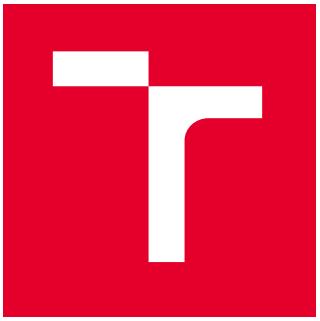
BRNO UNIVERSITY OF TECHNOLOGY

Faculty of Electrical Engineering
and Communication

MASTER'S THESIS

Brno, 2023 Bc. Norbert Lővinger



BRNO UNIVERSITY OF TECHNOLOGY

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION

FAKULTA ELEKTROTECHNIKY
A KOMUNIKAČNÍCH TECHNOLOGIÍ

DEPARTMENT OF TELECOMMUNICATIONS

ÚSTAV TELEKOMUNIKACÍ

DATA AND PRIVACY PROTECTION IN SMART TRANSPORT SERVICES

OCHRANA DAT A SOUKROMÍ V SYSTÉMECH CHYTRÉ DOPRAVY

MASTER'S THESIS
DIPLOMOVÁ PRÁCE

AUTHOR — **Bc. Norbert Lővinger**
AUTOR PRÁCE

SUPERVISOR — **doc. Ing. Lukáš Malina, Ph.D.**
VEDOUCÍ PRÁCE

BRNO 2023

BRNO UNIVERSITY OF TECHNOLOGY
FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION

Master's Thesis

Master's study program **Information Security**

Department of Telecommunications

Student: Bc. Norbert Lővinger ***ID:*** 197636

Year of study: 2 ***Academic year:*** 2022/23

TITLE OF THESIS:

Data and Privacy Protection in Smart Transport Services

INSTRUCTION:

Focus on cyber security in Intelligent Transport Systems (ITS) and smart transport services, e.g. car sharing, smart parking. Analyze current security threats, attacks and countermeasures in these areas and services. Evaluate and select appropriate methods for data security and privacy protection in smart transportation services. Furthermore, propose a solution to ensure data security and protect user privacy for the selected smart transport service. Prepare a basic verification implementation of the proposed solution in the chosen programming language. The main goal of the thesis will be a functional demonstration implementation of the proposed security and privacy protection methods. The security and performance analysis of the given solution will be provided.

RECOMMENDED LITERATURE:

[1] MENEZES, Alfred, Paul C VAN OORSCHOT a Scott A VANSTONE. Handbook of applied cryptography. Boca Raton: CRC Press, c1997. Discrete mathematics and its applications. ISBN 0-8493-8523-7.

[2] LONC, Brigitte, and Pierpaolo CINCILLA. Cooperative its security framework: Standards and implementations progress in europe. 2016 IEEE 17th International Symposium on A World of Wireless, Mobile and Multimedia Networks (WoWMoM). IEEE, 2016.

Date of project specification: 6.2.2023 ***Deadline for submission:*** 19.5.2023

Supervisor: doc. Ing. Lukáš Malina, Ph.D.

doc. Ing. Jan Hajný, Ph.D.
Chair of study program board

ABSTRACT

Smart Transportation Services are innovative means of user transportation. They offer numerous advantages including improved user comfort, enhanced safety, increased efficiency or better sustainability. A variety of sensors and units are collecting enormous volume of data including users' private information. This could result in serious consequences, if the data will not be preserved. Whether in services such as Smart Parking Services or Car Sharing Services, which are part of Smart Services, it is necessary to implement tools and techniques to provide protection for these data. In this thesis, Privacy Enhancing Technologies, which could protect data against multiple cyberattacks when implemented correctly, are further elaborated and analyzed in more detail. With the use of these techniques of data privacy protection, several phases of the car sharing process are described, in which these tools have been implemented as proof-of-concept in the Python programming language. Overall, 5 phases have been developed and evaluated, from which the conclusions are made. Privacy Enhancing Technologies are suitable for Car Sharing Services when they are applied in an appropriate way.

KEYWORDS

Smart Transport Services, Car Sharing Services, Privacy Enhancing Technologies, Cybersecurity, Data and privacy protection

ABSTRAKT

Inteligentné prepravné služby sú inovatívne spôsoby prepravy cestujúcich. Prinášajú množstvo výhod vrátane zvýšeného užívateľského pohodlia, zvýšenej bezpečnosti, vyššej efektívnosti alebo lepšej udržateľnosti. Množstvo snímačov a jednotiek zhromažďuje obrovské množstvo údajov vrátane osobných informácií používateľov. Ak tieto získané údaje nebudú chránené, môže to mať vážne dôsledky. Či už v rámci služieb, ako sú chytré parkovacie služby alebo služby zdieľaného využívania vozidiel, ktoré sú súčasťou inteligentných služieb, je potrebné zaviesť opatrenia a techniky na zabezpečenie ochrany týchto údajov. V tejto diplomovej práci sú ďalej rozpracované a podrobnejšie analyzované technológie na zvýšenie ochrany súkromia, ktoré by pri správnej implementácii mohli ochrániť údaje pred viacerými kybernetickými útokmi. S využitím týchto techník ochrany súkromia údajov je opísaných niekoľko fáz procesu zdieľania vozidiel, v ktorých boli tieto nástroje implementované ako proof-of-concept v programovacom jazyku Python. Celkovo bolo vytvorených a vyhodnotených 5 fáz, z ktorých sú vypracované závery. Technológie na zvýšenie ochrany súkromia sú vhodné pre služby zdieľania vozidiel, ak sa použijú správnym spôsobom.

KĽÚČOVÉ SLOVÁ

Inteligentné prepravné služby, Služby zdieľania vozidiel, Technológie na ochranu súkromia, Kybernetická bezpečnosť, Ochrana údajov a súkromia

ROZŠÍRENÝ ABSTRAKT

Inteligentné prepravné služby (angl. skratka **STS**) predstavujú pokročilé prepojené systémy, ktorých cieľom je poskytnúť inovatívne služby v oblasti prepravy cestujúcich alebo tovaru. Tieto systémy impementujú v sebe široké množstvo technológií a aplikácií na dostiahnutie **zvýšenej bezpečnosti na cestách, lepšej efektivite prepravy pri lepšej udržateľnosti.** Ku hlavným užívateľom týchto systémov patríte aj napríklad vy. Okrem vás to môžu byť napríklad samosprávy, ktorých cieľom je častokrát zvýšenie bezpečnosti v cestnej premávke na vlastnom území, návrhy na vylepšenie dopravnej infraštruktúry a celkové zvýšenie kvality života pre svojich občanov. Do tejto skupiny patria ďalej aj prepravné agentúry a operátory služieb, logistické prepravné služby, lokálny malí podnikatelia a v neposlednom rade každodenní dochádzajúci a cestujúci vo voľnom čase.

Medzi príklady použitia takýchto systémov patrí napríklad **systém riadenia premávky v reálnom čase** popísaný v sekcií 1.1, **služby inteligentného parkovania** v sekcií 1.6, **služby zdieľania vozidiel** v kapitole 2. Inteligentné parkovacie služby majú za cieľ ponúknuť efektívne riadenie parkovania v obmedzených priestoroch, zníženie času potrebného na nájdenie voľného miesta, možnosť rezervácie parkovacieho boxu vopred a zo získaných dát pomôcť samosprávam so správnym rozhodovaním pri tvorbe parkovacích plánov v danej oblasti.

Služby zdieľania vozidiel sa postupne stávali populárnejšími od konca minulého storočia. **Vysoké náklady na prevádzku a vlastnenie vozidiel, nedostatok parkovacích miest a vysoké ceny a dane na pohonné hmoty** sú hlavné dôvody veľkému rozmachu týchto služieb. Hlavné dôvody, ktoré výrazne ovplyvňujú adaptáciu služieb zdieľaných vozdiel sú **geografické a demografické faktory**. V rámci geografických faktorov rozhoduje hustota mestskej zástavby, dostupnosť verejej dopravy a parkovacích miest. Naopak demografické faktory hovoria o tom, že službu využívajú hlavne mladší ľudia, ktorí sa dožadujú vyššej mobility pri zachovaní častejších sociálnych interakcií, čo má výrazný vplyv na jej využívanie. Jednotlivé výhody a problémy spojené so službami zdieľaných vozidiel sú popísané podrobnejšie v sekcií 2.1. Existujú štyri typy služieb zdieľania vozidiel: **Zdieľanie na spiatočnú cestu, Zdieľanie na jednosmernú cestu, Vzájomné zdieľanie vozidla a Zdieľanie flotilových vozidiel**. Medzi najznámejšie služby zdieľaných vozidiel patria spočnosti ako **Zipcar, ShareNow, CityBee** alebo český **Car4Way** a estónsky **Autolevi**.

Ku hlavným cieľom a výzvam v oblasti inteligentných prepravných služieb patrí spoľahlivá integrácia údajov medzi rôznymi štandardmi a systémami, správna analýza získaných údajov s využitím umelej inteligencie a cieľom vylepšenia predpovedí a simulácií modelov, jednoduchšie zavádzanie týchto služieb do už existujúcej infraštruktúry pri zachovaní trvalej udržateľnosti a ochrane dát užívateľov.

Kybernetická bezpečnosť v inteligentných prepravných službách predstavuje jej dôležitú súčasť, ktorej sa zatiaľ nedostáva dostatočná pozornosť. Vzhľadom na to, ako rýchlo sa toto odvetvie vyvíja odvetvie, čelí jeho kybernetická bezpečnosť v súčasnosti novým výzvam. Akékoľvek kybernetické útoky na tieto služby môžu negatívne ovplyvniť bezpečnosť cestujúcich, narušiť dopravné služby a viesť aj ku vzniku hospodárskych škôd. A práve na efektívne riešenie týchto bezpečnostných problémov je potrebná hlavne **koordinácia medzi užívateľmi a správcami týchto služieb.** Takáto spolupráca dokáže výrazne zvýšiť šance na efektívnu ochranu služieb proti kybernetickým útokom (Tab. 1.4) a jej cieľom (Tab. 1.5). V rámci tejto diplomovej práce je podrobne skúmaná práve **problematika ochrany osobných údajov v inteligentných prepravných službách.** Intenzívny zber, spracovanie a zdieľanie údajov z rôznych zdrojov predstavuje riziko odhaľenia citlivých osobných údajov užívateľov služieb. Protiopatrenia na zamedzenie úniku dát sa skladajú z viacúrovňovej bezpečnostnej stratégie, ktorá v sebe zahŕňa **Administratívne, Fyzické a Technické zabezpečenie.** Každá inteligentná prepravná služba si musí vybrať najvhodnejšiu techniku na zabezpečenie údajov a ochrany súkromia na základe jednotlivých špecifických rizík, ktorým služba je vystavená.

