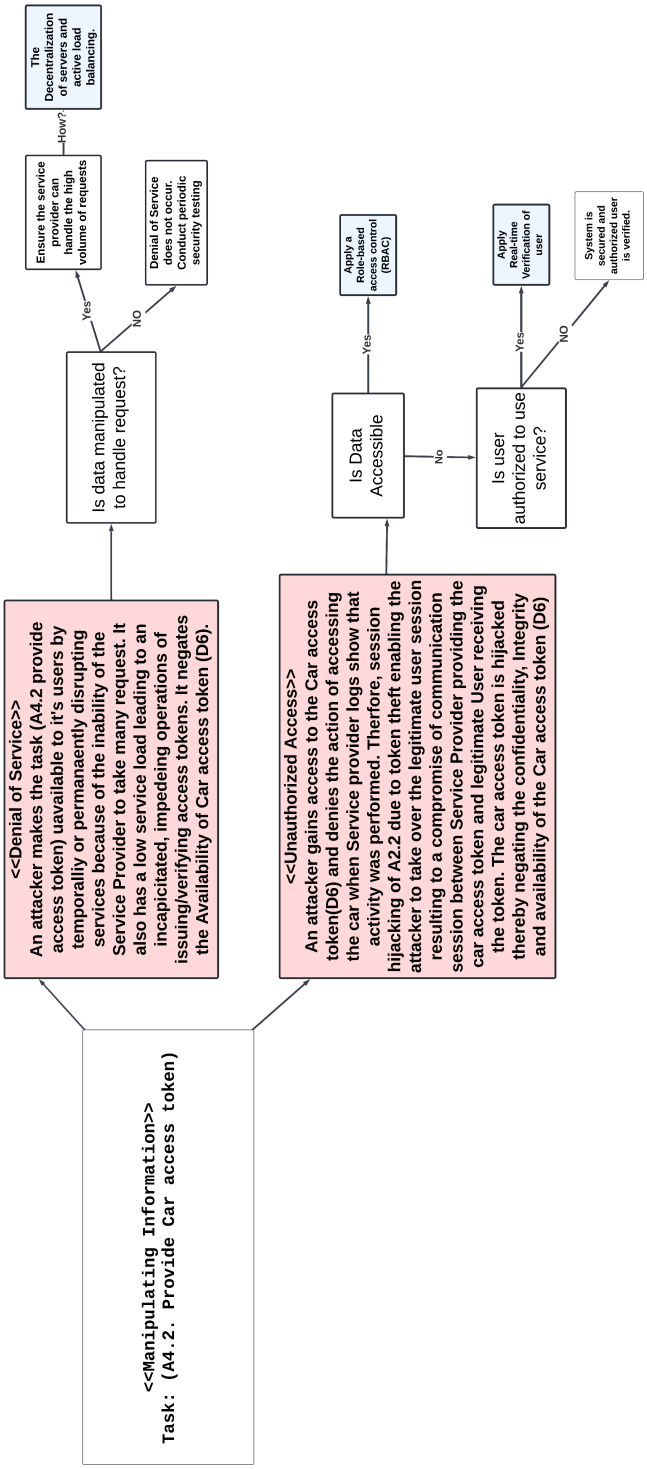

Figure 18. Instantiation of the Recommendation Model for Risk Reduction

7 Conclusion

In this thesis, we explored the security and privacy of different car-sharing scenarios by recommending how to mitigate the risks associated with the various scenarios. To achieve this, we conducted a systematic literature review to understand the context of car-sharing and scenarios within the system. In our findings, we used six car-sharing scenarios: User registration, User Verification, Booking of the service, Car access process, user behaviour monitoring and finally, the payment process. The scenarios were presented using BPMN to give an expanded insight into how the business assets are transferred from one entity to another. Furthermore, we presented the security aspects of the scenarios using the ISSRM approach to security risk management. Firstly, we identified the various assets (Business and IS assets) that need to be protected and utilised a threat-driven approach to determine the risks within the scenarios. Secondly, the elicitation of security requirements, and we went further to make recommendations to validate the control measures drawn from the literature. Finally, we developed our recommendation model, which captures how to protect the assets and instantiates the implementation of the recommendation model to optimise security in the car-sharing business process.