Na základe výskumu sú kapitole 3 bližšie popísané **Techniky a nástoje na zvýšenie ochrany súkromia** (angl. skratka **PET**), ktoré v posledných rokoch rastú na popularite. Techniky a nástoje na zvýšenie ochrany súkromia slúžia na **ochranu dôvernosti, integrity a dostupností údajov** pri zachovaní správneho používania služieb inteligentnej prepravy alebo zdieľania vozidiel. Medzi hlavné výhody týchto techník patrí hlavne anonymita používateľov, kontrola nad ich osobnými dátami, minimalizovanie zbieraných dát, transparentnosť správy osobných dát a Privacy-by-Design. Naopak, keďže sa jedná ešte o pomerne nové techniky a nástroje, vznikajú tu problémy napríklad s interoperabilitou, rýchlosťou, využitím, cenou či falošným pocitom zabezpečenia osobných dát. Taktiež je nutné podokntúť, že tieto techniky a nástroje musia byť prispôsobené požiadavkám jednotlivého systému a to vyžaduje špecifické technické znalosti. Podrobné rozdelenie ponúkaných techník a nástrojov popisuje sekcia 3.2.

Praktická časť diplomovej práce v kapitole 4 sa zaoberá práve spojením Služieb zdieľaných vozidiel pri využití techník a nástrojov na zvýšenie ochrany súkromia, nakoľko aktuálne ponúkané služby na trhu neposkytujú žiadne otvorené informácie pre užívateľov akými technikami a nástrojmi sú ich osobné dáta pri využívaní služieb chránené. Na základe analýzy procesov typickej služby na zdieľanie vozidiel bolo určených 5 špecifických fáz, ktoré sú rozpísané viac do detaiov. Fázy predstavujú: **Autentifikáciu používateľa do služby, Výber vozidla cez zobrazenie na mapách, Prístup do vozidla, Monitorovanie vozidla a Zabezpečenú**

platba za službu. Každá fáza má predstavený problém, ktorý rieši pomocou zvolených techník a nástroj na zvýšenie ochrany súkromia a jej následnú implementáciu v **programovacom jazyku Python** s využitím viacerých dostupných modulov.

Všetky zvolené fázy a proof-of-concept implementácie boli testované na **Windows 10 Pro 64-bit zariadení s vybaveným Intel i7-6500U CPU a 16GB RAM**. Zvolenou verziou programovacieho jazyka Python bola **3.9.7** v programe **Visual Studio Code 1.78.0.** Testované boli časové náročnosti jednotlivých častí nástrojov na zvýšenie ochrany súkromia. Každé testovanie bolo overené viacerými opakovaniami a výsledok predstavuje získaná priemerná hodnota v milisekundách. Jednotlivé výsledky sú zobrazené v tabuľke 4.4 a vykreslené na obrázkoch 4.9. Finálny výsledok praktickej časti diplomovej práce hovorí o náročnej možnosti aktuálneho využitia techník a nástrojov na zvýšenie ochrany súkromia v službách zdieľaných vozidiel. Ich nasadenie v komplexných a reálnych službách inteligentnej prepravy môže ešte predstavovať množstvo rizík, ako aj zhľadiska funkčnosti a bezpečnosti, tak aj z hľadiska používateľského komfortu.

Všetky stanovené ciele diplomovej práce boli splnené.

LÖVINGER, Norbert. *Data and Privacy Protection in Smart Transport Services*. Brno: Brno University of Technology, Faculty of Electrical Engineering and Communication, Department of Telecommunications, 2023, 113 p. Master's Thesis. Advised by doc. Ing. Lukáš Malina, PhD.

Author's Declaration

Author:	Bc. Norbert Lövinger
Author's ID:	197636
Paper type:	Master's Thesis
Academic year:	2022/23
Topic:	Data and Privacy Protection in Smart Transport Services

I declare that I have written this paper independently, under the guidance of the advisor and using exclusively the technical references and other sources of information cited in the paper and listed in the comprehensive bibliography at the end of the paper.

As the author, I furthermore declare that, with respect to the creation of this paper, I have not infringed any copyright or violated anyone's personal and/or ownership rights. In this context, I am fully aware of the consequences of breaking Regulation § 11 of the Copyright Act No. 121/2000 Coll. of the Czech Republic, as amended, and of any breach of rights related to intellectual property or introduced within amendments to relevant Acts such as the Intellectual Property Act or the Criminal Code, Act No. 40/2009 Coll. of the Czech Republic, Section 2, Head VI, Part 4.

Brno ....

author's signature*

*The author signs only in the printed version.

ACKNOWLEDGEMENT

I would like to use this opportunity to thank everyone who has supported me during my university studies. First and foremost, I would like to express my sincere thanks to doc. Ing. Lukáš Malina, PhD. who has been my thesis supervisor and whose advice, assistance and encouragement have been important during this entire process. I am also grateful to prof. Raimundas Matulevičius, PhD. for his insightful guidance and advice during my study abroad and also M.Sc. Mariia Bakhtina for her professional thesis consultation.

To my family and friends, I would be always grateful for their love, continuous support and inspiration, as well as for helping me stay motivated and focused throughout the highs and lows of this journey. A collaborative and motivating environment for my development and growth was provided also by my classmates, who I also would like to thank for sharing their thoughts and opinions with me. Thank you all for being an integral part of my academic journey and for making this accomplishment possible.

This thesis is supported 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.

Contents

List of Figures

List of Tables

Introduction

The advancement of technology is having significant effects on a number of industries, including transportation. The issues associated with the traditional transportation system have given rise to a solution in the form of **Smart Transportation Services**. Numerous advantages of these services include reduced traffic congestion, increased transit effectiveness and support for environmentally friendly transportation.

The objective of this diploma thesis is to provide an in-depth theoretical analysis of Smart Transportation Services, with a focus on the advantages and disadvantages, its real-world applications and **data privacy protection of the users**. The thesis also describes **Smart Parking Services** as well as **Car Sharing Services** in greater detail and outlines their benefits, types, regulatory status and cybersecurity concerns. Research of **Privacy Enhancing Technologies** and its potential use in Car Sharing Services data and privacy preservation is also studied. Privacy Enhancing Technologies are crucial component of Car Sharing Services and could significantly improve users' privacy and security.

The practical part of the diploma thesis handles with the **implementation of selected Privacy Enhancing Technologies tools and techniques in selected 5 phases of the Car Sharing process**. The selected 5 phases represent User Authentication, Vehicle Selection, Vehicle Access, Vehicle Monitoring and Secure Payment phase. All implementations in the Python programming language have been tested for time complexity and the **results are presented**. The last section of the thesis discusses the potential for further research and its trends.

1 Smart Transport Services

Smart Transport Services (STS) and Intelligent Transport Systems (ITS) are advanced systems whose goal is to offer innovative services across all methods of transportation to improve user comfort, safety, sustainability and efficiency. These systems include a wide variety of complex technologies and applications, such as interconnected autonomous vehicles, advanced public transportation systems or traffic management systems.

Their different scopes and focuses are where STS and ITS separate the most. STS has a broader scope than ITS, which usually refers to the implementation of technology in order to improve the performance of certain modes of transportation, such as traffic management systems or traffic lights. With a focus on user experience and demands, STS aspires to seamlessly and effectively combine multiple types of transportation and services. [1, 2]

Main Advantages of STS

There are numerous advantages of STS for users, the environment and transportation systems. Here are a few of the main advantages of STS: [3, 4]

- **Enhanced Safety:** STS could significantly help to reduce number of traffic accidents and dynamically route traffic away from emergency vehicles trying to exit congested areas by providing real-time information to drivers and by automating certain safety-critical tasks.
- **Increased Efficiency:** Among the primary goals of STS is to improve traffic flow by providing real-time traffic data with a wide range of information to optimize the routing and scheduling of vehicles, resulting in reducing congestion in the cities.
- **Better Sustainability:** The significant environmental effect of transportation could be reduced by STS through improving system efficiency and enabling the use of alternative fuels, vehicles and other modes of transportation.

Common Users of STS

Governments, transportation agencies, logistical companies, commuters and small local businesses are among the STS' regular consumers.

- **Governments:** One of the the biggest users of STS since they could utilize it to improve their transportation infrastructure and reduce traffic. They could use the information collected by STS to decide wisely about developing a new infrastructure, using public transportation, and handling emergencies to improve overall quality of life in the community.

- **Transportation Agencies:** Ride-sharing services, taxis, delivery companies and public transportation systems could use STS to optimize their routes, lower fuel costs and boost overall operational effectiveness. Cost reductions and better customer service may result from this.
- **Logistics Companies:** Logistic movement of trucks and cargo could be tracked by using STS, which could improve their routes and keep an eye on the efficiency of their fleet. They may be able to cut delivery times, increase service dependability, and reduce costs as a result.
- **Travelers and Commuters:** Real-time information on traffic conditions and timetables for public transportation along commuters' routes could be extremely useful and increase comfort while traveling by reducing stress and irritation.
- **Local Businesses:** Using STS could decrease the price and delivery time for items from small local businesses to the neighborhood. It might increase and improve the overall competitiveness of local businesses.

There is another viewpoint on the benefits of ITS systems from the perspective of organizations, companies, partnerships and the academic community. These companies are involved in research, promotion, physical development, deployment and demonstration of ITS technology and applications. Some examples include organisations as ERTICO [5], INRIX [6], Siemens ITS [7], Commsignia [8].

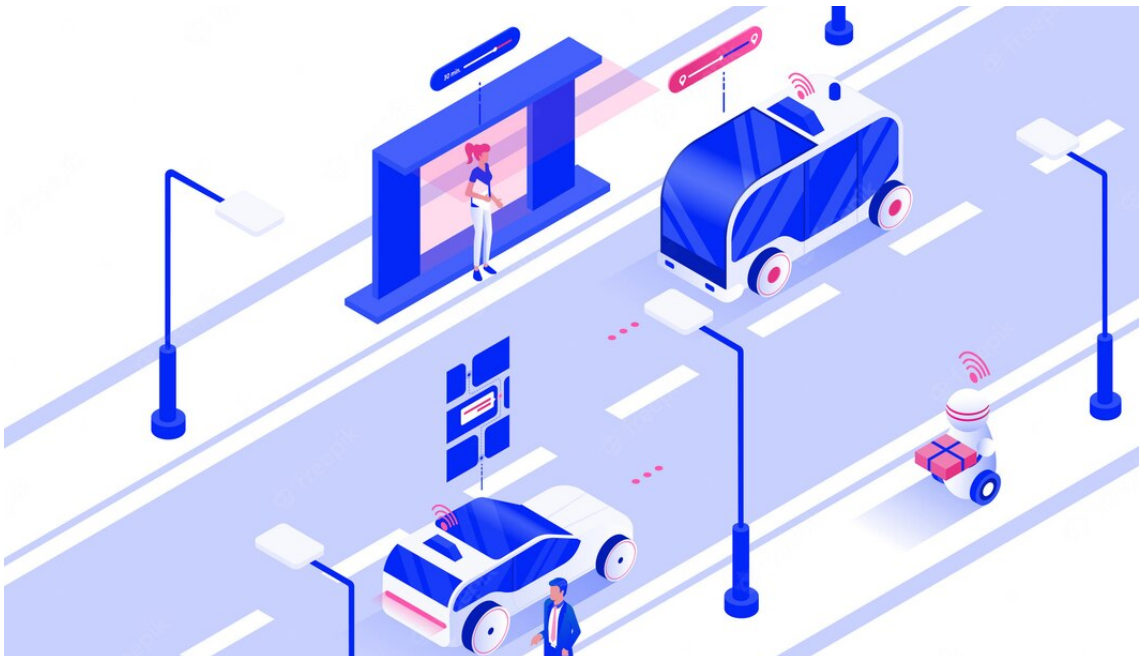


Fig. 1.1: Mostly Smart Transport Services users benefit from the inter-connectivity of these systems.

Examples of STS applications

- **Traffic Management Systems:** Continuously monitoring traffic conditions using sensors and cameras and provide real-time information to drivers and Traffic Control Centers (TCC), more in Section 1.1. Proper use of this information could improve traffic and reduce congestion. [9].
- **Smart Parking Services:** Make the most use of parking spots by utilizing technologies including sensors, cameras and communication systems. They assist drivers in finding available spots, monitor the status of slot occupancy in real-time and optimize parking fee pricing [10, 11]. Smart parking services are described in more detail in the Section 1.6.
- **Connected and Autonomous Vehicles:** These vehicles use sensors, cameras, lasers and other communication devices to communicate internally and to connect externally to other vehicles and the transportation infrastructure. This connectivity could enable advanced features, such as platooning[1] and collision avoidance. Using these technologies, Car sharing services could be developed to operate more effectively and safely. [12].
- **Pedestrian Tracking Systems:** Sensors, cameras and communication systems are used to accurately track pedestrian movement and schedule transportation services according to their needs. [13].
- **Real-time Ride Matching Services:** Utilizing real-time data and algorithms from these services to optimize the matching of passengers with available vehicles. The CSS could be more efficient if there were improved vehicle usage and fewer empty trips [14, 15]. The entire Chapter 2 is dedicated to Car Sharing Services.
- **Emergency Vehicle Priority Systems:** High reliable and demanding systems which utilize communication and detection technologies to grant priority to emergency vehicles at intersections and on roads. The city of Brno could also be proud of these systems [16, 17].
- **Advanced Public Transportation Systems:** Technologies including smart ticketing, real-time passenger information and vehicle tracking could be used to improve the effectiveness and convenience of public transportation [18, 19].
- **Road Weather Management Systems:** Data collected from weather sensors on the sides of the road, combined with weather forecasting computations, allows transportation authorities to make the appropriate decisions to ensure safety and mobility [20].
- **Freight Management systems:** Using of multiple technologies including GPS tracking, electronic information interchange and wireless communication

[1] A group of connected vehicles travel in close formation

could increase the effectiveness of freight transportation [21].

- **Advanced Traveler Information Systems:** Very popular systems in larger cities uses technology such as variable message signs, mobile applications, satellite maps and websites to alert drivers about traffic conditions, roadwork, accidents or other events that could affect their journey [22, 23].
- **Airport Surface Management Systems:** The effectiveness and safety of ground operations on the airports could be increased by utilizing technology using sensors, communication systems and optimization algorithms. They could lead to shorter wait times, more effective ground vehicle routing and better coordination of aircraft movement [24].
- **Modern Railway Control Systems:** Train operations could increase the efficiency and safety using GPS, sensors and various communication systems. They could be used to improve train routing and scheduling, automate certain operations and provide passengers or train operators real-time information [25].
- **Intelligent Street Lighting Systems:** To reduce the energy consumption of street lights are multiple sensors and communication systems used. They could be set up to dim or turn off the lights when not in use and modify the brightness of the lights based on the amount of ambient light [26].

Data Flow in STS

Smart Transport Services optimize the performance of the system by collecting and evaluating data from a variety of sources. **Data collection** is fundamental for providing the information required to make decisions and take action. A few examples of the data sources and technologies used are roadside infrastructure, crowdsourcing and vehicle-based sensors. Vehicle-based sensors are used to monitor vehicle position, speed and traffic conditions. Roadside infrastructure is installed to collect information regarding traffic flow, vehicle speeds and visit times. See more details in Section 1.1. Driver and passenger data could be collected as well using mobile applications and other crowdsourcing methods.

The ability of the components to communicate with one another is critical to the STS's proper operation. Real-time information and **data transmission** between vehicles, roadside infrastructure and centralized control systems becomes possible. Examples of wireless communication technologies used for transmitting data include Wi-Fi, Dedicated Short-Range Communications (DSRC) and cellular networks (3G, 4G, and 5G). Wired communication is an additional option to Wi-Fi. In large-scale systems, it provides better bandwidth, more reliable communication over greater distances with minimal noticeable signal losses and lower costs.

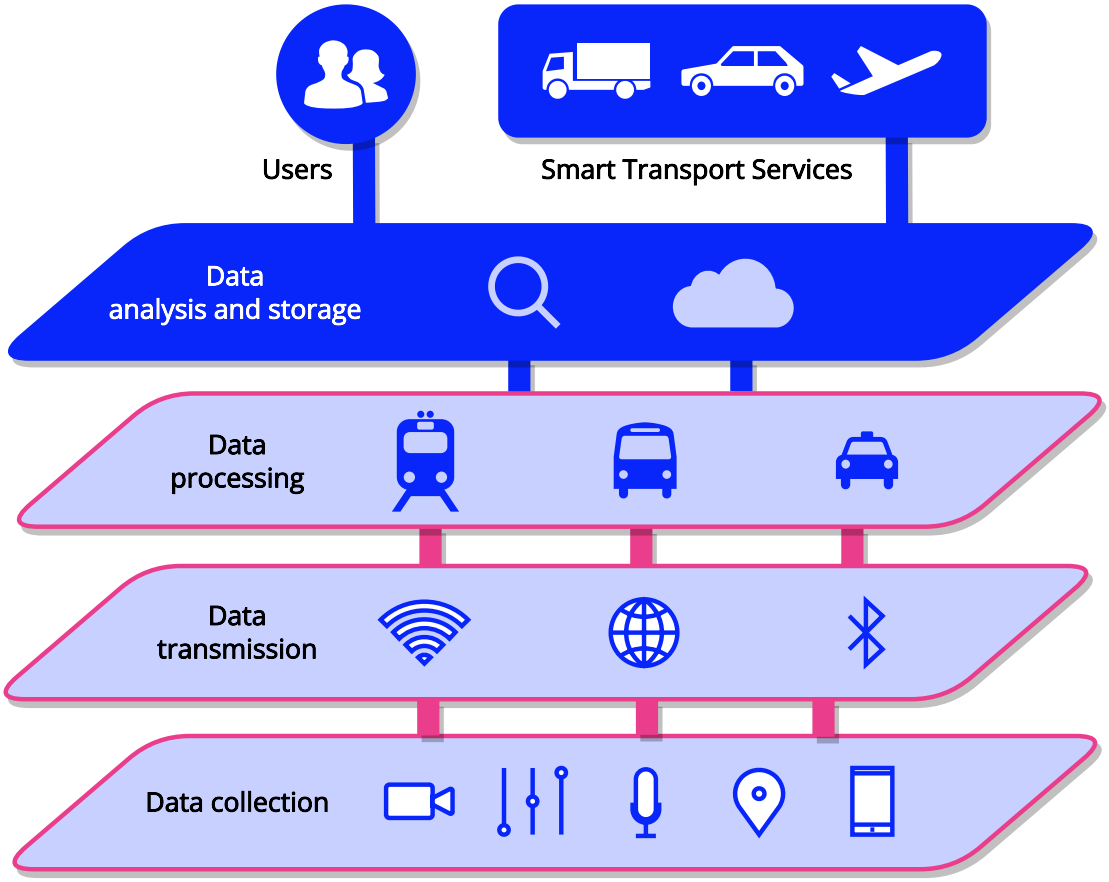


Fig. 1.2: Data Flow in Smart Transport Services.

Data processing and analysis are the following steps in developing and training machine learning models to forecast traffic patterns during rush hour, identify bottlenecks in congested areas before accidents or take the necessary actions to optimize traffic flow and safety. The STS application's goal determines how the data are examined once they have been collected.

Secure **data storage** and management technologies, such as encryption, data anonymization, access control or privacy enhancing technologies (PET), protect data against unauthorized access, modification and theft. An incident response plan is also an important factor to help reduce damage and accelerate system restoration in the case of a security breach, hardware failure or other unforeseen consequences.

The full data flow process in STS is illustrated as single layers in Figure 1.2. More detailed information about these cyberattacks are available for reading in Table 1.4. PET are described in more detail in the entire Chapter 3. [27, 28, 29]

Goals and Challenges in STS

The STS are complex systems of connected technology and services. Adoption and deployment of STS are not without challenges. In order to increase transportation efficiency, safety and sustainability, these concerns have to be addressed and resolved in the fields of law and regulations, ethics, technology and economics. [1, 30, 31]

- **Data Integration:** It is a significant challenge as STS is built up of many different communication standards, various types of data sources and various already installed systems. The objective is to increase these systems' overall effectiveness and productivity, which could result in cost savings and improved quality. This could also be supported by approved international standards, which are described in the Section 1.2.
- **Data Management and Analysis:** They are necessary to protect the privacy and integrity of the enormous amount of data created by various sources. Using machine learning and advanced processing techniques, useful information could be retrieved from the data. Making smarter choices could be a result of better STS data management.
- **Deployment and Adoption:** A continuous process that starts with education and awareness campaigns to non-technical audiences about the main benefits, overcomes challenges including securing funding for implementation costs and also legal perspectives about privacy and data security to propose and develop useful solutions to make cities more livable.
- **Sustainability:** To accelerate the development of smart cities, STS have to be developed and maintained in a way which could reduce the negative environmental impacts of transportation—primarily the decrease of CO2 emissions. To make STS more sustainable, emissions have to be reduced and air quality needs to improve.
- **Cybersecurity and Data Privacy:** Due to the environment's vulnerability to cyberattacks, which could cause data breaches, system failures or other security challenges, these are significant STS concerns. Therefore, STS have to preserve the privacy of users whose information is collected and protect the data from unauthorized access or modification. Types of cyberattacks are described in the Section 1.3. Privacy preserving could be done with PET, which are discussed in Chapter 3.