7.1 Limitation

This thesis has certain limitations, and our main **threat to validity** acknowledges that there can be search strategy bias while conducting SLR. Researchers may have their own bias towards the terminologies used, limiting the coverage of the selected keywords during the SLR selection phase of the article. We expand our search strategies to limit this bias by using keywords to target our scope and other car-sharing areas. Another limitation is that the scope of our recommendation may not have captured all privacy-enhancing technologies for mitigating risks in car-sharing. Hence, future work on mitigation strategies would benefit from developing a more robust model to validate the proposed model further and make informed policy decisions. Also, the thesis does not discuss the computational cost or cost-effectiveness of the risk reduction as privacy-enhancing solutions are expensive to implement; thus, we gave the proposal as ways to reduce the risk in the scenario without further research on its cost. Finally, our results from SLR focused on the scenarios related to car-sharing. While the thesis presented the possible risk scenarios, there could be possible omissions in the captured risks in the research. However, the extracted results presented are from the various researchers' work.

7.2 Answer to Research Questions

In this thesis section, we answer our main research question, **MRQ: How to manage security risks in car-sharing scenarios?**. We would answer the three sub-questions of

the thesis, which were further divided into sub-questions in the different chapters to give the context of the scenarios.

RQ1: What is the context of the car-sharing system? To understand the context of the car-sharing system, we found that the authors used different terminologies and concepts to describe the specific entities in the system. It is crucial to say that fewer researchers discussed the processes of the car-sharing system, as some researchers focused on a particular use case. In the context of car-sharing, we identified from the literature the six main business processes that contribute to the successful usage of the service. These main processes were further broken down into sub-processes to enable us to understand the flow of information from the different entities using BPMN to depict each actor's tasks and the type of information required for the scenario. The activities within the process capture the data captured, transferred, manipulated and stored,

RQ2: What are the protected assets in car-sharing scenarios? We identified the assets in Chapter 4 to understand the assets to be protected. We further divided the question into three sub-questions to capture each question and answer the research question. According to the scenario, business assets are the core information used to support the operation of the service. Such as data used to register (Identity Details D1), verify (Login Credentials D2, Random number D3), book the car (Booking Details D4), (Reservation Details D5), access the car (Car Access Token D4), monitor user behaviour (Real-time information D6) and payment for service (Payment Details D8). The system assets act as the components that support the system (User, Service Provider, Identity Provider, Car, Database). Furthermore, we ascertained the security need, that is, each asset's confidentiality, integrity, and availability, to understand what security requirements need to be applied and which of the needs will likely be negated by the security risk.

RQ3: What are the security risks and their reduction approaches in the car-sharing scenarios?: We looked at ways to protect the assets from adversary attacks to address this question. In Chapter 4, we applied the threat model to identify the threats posed to the assets and a risk analysis was conducted to analyse their impact. However, these risks appeared in 33 places within the risk models, depicting where they may occur. We found out that the ***Man-in-the-Middle (MitM)*** attack appears more frequently in different scenarios and targets the transfer of information between entities throughout the scenario. The *Identity details(D1)* of the user appears to be the most vulnerable asset as five risks occur in the scenario. The security requirements and security are developed based on the literature and hence provide us with the security measures that apply to car-sharing This study introduced the recommendation model in Chapter 5 as a mitigation technique to protect assets from risks using car-sharing scenarios as a case study, resulting in integrating recommendations extracted from the security requirements and controls mentioned in the previous answer. Additionally, the recommendation model encompasses the entire cycle of security risk management by first applying the risks

discovered from the SLR to the specific functions where they pose threats to assets and describing the mitigation strategy for protecting the specified assets in the scenario. To further validate the model, we present an illustrative example demonstrating how the recommendation model implements risk reduction. This illustration further validates the theoretical concepts retrieved from the research and their applicability to mitigating risks in real-world car-sharing scenarios.

7.3 Future Work

In the future, the recommendation model needs to be validated with car-sharing companies and garner more feedback from the theoretical framework on improving the existing model to enhance the security of the car-sharing business process. However, we have presented the results in the CHESS seminar further to gather insights on the improvement of the model. Although we carried out a systematic literature review for this research, there are tendencies of a gap in that the security risks applied in this thesis do not capture all the risks. Hence, future work should explore more research to analyse Privacy-Enhancing Technologies to reduce the risks of car sharing. Researchers can conduct a robust systematic literature review for the entire car-sharing system since, in our work, we focused on the scenarios found in the literature without discussing the mitigation cost of implementing the recommendations made for the car-sharing industry.