1.1 Basic Components of STS

On-Board Unit

The On-Board Unit (OBU) refers to an inside vehicle component which is capable of storing a variety of sensors, cameras, GPS units and other devices. OBUs are widely used in STS for collecting real-time data about the system's performance, including traffic conditions, schedules for public transportation and other events that could have an impact. The data which OBUs have collected could be connected with and transferred to a central server or another system for further processing and analysis. [32]

Fig. 1.3: On-Board Unit from company CiDi [33].

Road Side Unit

The Road Side Unit (RSU) is an essential part which could be found usually at the intersection or along the side of the road. It acts as a link between the infrastructure and vehicle, allowing information to be transferred back and forth between them. RSU communication supports cooperative collision warning systems, enables the exchange of information between vehicles and traffic management systems and provides real-time traffic data. [34]

OBUs and RSUs in STS are able to communicate with one another in real-time using a variety of systems and protocols, such as cellular, Wi-Fi and DSRC. These technologies could improve the efficiency, economy and safety of the transportation sector.

Fig. 1.4: Road Side Unit from company Siemens ITS [35].

Sensors

A variety of sensors are used in STS to collect information on the system's performance, including data about the current road condition, traffic congestion, accidents, work zones and parking availability. [36]

Several examples of sensors used frequently in STS include:

- **Vehicle Sensors:** They collect data on a vehicle's performance and operation, including its speed, acceleration, fuel efficiency and other factors.
- **Traffic Sensors:** They collect data about speed, volume and other aspects of traffic on roads and highways to optimize traffic management systems.
- **Environmental Sensors:** They collect data about the weather, air quality and other environmental factors in real-time that could have an impact on the transportation system.
- **Cameras:** They capture visual information about the transportation system, such as traffic patterns, schedules for public transportation and other incidents.
- **GPS:** They collects location information about vehicles and other devices in the transportation system, enabling real-time tracking and routing of vehicles and other objects.

Signals and traffic controls

The operation of the STS could be improved by multiple types of signal and traffic control systems. The following represent a few frequent STS examples:

Fig. 1.5: Leddar T16 Traffic Sensor from LeddarTech Inc. [37]

- **Traffic Lights:** They could manage the movement of traffic at intersections, to reduce delays and increase the effectiveness of the transportation system by using advanced algorithms and real-time data.
- **Adaptive Signal Control:** They modifies the timing of traffic signals based on real-time information about the flow of traffic in order to maximize efficiency and reduce delays.
- **Ramp Metering:** They regulates the flow at which vehicles enter the area using traffic signals or other control devices, decreasing congestion and improving safety.
- **Traffic Cameras and Sensors:** They collect real-time visual data of the traffic flow, vehicle speeds and other road conditions to increasing safety.
- **Variable Message Signs:** They could display real-time updates traffic conditions, public transit schedules and other events, which could have an impact on the transportation system.
- **Parking Management:** They controls parking availability and helps drivers locate available parking spots. Real-time data on parking availability, dynamic pricing and reservation platforms could be included.
- **E-toll:** They uses drivers' toll payments to speed up toll collection and reduce off waiting times.
- **Speed Cameras:** They track and record passing vehicle speeds, capturing data that could be used to identify speeding cars and enforce speed restrictions to increase safety.

Traffic Control Centers

Traffic Control Centers (TCC) are significant STS components that perform a variety of important functions, such as controlling traffic flow, identifying and responding to traffic incidents or providing drivers real-time information about the conditions on the road ahead. **Data from multiple sources and sensors are usually received and processed in real-time by these systems**, which are typically centralized in one location. [38]

Fig. 1.6: Smart Transport Services are interconnected components mentioned above. [39].

1.2 International Standards in STS

Compliance to international standards is necessary for the development and deployment of STS in order to ensure interoperability, dependability and security. Numerous international standards groups, including ISO, IEEE and ETSI, have established standards for many ITS/STS components, including cybersecurity, data privacy and technical requirements for communication protocols or data sharing. **Compliance with these standards is necessary for the efficiency and security of these systems**, global collaboration and the development of advanced innovative solutions in the field. The following are some of the most known standards:

Tab. 1.1: ISO standards

Standard	**Description**
ISO 13111-2:2022	The use of personal ITS stations to support ITS service provision for travellers. [40]
ISO 15638 series (Parts 1 to 24)	Framework for collaborative telematics applications for regulated commercial freight vehicles. [41]
ISO 17419:2018	Specifies the requirements for the secure authentication and authorization of ITS using global unique identifiers. [42]
ISO/TS 19091:2019	Using V2I and I2V communications for applications related to signalized intersections. [43]
ISO 21177:2023	STS station security services for secure session establishment and authentication between trusted devices. [44]
ISO 24102 series (Parts 1 to 6)	Provides guidelines and recommendations for cybersecurity in ITS. [45]

Tab. 1.2: IEEE standards [46]

Standard	Description
IEEE 1609 Family	It provides a comprehensive set of guidelines and specifications for ensuring the security and privacy of wireless communication in vehicular environments. These standards are critical to the development and deployment of safe and secure STS systems. [47]
IEEE 802.11p	Specifies the communication protocols for wireless access in vehicular environments (WAVE). One of the key aspect is security, which is designed to ensure the privacy and confidentiality of data transmitted over the WAVE network. [48]

Tab. 1.3: ETSI standards [49, 50]

Standard	Description
ETSI TS 102 940	This standard specifies the architecture and protocols for Cooperative Intelligent Transport Systems (C-ITS) communication. It defines security and privacy mechanisms for protecting against unauthorized access, tampering and interception of C-ITS messages. It also specifies authentication, confidentiality, integrity and non-repudiation services. [51]
ETSI TS 102 941	This standard specifies the security requirements for Cooperative Intelligent Transport Systems (C-ITS) communication. It defines security services and protocols for ensuring privacy, confidentiality and integrity in C-ITS messaging. [52]
ETSI TS 103 097	This standard specifies the security services and protocols for secure communication between vehicles and between vehicles and roadside infrastructure. It defines requirements for authentication, confidentiality, integrity and non-repudiation. [53]

1.3 Cybersecurity in STS

Thanks to improvements in the Internet of Things, cloud computing and artificial intelligence, the development of STS is accelerating at a never-before-seen rate. **These technologies are expected to change how we travel, improve efficiency, reduce emissions and improve road safety.** However, considering how quickly STS industry is developing, cybersecurity is currently facing new challenges. There are more potential threat vectors as STS become more complex and connected. Unfortunately, STS are vulnerable to cyberattacks because cybersecurity measures are unable to keep up with the rate of STS development.

STS is still developing and is in its early stages at the moment. Many service operators are still experimenting with multiple technologies and looking for the best methods for implementing them. A lot of operators are working with limited resources, which makes it difficult to develop complete security solutions. Moreover, **cybersecurity is not always a top priority for STS operators**, as they focus on providing efficient and cost-effective transportation services. And a result, the security features in STS are often overlooked, leaving these systems vulnerable to threats.

The absence of cybersecurity in STS could have negative consequences. Cyberattacks on STS have the possibility to negatively impact passenger safety, disrupt transportation services and lead to economic damages. As an example, hackers could hijack vehicles, change traffic lights or steal private data from these systems. These attacks could **result in accidents, congestion and even fatalities**. It is essential to develop comprehensive cybersecurity solutions for STS that could reduce these risks.

Coordination between transport service operators, cybersecurity experts and government agencies **is necessary for solving the cybersecurity-related security concerns** that STS are experiencing. In order to make sure that security measures are implemented throughout the STS system, cybersecurity experts should be involved in STS system development from the initial phase. Government agencies should develop regulations and guidelines that require the implementation of cybersecurity measures in STS. Only by taking these coordination measures, there could be guarantee for the security and safety of STS while preserving its effectiveness and resilience. [54]

Tab. 1.4: General cyberattacks in STS [55, 56].

Attack	**Description**
Malware	By modifying files, stealing data or tampering with the system's functionality, malware or ransomware could infect the STS and cause fatal damages.
Distributed Denial-of-Service	Due to the network overload and crash caused by jamming or flood attacks, the STS becomes unable to operate.
Eavesdropping	Hackers could be man-in-the-middle in system communication in order to steal data or manipulate instructions.
Spoofing	To access data or take control over the STS, hackers could pretend to be a legitimate system or user using sybil attack.
False information	Hackers purposefully spread false information to manipulate with the transportation system or mislead users.
Social engineering	Phishing attacks and other scams could be used by hackers to fool users into providing important information.
Side channels	To get over traditional security measures, hackers could target other systems or properties.
Profiling	Attacks to target weak points in STS by analyzing user behavior, traffic patterns or frequently traveled paths.

Tab. 1.5: Targets of cyberattacks in STS.

Attack	**Description**
Vehicle hijacking	Hackers could be able to obtain access to a vehicle's control unit without permission and take over operations including braking, steering or acceleration [57].
Safety compromise	Hackers could put at risk passenger safety by accessing into STS controlling security features including airbags or seat belts.
GPS spoofing	Hackers could tamper with GPS signals to steer vehicles off track or bring them to a stop.
Traffic signal manipulation	By remotely manipulating the timing of traffic lights, hackers could control traffic signals to increase congestion or cause accidents.
Infrastructure damage	Hackers or terrorists could physically harm transportation infrastructure, such as bridges or tunnels, to obstruct the operation of STS.
Payment fraud	Hackers could manipulate payment systems, such as parking meters or toll booths, to steal money or cause financial losses to STS provider.
Data theft	Hackers have the ability to steal private data from STS, including personal, location or payment data.

Data Privacy concerns in STS

Data privacy is essential to ensuring cybersecurity in STS. The privacy and security of users could be seriously threatened by the enormous volume of data collected in these systems. **STS heavily relies on data collection, processing and sharing** which exposes users' sensitive information among different entities. Significant consequences, including financial losses, social harm and even physically injury to individuals, could result from failing to protect these data.

Tab. 1.6: Data Privacy Threats in STS.