List of References

[1] J. Arm, P. Dvorsky, P. Fiedler, C. Falcou, and J. Orlicky. Safety and Security of the Car-Sharing System. *IFAC-PapersOnLine*, 55(4):121–126, 2022.

[2] Sophia Auer, Sophia Nagler, Somnath Mazumdar, and Raghava Rao Mukkamala. Towards blockchain-IoT based shared mobility: Car-sharing and leasing as a case study. *Journal of Network and Computer Applications*, 200:103316, April 2022.

[3] Paul Bossauer, Thomas Neifer, Gunnar Stevens, and Christina Pakusch. Trust versus Privacy: Using Connected Car Data in Peer-to-Peer Carsharing. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, CHI '20, pages 1–13, New York, NY, USA, April 2020. Association for Computing Machinery.

[4] Fidan Bozkurt, Mustafa Kara, Muhammed Ali Aydın, and Hasan Hüseyin Balik. Exploring the Vulnerabilities and Countermeasures of SSL/TLS Protocols in Secure Data Transmission Over Computer Networks. In *2023 IEEE 12th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS)*, volume 1, pages 400–407, September 2023. ISSN: 2770-4254.

[5] Fengkuan Cao and Wenxve Wei. User Anonymous Authentication Key Exchange Protocol Based on Biometrics and Password. In *2022 IEEE 6th Advanced Information Technology, Electronic and Automation Control Conference (IAEAC)*, pages 1344–1350, Beijing, China, October 2022. IEEE.

[6] Capec. CAPEC - CAPEC-94: Adversary in the Middle (AiTM) (Version 3.9).

[7] Xusen Cheng, Tingting Hou, and Jian Mou. Investigating perceived risks and benefits of information privacy disclosure in IT-enabled ride-sharing. *Information & Management*, 58(6):103450, September 2021.

[8] Petr Dzurenda, Lukas Malina, Pavel Loutocky, Frantisek Kasl, Pavel Kristof, and Jan Hajny. Towards to Lightweight and Secure Access Control Systems for Car-Sharing Services. In *2022 14th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT)*, pages 104–109, Valencia, Spain, October 2022. IEEE.

[9] Hassan El-Hadary and Sherif El-Kassas. Capturing security requirements for software systems. *Journal of Advanced Research*, 5(4):463–472, July 2014.

[10] Donald Firesmith. Engineering Security Requirements. *JOT*, 2(1):53, 2003.

[11] Carol Fung, Quanyan Zhu, Raouf Boutaba, and Tamer Basar. SMURFEN: A Knowledge Sharing Intrusion Detection Network.

[12] Daniel Ganji, Christos Kalloniatis, Haralambos Mouratidis, and Saeed Malekshahi Gheytassi. Approaches to Develop and Implement ISO/IEC 27001 Standard - Information Security Management Systems: A Systematic Literature Review. 2019.

[13] Myeonghyun Kim, Joonyoung Lee, Kisung Park, Yohan Park, Kil Houm Park, and Youngho Park. Design of Secure Decentralized Car-Sharing System Using Blockchain. *IEEE Access*, 9:54796–54810, 2021.

[14] Barbara Kitchenham. *Kitchenham, B.: Guidelines for performing Systematic Literature Reviews in software engineering. EBSE Technical Report EBSE-2007-01*. January 2007.

[15] Wenyin Liu, Yin Lin, Zongcheng Qi, Zekai Wu, Guipeng Zhang, Kai Wang, Shuai Fan, and Zhenguo Yang. LoginSoEasy: a System Enabling both Authentication and Protection of Personal Information based on Trusted User Agent. In *2021 IEEE Sixth International Conference on Data Science in Cyberspace (DSC)*, pages 122–129, October 2021.

[16] Yinan Ma, Jing Wu, Chengnian Long, and Yi-Bing Lin. MobiDIV: A Privacy-Aware Real-Time Driver Identity Verification on Mobile Phone. *IEEE Internet Things J.*, 9(4):2802–2816, February 2022.