Threat	Description
Data Breaches and Mining	Data breaches are one of the biggest threats to data privacy in STS. The sensitive information collected by STS, including location data, travel patterns and personal data, are vulnerable to hackers. Collected data could be analysed by hacker in order to find out patterns and insights to follow individuals or perform targeted advertising [58].
Unsecured Communication	Various communication protocols are implemented by STS to exchange data between network components. Data interception and illegal access could result from using insecure communication channels.
Insider Threats	Data privacy could be seriously threatened by individuals who have been granted access to STS data. These insiders have the potential to violate privacy by purposefully or accidentally misusing the data they have access to.

Unauthorized Access in STS

Unauthorized access is also one of the main security concerns of STS as it could affect connected transportation infrastructure. It might occur when a person or machine accesses STS data or systems **without the necessary authorization or credentials.** System failures, loss of user data and privacy and other serious consequences could be the result of this kind of attack. The following threats could provide unauthorized access to a hacker.

Tab. 1.7: Unauthorized Access Threats in STS.

Threat	Description
Weak Authentication	Hackers could be able to overcome authentication and gain unauthorized access through the use of weak or easily guessed passwords, outdated authentication protocols or incorrectly set access controls.
Social Engineering	Users could be mislead into giving their login credentials or other sensitive information by social engineering attacks including phishing emails or phone calls, which could be used to gain unauthorized access.
Misconfiguration	Hackers could be able to gain unauthorized access by exploiting unpatched vulnerabilities or poorly configured systems.

Physical Security in STS

The physical security is a **crucial non-digital component of STS infrastructure**, which needs to be also protected. The STS infrastructure is vulnerable to a variety of physical security threats that could disable or damage STS functionality and significantly impact transportation services.

Tab. 1.8: Physical Security Threats in STS.

Threat	Description
Vandalism and Theft	Vandalism or theft, which could include the removal of necessary infrastructure, equipment damage and graffiti, is a frequent physical security risk to STS infrastructure.
Sabotage	Equipment or the entire system could be harmed as a result of it, either on purpose or by mistake.
Natural Disasters	Disasters including floods, earthquakes or hurricanes are just a few examples of how they could seriously damage STS infrastructure, disrupting travel plans and causing security risks.

Countermeasures and Best Practices

STS operators should implement **a multi-layered security strategy** that combines technical, physical and administrative controls to protect against cyberattacks in STS.

Protections against malware, data encryption and anonymization, strong password authentication and monitoring systems should all be part of **technical countermeasures**. **Physical countermeasures** including access controls and surveillance systems could help stop attacks including theft, vandalism or sabotage. **Administrative countermeasures** as employee awareness and training programs could be used to avoid attacks that rely on social engineering methods as phishing.

Penetration testing, software security-by-design and regular security audits could all be implemented to identify and correct vulnerabilities in STS systems before they are exploited by hackers.

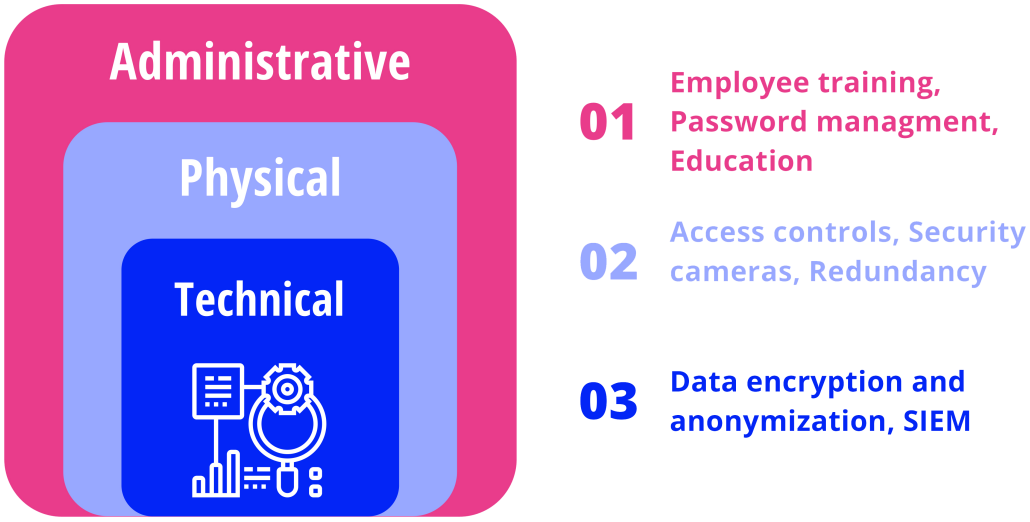


Fig. 1.7: Multi-layered security strategy should be implemented to STS.

Cybersecurity Evaluation in STS

The most appropriate techniques for data security and privacy protection in STS have to be chosen by taking into account the specific risks and threats to which the entire system is subject to. There is a need for industry-wide collaboration to develop **robust security guidelines and processes** due to the growing risk of cyberattacks and the potential harm that STS cybersecurity breaches could cause to the economy and society. The lack of cybersecurity guidelines in STS is **an alarming issue** which has to be solved quickly.

Tab. 1.9: Cyberattacks Countermeasures in STS.

Countermeasure	Description
Privacy Enhancing Technology (PET)	An efficient protection against data privacy cyberattacks in STS by providing tools and methods to protect sensitive data using techniques as data encryption and anonymization. More information in Chapter 3.
Role-Based Access Control (RBAC)	Based on employment roles, authorizations and responsibilities, RBAC could be used to limit access to sensitive information and system functions. It offers granular access control and reduces the possibility of unauthorized access.
Data Encryption	STS operators could avoid data breaches and data mining by implement security measures such as data encryption and anonymization, firewalls, IDS/IPS or PET.
Security Information and Event Management (SIEM)	STS data exchange could be monitored and unauthorized access attempts could be quickly identified using SIEM systems. Additionally, SIEM could be used to correlate events across several systems to spot sophisticated attacks techniques and offer useful information.
Password Management	By using multiple factors of authentication (MFA) and strong passwords, unauthorised access attacks could be stopped. Furthermore, it is important to enforce strict password policies and make regular password changes obligatory.
Employee Training and Education	STS operators could implement understandable security measures for their employees including access controls, firewalls, SIEM systems and End point security systems to prevent data breaches and data mining. They should regularly perform security audits and vulnerability evaluations on their systems in order to look for any possible weaknesses.

- **Lack of Consistency:** STS cybersecurity is lacking in widely acknowledged standards, making the system open to cyberattacks.
- **The Lack of Adequate Legal Recourse:** Hackers who abuse STS are frequently difficult to identify and bring to justice.
- **Insufficient Regulatory Control:** The vast majority of authorities lack the knowledge and resources necessary to effectively manage STS cybersecurity.
- **Lack of Standardized Security Procedures:** While some service operators could have strong cybersecurity measures in place, others might have few or none at all. Hackers could simply exploit these vulnerabilities as a result of this inequality.
- **Accountability:** Breach of STS cybersecurity could have enormous negative effects on the economy and society.

To overcome these issues, STS cybersecurity **needs to be standardized.** The best security practices, regulations and laws developed as part of this standards should be required for all STS companies.

The smart transportation industry should also invest in cybersecurity education and training to **increase awareness of cybersecurity threats and best practices.** Other potential countermeasures for these concerns include the implementation of data encryption, access control systems, network segregation, IDS/IPS, disaster recovery planning systems and other above mentioned solutions. In order to identify vulnerabilities and take precautions to eliminate them, regular security audits and assessments should be performed. This subject is further elaborated in more detail in the following reference [59].

1.4 Related Research in STS

Smart Transport Services are still considered to **be a new field of research**, which combines modern technology and data-driven approaches to achieve the mentioned benefits in Chapter 1. As a result, there have been more research work and projects in recent years focused on developing and implementing STS.

Fredianelli et al. (2022) have been working on a system of using low cost cameras to increase traffic flow efficiency in the Italian city of Piombino [60]. **Dynamic price techniques** are also a key component for handling a wide range of STS challenges, including parking, traffic flow or the public transportation usage. Saharan et al. (2019) have performed a systematic review on the use of these techniques [61]. Pedestrians safety and protection is discussed by El Hamdani et. al (2020) in [62] as a component of STS, who significantly influence traffic flow, road infrastructure and vehicle design.

An equally important area for research is **smart parking management** where Dzurenda et al. (2021, 2022) have been exploring the possibilities of using blockchain technology and smart contracts for parking in city centre zones [63]. The same author also extended his research with information about user data protection [64] in Czechia. Alsafery et al. (2018) proposed a functional system to the parking issue with a significant reduction in the amount of data transmitted in order to reduce energy consumption [65]. Smart parking services are described in more detail in the Section 1.6.

Car and scooter sharing services, which are growing popular in STS, now offers the best research opportunities. Mounce et al. (2019) who has been investigating the possibility of connecting electric cars with a one-way car sharing system. The benefits of autonomous driving, usability, legislation and current solutions have been elaborated by the authors [66]. Roblek et al. (2021) provided us a closer look at the fundamental issues with the CSS and how they affect urban sustainability [67]. Nansubuga et al. (2021) presented an extensive systematic review of CSS with in-depth analyses of this trend [68].

Several studies have looked into the use of **Privacy Enhancing Technologies** in STS, which are also described in Chapter 3. For instance, Pollicino et al. (2021) have developed a new accountability protocol for use in real car sharing environments [69]. In another study, Huang et al. (2020) proposed the DAPA architecture to address customers' concerns about data privacy in relation to CSS operators [70]. Avodji et al. (2016) have developed a prototype implementation of privacy-preserving meeting points computing in response to the finding that meeting locations using CSS could represent significant data privacy concern [71]. After the conclusion of this thesis, an attached bibliography provides further specific literature references.

1.5 Current Solutions in STS

Current smart transport services **have fundamentally changed how we travel, park and share vehicles.** These modern technology-based solutions have increased everyone's accessibility and convenience when it comes to transportation. A brief overview of current STS solutions are shown in the tables 1.10 and 1.11 below.

1.6 Smart Parking Services

A technology-driven system offers **efficient parking management** while improving user experience. The smart parking service (SPS) falls under the general category of STS, which aim to improve urban sustainability, optimize the use of existing infrastructure and reduce traffic. Many different parties are involved in SPS, including:

- **Users:** They could access parking services including reservations, payments and real-time information through mobile application or web portals to connect with SPS.
- **Technology Vendors:** Developing and place into use hardware and software components for SPS, as well as providing technical support and maintenance services.
- **Parking Lot Operators:** They are in charge of monitoring the management of parking spots, the installation and upkeep of technological infrastructure and the security and safety of users.

Main Advantages of SPS

Smart parking services have numerous advantages over traditional parking options for both users and the general public. [95]

- **Time-Reducing:** SPS use technology to reduce down on time spent trying to find parking spots, which minimizes traffic congestion and fuel consumption.
- **Efficient:** SPS give users the option to reserve parking spots ahead of time, reducing the possibility of overbooking and the requirement for conventional ticketing systems.
- **Convenient:** SPS increase convenience and user experience by offering real-time information on parking availability, costs and distances from the destination [65].
- **Future Planning:** By providing useful information about parking usage, traffic flow and user habits, SPS could improve urban planning.

Tab. 1.10: Current Solutions in STS – part 1 of 2

Solution	Description
Car sharing Car4way, HoppyGo, Autonapul [72, 73, 74]	Progressively used platforms allow individuals to rent out their own vehicles or use cars owned by the service operator, providing a convenient and sustainable alternative to car ownership, mainly in the cities and suburban areas. Solutions are discussed in more detail in Chapter 2.
Bike and scooter sharing Rekola, Nextbike, Bolt, Lime, Tier [75, 76, 77, 78, 79]	Bike and e-scooter sharing systems have become increasingly popular in cities around the world, providing a convenient and environmentally friendly mode of last mile type of transportation.
Smart car parking Brno smart parking [80]	Smart parking solutions use sensors and real-time data to guide drivers to available parking spots, reducing congestion and reducing the time and fuel wasted searching for a place to park. They are usually linked to the mobile application for easier parking navigation and more flexible payments options depending on the specific location. More details in Section 1.6.
Automatic e-toll MYTOCZ, Tool4Europe, EETS [81, 82, 83]	Electronic toll systems are widely used in many countries, providing a convenient and fast way to pay tolls without stopping the vehicle. These systems have improved the efficiency of toll roads and reduced the environmental impact of congestion.
Emergency Call System STMicroelectronics [84]	Lifesaving technology used in vehicles that automatically sends an emergency call to a response center in the event of a crash. The system is triggered by a device in the vehicle, such as an airbag sensor, that detects a crash and sends a message to the response center with the vehicle's location and other relevant information.

Tab. 1.11: Current Solutions in STS – part 2 of 2

Solution	Description
Real-time Passenger Information System DPMB Info App [85]	System provides real-time information about bus, tram and train schedules, delays or route changes to passengers through various channels such as variable signs, mobile applications and websites.
Public Transport Network Planning and Optimization ESRI, PTV VISUM, CONDUENT Transportation [86, 87, 88]	System uses advanced analytics and simulation tools to optimize public transport networks, reduce costs and improve passenger experience [89]. The Digital twin model is virtual system representation that models its life cycle with updated real-time data and uses simulation, machine learning and reasoning to help decision-making for real system [90].
Demand Responsive Transport Liftango, Ridandgo [91, 92]	System provides on-demand transportation services to passengers in areas with low or irregular demand, reducing the need for fixed-route services [93].
Intelligent traffic lights and signs TrafficSmart [94]	Systems use real-time data to optimize the timing of traffic lights, reducing wait times and improving the flow of traffic. Most often used to create a "Green Wave" to move more traffic quickly in or out of the city centre.

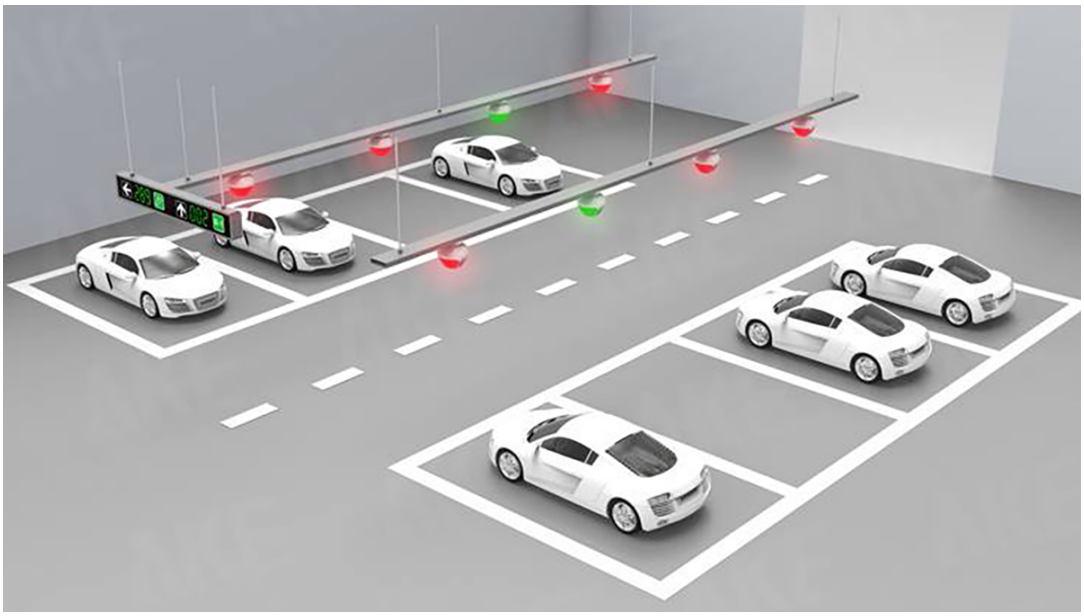


Fig. 1.8: Smart parking service simplifies the parking process with the use of multiple sensors.

Challenges and Concerns

Despite the advantages, smart parking services meet a number of challenges, such as concerns about privacy protection and cybersecurity, problems with interoperability and the requirement for infrastructure and technology investment.

Service operators have to collaborate together to develop common guidelines and procedures that allow seamless integration of various SPS in order to overcome these challenges. Potential risks associated with data privacy and security could also be reduced by using PET tools.

Data and Privacy Protection

Smart parking services collect and process user's private information, such as vehicle number plate, vehicle type and location information. Therefore, while developing and implementing SPS, **data protection and cybersecurity are the most important concerns.** Industry best practices including secure software development, network and access control should generally be implemented by SPS. [96]

Services are also vulnerable to a range of cyberattacks mentioned in the Section 1.3. Because PET enable the processing and analysis of sensitive user data without disclosing the information to unauthorized parties, their usage in SPS could assist with improving data and privacy protection. Chapter 3 provides more information about PET tools.

Solutions and Future Work

Since parking has become a big issue for users, as cities become more densely populated, **SPS have attracted a lot of interest**. Many approaches have been proposed to address this issue with the goal to optimize parking spots, reduce traffic and improve user experience.

- **Reservation Systems:** Implementing reservation systems allowing users reserve a parking spot in advance is popular SPS feature. It is especially helpful in congested locations or at events when parking is limited and users might have to wait a while.
- **Real-Time Parking Availability:** Using sensors to find available parking spot is one of the most popular implemented feature of SPS. Drivers could quickly recognize a parking spots by using mobile applications, websites or variable signs to communicate this information to them.
- **Dynamic Pricing:** To maximize parking usage, SPS often employ dynamic pricing. Cities could encourage users to park in underused locations, easing congestion in busy areas, by altering parking prices based on demand [97].

Future work in the SPS is likely to focus on emerging technologies such as:

- **Autonomous Parking:** Autonomous parking systems use sensors and artificial intelligence to find available parking spots, park vehicles automatically and then return them when needed by users.
- **Shared and Predictive parking:** Shared predictive parking is a concept in which parking spots are shared upfront among users. With this strategy, fewer parking spots could be needed and CSS could become more popular.
- **Integration with Public Transportation:** Another area of future research for SPS is integration with public transportation networks. Cities could provide users more effective transportation options, reducing traffic congestion and improving mobility.

The importance of this technology is constantly defined by the smart parking services which **deal with the growing parking problem** in densely populated urban areas. SPS provide many advantages, but there are also challenges such as cybersecurity and user data privacy protection that need to be resolved.

In this context, the integration of **PET could help in protecting user information** while still preserving the main operation of parking services. Future work in this field could be focused on innovative technologies including shared parking, autonomous parking and integration with transportation systems. Each of these technologies have the potential to completely transform urban mobility and improve the standard of living for city residents. This research is beyond the scope of this thesis.

2 Car Sharing Services

The concept of car sharing dates back to the 1940s, but it was not until the 1990s when Car Sharing Service (CSS) as a form of transportation has gained popularity. Due to the **high cost of owning, maintaining a car and a lack of parking spots**, car sharing has become popular throughout Europe as an alternative to owning a vehicle. Car sharing also became popular in the US as a response to the high cost of living in the cities and increased environmental awareness. Reducing the production of greenhouse gases, reducing traffic and offering economical options for transportation are some of the main reasons for car sharing.

The rise of these services are due to advancements in technology which made car sharing more accessible and convenient. **Car sharing is now a popular application of STS** and well-established transportation system in many countries worldwide, with a significant impact on the transportation industry. [98, 102]

Adoption Factors for CSS

The adoption of car sharing services is **significantly influenced by geographic and demographic factors**. CSS are more likely to be adopted at a higher rate in with dense populations and few available parking spots.

Geographical factors including urban density, accessibility to public transportation and availability of parking spots also affect the popularity of car sharing. **Urban areas with dense populations** and few parking spots are those where car sharing is most common. The adoption of car sharing also depends on the availability of public transportation, as people may choose to use their own vehicles when public transportation is unavailable or unreliable.