[17] Raimundas Matulevičius. *Fundamentals of Secure System Modelling*. Springer International Publishing, Cham, 2017.

[18] Veelasha Moonsamy and Lynn Batten. Mitigating man-in-the-middle attacks on smartphones – a discussion of SSL pinning and DNSSec. *12th Australian Information Security Management Conference. Held on the 1-3 December*, 2014 at Edith Cowan University:Western Australia., 2014. Medium: PDF Publisher: Security Research Institute (SRI), Edith Cowan University.

[19] Rafael Torres Moreno, Jesús García-Rodríguez, Jorge Bernal Bernabé, and Antonio Skarmeta. A Trusted Approach for Decentralised and Privacy-Preserving Identity Management. *IEEE Access*, 9:105788–105804, 2021. Conference Name: IEEE Access.

[20] H.R Nagesh, K. Chandra Sekaran, and Adarsh Rao Kordcal. Proactive model for Mitigating Internet Denial-of-Service Attacks. In *Fourth International Conference on Information Technology (ITNG'07)*, pages 96–101, April 2007.

[21] Brenda Nansubuga and Christian Kowalkowski. Carsharing: a systematic literature review and research agenda. *Journal of Service Management*, 32(6):55–91, January 2021. Publisher: Emerald Publishing Limited.

[22] Maragathavalli Palanivel and Kanmani Selvadurai. Risk-driven security testing using risk analysis with threat modeling approach. *SpringerPlus*, 3(1):754, December 2014.

[23] Francesco Pollicino, Luca Ferretti, Dario Stabili, and Mirco Marchetti. Accountable and privacy-aware flexible car sharing and rental services. In *2021 IEEE 20th International Symposium on Network Computing and Applications (NCA)*, pages 1–7, Boston, MA, USA, November 2021. IEEE.

[24] Muhammad Safdar, Arshad Jamal, Hassan M. Al-Ahmadi, Muhammad Tauhidur Rahman, and Meshal Almoshaogeh. Analysis of the Influential Factors towards Adoption of Car-Sharing: A Case Study of a Megacity in a Developing Country. *Sustainability*, 14(5):2778, February 2022.

[25] Riccardo Scandariato, Kim Wuyts, and Wouter Joosen. A descriptive study of Microsoft's threat modeling technique. *Requirements Eng*, 20(2):163–180, June 2015.

[26] Ariel Segall. *Trusted Platform Modules: Why, when and how to use them*. IET Digital Library, November 2016.

[27] Rajesh Kumar Shrivastava, Sanket Mishra, V. E Archana, and Chittaranjan Hota. Preventing data tampering in IoT networks. In *2019 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS)*, pages 1–6, December 2019. ISSN: 2153-1684.

[28] Iraklis Symeonidis, Abdelrahaman Aly, Mustafa Asan Mustafa, Bart Mennink, Siemen Dhooghe, and Bart Preneel. SePCAR: A Secure and Privacy-Enhancing Protocol for Car Access Provision. In Simon N. Foley, Dieter Gollmann, and Einar Snekkenes, editors, *Computer Security – ESORICS 2017*, volume 10493, pages 475–493. Springer International Publishing, Cham, 2017. Series Title: Lecture Notes in Computer Science.

[29] Viktor Valastin, Kritian Kost'al, Rastislav Bencel, and Ivan Kotuliak. Blockchain Based Car-Sharing Platform. In *2019 International Symposium ELMAR*, pages 5–8, Zadar, Croatia, September 2019. IEEE.

[30] Qingxuan Wang and Ding Wang. Understanding Failures in Security Proofs of Multi-Factor Authentication for Mobile Devices. *IEEE Transactions on Information Forensics and Security*, 18:597–612, 2023. Conference Name: IEEE Transactions on Information Forensics and Security.

[31] Zhuo Wei, Yang Yanjiang, Yongdong Wu, Jian Weng, and Robert H. Deng. HIBS-KSharing: Hierarchical Identity-Based Signature Key Sharing for Automotive. *IEEE Access*, 5:16314–16323, 2017.