Millennials and younger people are more likely to take advantage of CSS than older generations because to their lower incomes and higher mobility needs, according to **demographic factors**. Their tendency for social interactions and dedication to a more environmentally friendly way of living are the explanations for this. Additionally, people who utilize CSS as an alternative for owning a car are more likely to be individuals who live in households with fewer cars. [98, 99]

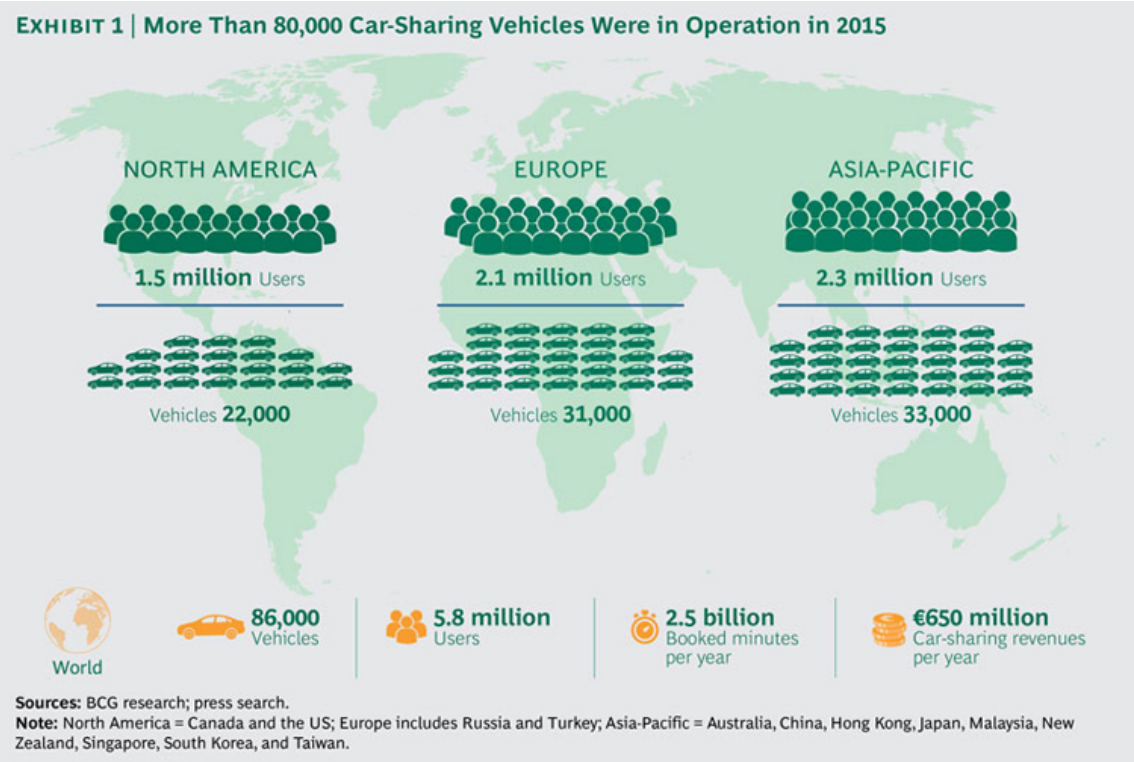


Fig. 2.1: Car Sharing Services are increasing their popularity every year [100].

2.1 Advantages and Challenges

In comparison to conventional modes of transportation, CSS have numerous benefits and advantages. Here are some of the main advantages of using CSS:

- **Flexibility:** CSS are more flexible than other forms of transportation. There are many different vehicles types available to chose from, including budget, luxury and electric vehicles. Furthermore, services usually offer 24/7 accessibility that allow users to reserve a vehicle for as little as an hour, making it practical for individuals who simply need a vehicle for short trips or specific purposes.
- **Cost Savings:** CSS offer a cost-effective alternative to car ownership, especially for people who drive occasionally. It also provides a cheap choice for many individuals because it reduces the cost of car maintenance, insurance and fuel [101].
- **Environmentally Friendly:** The positive impacts of CSS on the environment are among their most important advantages. By reducing the number of vehicles on the road, car sharing lowers carbon emissions and air pollution. Increasing the popularity of CSS could help create a healthier and cleaner environment.

- **Social Impact:** CSS encourage resource sharing and collaboration, which has a positive impact on society in general. People could save money and contribute to a more sustainable future by sharing a vehicle. In urban areas where social isolation is problematic, CSS may encourage opportunities for interaction and community building.
- **Traffic Reduction:** CSS assist in reducing traffic congestion and reduce parking demand in urban areas by lowering the number of vehicles on the road, which results in quicker commutes and improved air quality. Additionally, they could lower the demand for parking spots, which is crucial in urban areas where parking is expensive and difficult to find.

While CSS have several advantages over traditional forms of transportation, they also have certain disadvantages that may restrict their practicality. The following are some of the significant challenges and disadvantages of using car sharing:

- **Limitations and Restrictions:** Limitations and restrictions on usage apply to CSS, particularly in terms of where and how the vehicles could be driven. As an example, CSS may place usage restrictions on certain geographic areas, the types of roads or highways that could be used and mileage or time limits. Users who need more flexibility in their transportation options may find these limitations to be a drawback.
- **Availability and Accessibility:** Certain areas, particularly those that are rural or suburban, may not have easy access to the availability of CSS. Furthermore, during periods of high demand, such as rush hour or weekends, CSS could not have enough vehicles accessible. It could be challenging for users to locate to a available vehicle when they need one as a result of this.
- **User Behavior:** User behavior could have an impact on the overall effectiveness and efficiency of CSS. Users might damage the vehicle, return it late or leave it at the wrong location, besides other incidents. These challenges may raise expenses for the CSS, which may result in higher user prices.
- **Dependence on Technology:** Technology and infrastructure are necessary for CSS to operate efficiently. As an illustration, CSS use GPS systems, mobile applications and wireless communication networks to monitor vehicle usage and support user interactions. The effectiveness and availability of the service may be affected by any disruptions or failures in these systems.
- **Insurance and Liability:** Insurance and liability concerns for CSS could have an effect on the service's overall cost and feasibility. The cost of liability insurance to cover accidents and damages is often required of service operator. In addition, there could be legal and regulatory barriers for CSS in terms of liability and insurance at the specific location of use of the service.

2.2 Types of CSS

Car sharing is a practical and cost-effective alternative for owning a vehicle because it enables users to borrow a vehicle for a short period of time. Various kinds of CSS are offered on the market, including: [68, 103]

- **Round-trip Car Sharing**
- **One-way Car Sharing**
- **Peer-to-peer Car Sharing**
- **Fleet-based Car Sharing**

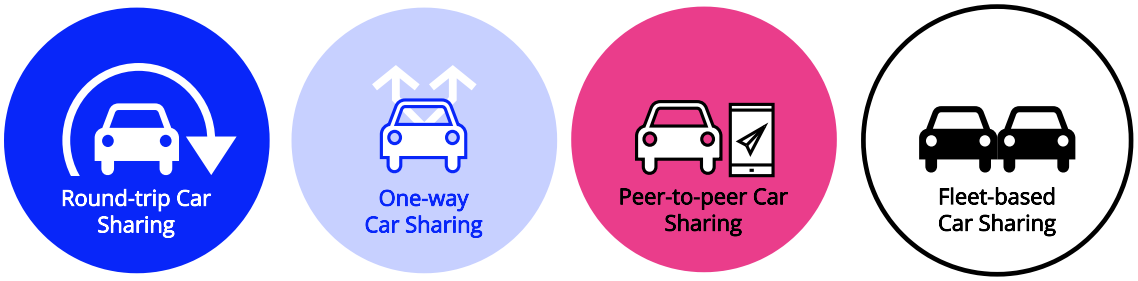


Fig. 2.2: Various types of Car Sharing Services.

Round-trip Car Sharing

The most popular type of Car sharing is round-trip service. In this type of service, users pick up a vehicle from a predetermined location, drive it to their destination and then drop it off again at the same location. This type is popular among users who require a vehicle for a specific trip or work, such as grocery shopping or appointment running.

One-way Car Sharing

A relatively new form of CSS is one-way Car sharing. Within the defined zones of service, users could pick up a vehicle from a specific location and drop it off at another. Users who need to travel between two or more locations but do not want to return the vehicle to its starting location typically opt for this form.

Peer-to-peer Car Sharing

Individuals could rent out their personal vehicles to other users with Peer-to-Peer Car sharing. This type of business concept is popular by individuals who would like to earn additional income by renting out their vehicles when they are not using them.

Fleet-based Car Sharing

In a fleet-based Car sharing model, a business or organization owns a fleet of vehicles that become available to users. Companies and organizations who want to give their employees or customers access to vehicles use this type of car sharing.

CSS is a rapidly growing industry, with many players on the market. Some of the major players in the car sharing industry include:

Tab. 2.1: Major players in different types of CSS

Title	Type of CSS	Headquarter	Available locations
Getaround	Round-trip	San Francisco, US	US, EU[104]
Zipcar	One-way	Boston, US	US, EU, Asia [105]
ShareNow	One-way	Berlin, Germany	Europe [106]
Bolt Drive	One-way	Tallinn, Estonia	Baltics, France [107]
CityBee	One-way	Vilnius, Lithuania	Baltics [108]
Car4Way	One-way	Poděbrady, Czechia	Czechia [72]
Turo	Peer-to-peer	San Francisco, US	US, EU, Australia [109]
Autolevi	Peer-to-peer	Tallinn, Estonia	Baltics [110]
Enterprise	Fleet-based	St. Louis, US	Worldwide [111]
Hertz	Fleet-based	Chicago, US	Worldwide [112]

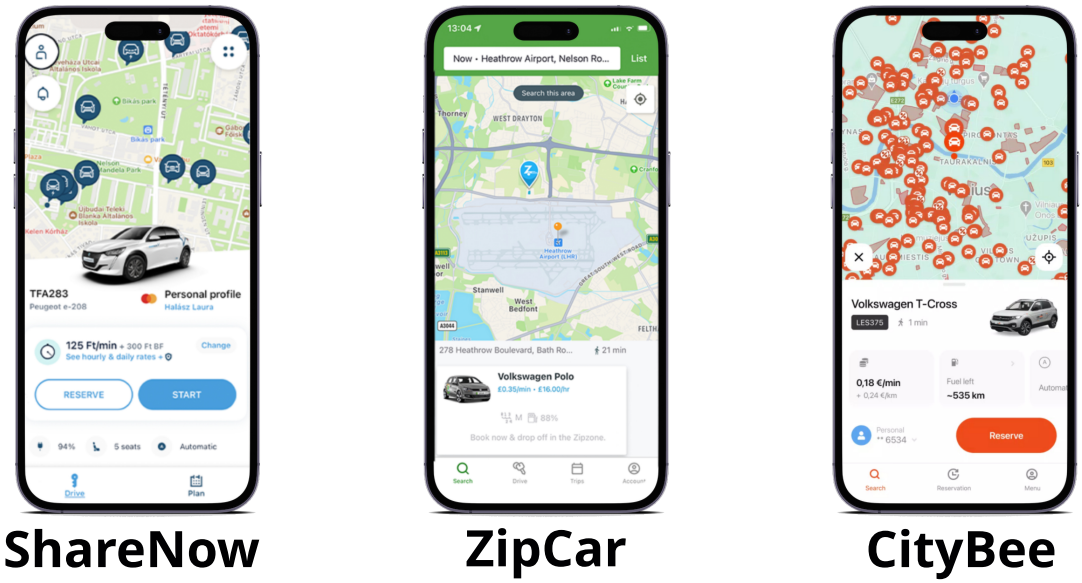


Fig. 2.3: User-friendly and easy-to-use interface of Car Sharing applications.

2.3 Requirements for CSS

A number of requirements needs to be completed in order for these CSS to operate safely and reliably. These requirements deal with **user eligibility and authentication, vehicle selection and maintenance, insurance coverage and privacy protection.**

Eligibility and Authentication of Users

A user's eligibility and authentication have to be a prerequisite for CSS. To rent and use the available vehicles, users must be of a **certain age and hold a valid driving license**. CSS have to perform background checks on customers in order to check for traffic violations, criminal records and other factors that could affect their ability to drive safely.