[32] Qihao Zhou, Zhe Yang, Kuan Zhang, Kan Zheng, and Jie Liu. A Decentralized Car-Sharing Control Scheme Based on Smart Contract in Internet-of-Vehicles. In *2020 IEEE 91st Vehicular Technology Conference (VTC2020-Spring)*, pages 1–5, Antwerp, Belgium, May 2020. IEEE.

1 Glossary

AViSPA - Automated Validation of Internet Security Protocols and Applications
BAN - Belief, Authorisation and Knowledge
BLE - Bluetooth Low Energy
BPMN - Business Process Management Notation
B2B - Business-to-Business
B2C - Business-to-Customer
CIA- Confidentiality, Integrity and Availability
CHESS - Cyber-security Excellence Hub in Estonia and South Moravia
DOS - Denial of Service
HSM - Hardware Security Module
HTTP - Hypertext Transfer Protocol Secure
IDP - Identity Provider
IDS - Intrusion Detection Server
IoT - Internet of Things
ISMS-CORAS- Information Security Management System-CORAS
ISSRM - Information Systems Security Risk Management
KYC - Know-your-Customer
MFA - Multi-Factor Authentication
MitM - Man-in-the-Middle
MPC - Multi-party Computation
MRQ - Main Research Question
MQTT - Message Query Telemetry
NFC - Near Field Communication
OBU - On-Board Unit
PKI - Public Key Infrastructure
P2P - Peer-to-Peer
RBAC - Role Based Access Control
REST-API - Representational State Transfer Application Programming Interface
RFID - Radio Frequency Identification
RQ- Research Question
SLR - Systematic literature Review
SQL - Structured Query Language SR- Security Requirement
SRM - Security Risk Management
SRQ - Sub-Research Question
SSL- Secure Socket Layer
STRIDE - Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service and Elevation of Privilege
TLS - Transport Layer Security

2 Sub-Processes of the Car-sharing system

1. **User registration**

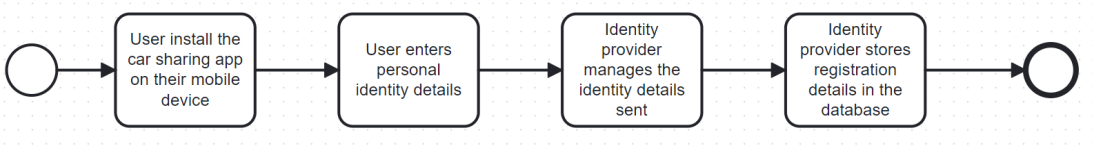

Figure 19. User Registration key activities

2. **Verification of User**

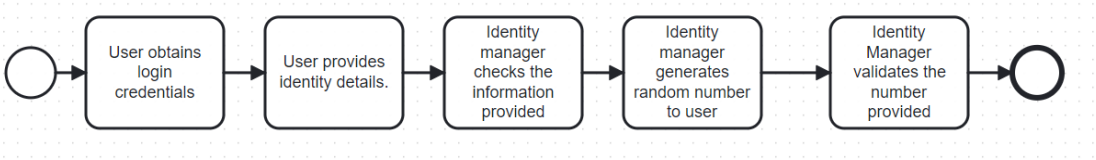

Figure 20. Verification of User key activities

3. **Booking**

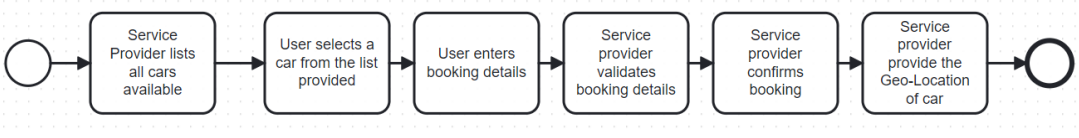

Figure 21. Booking key activities

4. **Car Access**

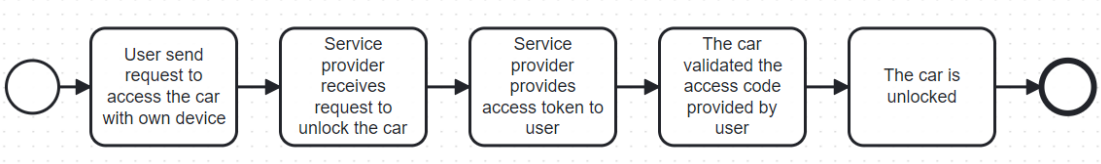

Figure 22. Car Access key activities

5. **User Behaviour**

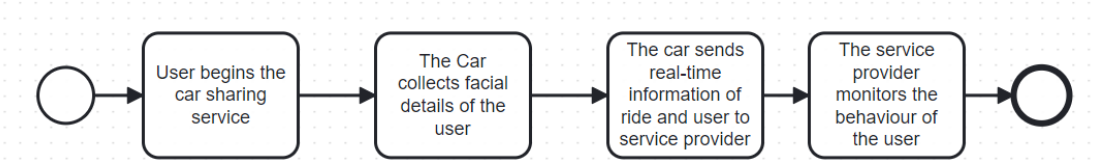

Figure 23. User Behaviour key activities

6. **Payment**

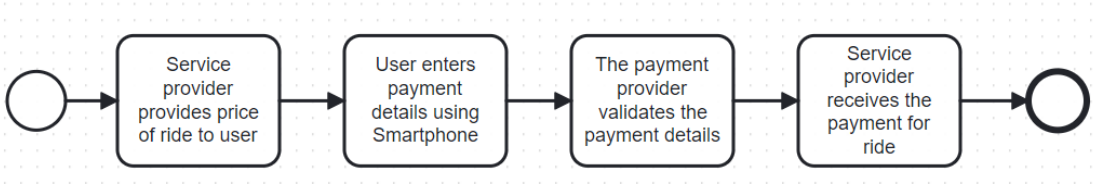

Figure 24. Payment key activities

3 Concepts of Car-sharing

Table 25. User Registration Concepts

User Registration information type				
Activity	**User install the car-sharing app with their mobile phone**	**User enters personal details**	**Identity Provider manages the Identity details**	**Identity Provider stores identity details in the database**
Cao et al.	-	User chooses Identity Information	Server receives identity details	Server saves identity details
Ma et al.	Install app on mobile phone	User registers facial features	-	-
Auer et al.	-	User provides personal details	Send unique digital identity	-
Wei et al.	Download App and Install	User Submits legal information	Register Identity/-Driver's License	UMC saves legal information
Dzurenda et al.	-	User registers personal details	Identity provider manages user identities and issues access token	Personal details saved in database
Arm et al.	Acess app using Mobile app or computer browser	User Register using official document	Identity provider checks documents submitted	-
Zhou et al.	-	User registers details in cloud server	Cloud server provides account address, key pairs and digital certificate	-
Kim et al.	-	User sends real identities	-	Trusted Authority saves real identities

Table 26. Verification of User concepts

User Verification Information type				
Activity	**User obtains Login Credentials**	**Identity provider checks the information provided by user**	**Identity provider generates random number**	**Identity Provider validates the random number provided**
Cao et al.	User enters identity details	Server computes details sent by user	Server generates random number	Server validates the random number received
Ma et al.	User inputs facial details	Server validates facial details	-	-
Auer et al.	-	Leaasing entity performs Know-your-customer (KYC)	-	-
Wei et al.	User obtains ID	-	Car Owner provides user digital sharing key	UMC creates a private password for user
Arm et al.	Login using credentials	cloud-based identity verification validates user details	Cloud-based identity manager sends Time-restricted virtual key	-
Zhou et al.	Obtain account address,key pairs and digital certificates	-	-	-
Kim et al.	Trusted authority issue credential and pseudo-identity to user and vehicle owner	The station authenticates user based on information stored o blockchain	-	-

Table 27. Booking Concepts

Booking Information type						
Activity	**Service Provider lists all cars available**	**User selects a car from list provided**	**User enters booking details**	**Service Provider validates booking details**	**Service provider confirms booking**	**Service provider provide Geo-Location of car**
Auer et al.	OEM lists all available cars	Short term renter selects car from list	User provides personal details	Leasing Entity performs KYC	-	-
Valaštín et al.	-	-	User enters booking details	-	Booking confirmed by service provider	-
Pollicino et al.	-	-	User submits credentials	Broker handles rental request	Broker releases authorization grant	-
Safdar et al.	-	-	User submits credentials	-	Service provider confirms booking details	User locates car
Symeonidis et al.	-	-	User enters booking details	Service provider validates booking details	Booking requests confirmed	-
Wei et al.	-	-	User sends booking details to the car	Service provider handles booking request	-	User locates car
Dzurenda et al.	-	-	User makes car reservations	-	-	CSSP provide Geo-location of car
Arm et al.	-	-	User chooses vehicle	User creates reservation	-	-
Zhou et al.	Obtain state information of nearby vehicles	User selects Vehicle	-	Smart contract determines booking order	Smart contract accepts booking request	-

Table 28. Car Access Concepts

Car Access Information type					
Activity	**User send request to access the car using smartphone**	**Service provider receives request to unlock the car**	**Service provider provides access token to user**	**The car validates the access code provided by user**	**The Car is unlocked**
Ma et al.	User sends request for car control	Cloud server receives request for car control	Cloud server retrieves and sends the unique OS to user	-	car activates app and ORS confirmation
Valaštín et al.	request for car access through unlock token	-	Service provider provide unlock token with an executed smart contract	Car receives unlock token and verify its validity with the blockchain network	The car is ready to drive
Pollicino et al.	-	-	Broker provides authorization detail	-	Car is unlocked by a smart start system
Symeonidis et al.	-	Service provider receives car access request	User receives access tokens and generates two symmetric keys	The OBU verifies the condition of lent, if there was modification of booking details and modification of identity	OBU unlocks the car
Wei et al.	-	Owner generates user key with smartphone app	User generate signature on random challenge and send signature to car	The car receives signature through NFC protocol and validates	Car unlock
Dzurenda et al.	-	-	User receives access code	The car validates access key	OBU lock/unlock the car
Arm et al.	-	Identity management service updates credentials received	Identity management service push access right update	The car receives access rights in the access control unit	Car is unlocked using a mobile device with stored virtual key via BLE or NFC technology
Zhou et al.	Tenant sends opening request to the vehicle through the terminal	-	Service provider provides access code	The car receives code from terminal and validates the access code	Car unlock
Kim et al.	Station send user request	-	Owner generate Access code and transmit to station	The car receives vehicle access code and validates user	Access granted using mobile phone

Table 29. User Behaviour Concepts

User Behaviour Information type			
Activity	**User begins the car sharing service**	**The Car collects and sends real-time information details of the driver**	**The service provider monitors the behaviour of the user**
Ma et al.	User begins ride	Car collects facial details of driver	The car continuously collects facial details of driver and verifies it
Pollicino et al.	User start ride	-	Vehicle Owner detects misbehaviour during the ride
Safdar et al.	User drives to destination	-	-
Dzurenda et al.	User drives to destination	-	-
Zhou et al.	User drive to place	The vehicle show real-time information of the ride	-

Table 30. Payment Concepts

Payment Information type				
Activity	**Service Provider provides price of ride to user**	**User enters payment details using smartphone**	**The Payment provider validates the payment details**	**Service Provider receives payment for ride**
Auer et al.	Lessee receive the appropriate payment as cryptocurrency	Lessee makes payment through smart contract to ensure fair payout	-	Payment successful
Zhou et al.	Owner generates hours spent on ride and sends invoice	tenant transfer specific amount of money to owner	The payment provider validates card	Payment received

4 Licence

Non-exclusive licence to reproduce thesis and make thesis public

I, **Ijeoma Faustina Ekeh**,
(author's name)

1. herewith grant the University of Tartu a free permit (non-exclusive licence) to

   reproduce for the purpose of preservation, including for adding to the DSpace digital archives until the expiry of the term of copyright,

   A Recommendation Model for Security Risk Management in Car Sharing Scenarios,

   (title of thesis)

   supervised by Raimundas Matulevičius.

   (supervisor's name)

2. I grant the University of Tartu a permit to make the work specified in p. 1 available to the public via the web environment of the University of Tartu, including via the DSpace digital archives, under the Creative Commons licence CC BY NC ND 3.0, which allows, by giving appropriate credit to the author, to reproduce, distribute the work and communicate it to the public, and prohibits the creation of derivative works and any commercial use of the work until the expiry of the term of copyright.

3. I am aware of the fact that the author retains the rights specified in p. 1 and 2.

4. I certify that granting the non-exclusive licence does not infringe other persons' intellectual property rights or rights arising from the personal data protection legislation.

Ijeoma Faustina Ekeh
15/05/2024