Vehicle Selection and Maintenance

In order to gain an advantage in the market, local authorities or particular service could **set specific technical requirements for the vehicles** used in their services. Depending on the specific area in which the service is provided, these criteria may change. Vehicles have to meet, for example, stricter emission requirements in areas with high pollution levels. Additionally, in order to maintain vehicles in top condition and safe to operate, they have to go through regular maintenance and safety inspections.

Responsibility and Insurance Protection

To protect both the Service operator and the users, CSS have to have responsibility and insurance protection. For the purpose of **covering accidents and damages** that could happen while using a vehicle, liability insurance is a need for CSS. The same rules apply to users of the service. The vehicles themselves have to be insured by CSS against additionally risk factors such as damage, theft, weather and more.

Data and Privacy Protection

For the purpose of of protecting user personal data, CSS have to comply to **local data protection and privacy regulations**. CSS frequently collect a lot of user data, such as demographic information, driving records and patterns of use. This kind of information needs to be collected and stored in an encrypted format, with the appropriate levels of security in place to protect against data breaches and other security risks mentioned in the Table 1.4.

Additionally, CSS **have to open and transparent about how user data are collected, analyzed, and shared.** The use of user data for unapproved goals, such as marketing or other commercial activities, have to be forbidden. Unfortunately, this approach is often not followed and therefore in the Chapter 3 is described a possibility of using PET tools in the processes of CSS.

2.4 Regulatory Area in CSS

The legal status of CSS has been a subject of research and controversies, particularly in relation to regulatory guidelines, compliance standards, and numerous challenges.

CSS regulations could vary **significantly between countries and geographical areas.** The European Union's regulation on CSS acts as the foundation for the legal framework guiding these services in Europe by removing administrative obstacles and promoting the car sharing initiation [113, 114]. Services may be also subject to regulations on user eligibility requirements, safety, emission levels, insurance, responsibility, as well as data and privacy protection. Service operators could face significant compliance challenges, especially if they operate in multiple locations with unique regulatory frameworks.

Tab. 2.2: Comparison of some selected regulations between the EU and the US.

Regulation	**Europe**	**United States**
Driver's License	Must have a valid driver's license.	
Age Limits	Typically 18 years old.	Varies by state, typically 18 or 21 years old.
Insurance	Mandatory for all car sharing services.	Requirements vary by state.
Data Protection	Stricter regulations under the GDPR.	Regulations vary by state [115]
Regulations	More unified and strict framework at the EU level.	Regulations could vary by state and local government.

With ongoing discussions and arguments about regulations and compliance requirements, the **legal status of CSS is still evolving**. However, there are some new trends that are appearing in this field. For example, many service operators are switching to electric vehicles (EV) to reduce emissions and promote sustainability. Also, services are looking into new revenue models like **Peer-to-Peer sharing and subscription-based services**. With an emphasis on these reasons, it is highly possible that CSS will continue to evolve in the future.

2.5 Security Threats in CSS

To protect user safety and privacy, it is important to address the security concerns that CSS also present. The risk factors that CSS address are explained along with the techniques and processes that could be used to mitigate them. They could be vulnerable to both physical and cyberthreats, which could potentially harm both the vehicle and the user. For perspective, Figure 2.4 illustrates the areas of cyberattacks on vehicle systems over the last 10 years.

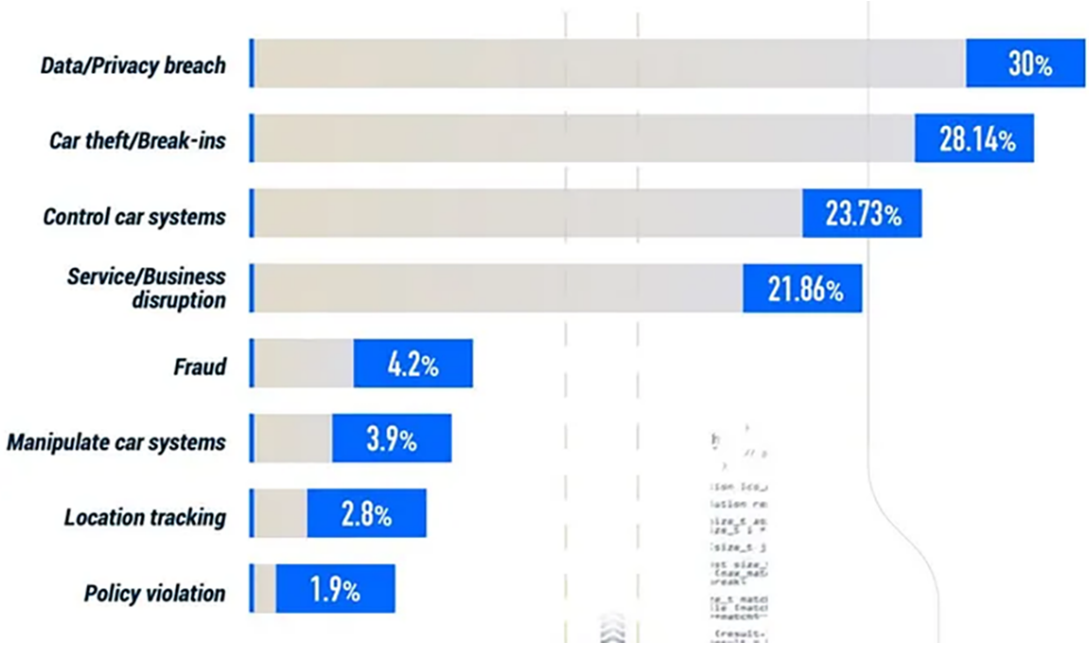


Fig. 2.4: Areas of cyberattacks on vehicle manufacturers over the past decade [116].

Physical Threats

Physical threats to the vehicle and the user belong to the CSS most evident security issues. Theft, vandalism and even carjacking are a few of examples of this behavior. In order to protect their vehicles from these hazards, service operators have to **take appropriate safety precautions**, including GPS monitoring, remote locking and unlocking, cameras and alarms that could stop unauthorized access to the vehicle. Furthermore, a lot of CSS require users to show a **valid driver's license and credit card** before renting a vehicle, which could help prevent fraud.

Cybersecurity Threats

CSS raise concerns about cybersecurity risks to user and vehicle security. Modern connected vehicles are more vulnerable to cyberattacks (tab. 1.4) which could

threaten user safety and privacy. Having technologies including GPS tracking, in-car entertainment systems with mobile data hot-spot and Bluetooth connectivity, **vehicles are becoming ever more interconnected**. Due to this, they are susceptible to cyberattacks which could compromise user data, safety or even provide hackers access to the vehicle. To prevent such attacks, CSS have implemented in place a number of protections and guidelines to reduce these concerns. [117]

Data and Privacy Threats

Data and privacy vulnerabilities are an increasing security concern for CSS. Users' data, including credit card information, location data and other personal identification, could be stolen by hackers. CSS have to put in place strong data protection mechanisms, including data encryption, access controls and frequent security audits to identify and mitigate potential vulnerabilities.

Countermeasures

To mitigate these threats, CSS could implement several countermeasures, including **strong data encryption methods, access control with two-factor authentication, vehicle monitoring and control systems, advanced prevention and analytics algorithms, regular security audits and user training.**

In addition to these countermeasures, CSS could also leverage advanced technologies to detect and respond to potential threats in real-time. It is important to highlight that depending on the specific area, users or vehicle services, CSS could encounter different threat models. For example, services operating in metropolitan areas could be more vulnerable to physical threats, while those operating in rural areas could encounter different challenges with users demand or vehicle access. CSS need to perform an **in-depth risk assessment and develop a comprehensive security strategy** that is suited to their specific needs and requirements, to effectively address these challenges. The long-term success of CSS could be ensured by implementing strong security measures and taking a proactive approach to risk management.

3 Privacy Enhancing Technologies

In recent years, Smart Transport Services have become increasingly popular due to their ability to provide efficient, sustainable and environmentally friendly mobility solutions. Widely used services such as smart parking services and car sharing services rely on data collection, processing and analysis, which **raises new concerns about privacy and data protection.**

Privacy Enhancing Technologies (PET) have been developed to address and solve these concerns by providing **techniques and tools to protect the confidentiality, integrity and availability of data** while still enabling correct use of the mentioned STS. PET could be extremely important in the STS context for preserving privacy of the user. The large amount of sensitive data which STS generates about travel patterns, sensors, user behavior and preferences could lead to privacy violations, such as unauthorized tracking or profiling of users. [118] This chapter presents an overview of PET with an additional focus on Smart Transportation Services, Smart Parking Services and Car Sharing Services.

3.1 Advantages and Challenges of PET

PET have multiple advantages, including:

- **Anonymity:** PET could provide anonymity to users by masking their identity and personal information, thus protecting them from unauthorized tracking or profiling.
- **Control over Personal Data:** PET could enable users to have greater control over their personal data by allowing them to choose what information is shared and with whom and for what purpose.
- **Privacy-by-Design:** PET could be designed to prioritize user privacy from the outset, rather than as an afterthought. This means that privacy is built into the technology itself, rather than being an add-on or optional feature.
- **Minimizing Data Collection:** PET could be designed to minimize the collection of personal data, thereby reducing the risk of data breaches or unauthorized use of personal information.
- **Transparency:** PET could enable greater transparency around how personal data are being collected, used and shared, which could help build trust between users and service operators.

Also in terms of STS, PET could provide a number of advantages. First, PET could help in ensuring **compliance to privacy regulations** and preserving the privacy of users. Second, PET could **increase user trust and confidence** in STS, which

will encourage more use of these services. Third, PET could provide STS operators an **advantage over their competitors**. These services could use privacy as a marketing aspect to attract more new customers. Fourth, by removing any biases or mistakes caused on by privacy concerns, PET could **improve the accuracy and quality** of data collected.

Despite the advantages of PET, there are also challenges and requirements that need to be considered, including:

- **Interoperability:** PET could have issues with other privacy-enhancing technologies or services, which could lead to fragmentation and decrease their effectiveness.
- **Performance:** PET could cause systems or devices to function less efficiently. For some users, this could result in discomfort and decrease in performance.
- **Usability:** PET could be challenging to put into use and require technical knowledge. Due to this, it could be more difficult for users to adapt new technologies and use them on a regular basis.
- **Cost:** Some PET could cost considerably much to use or request continuous subscription payments. As a result, users with limited resources could consider them to be unsuitable.
- **False Sense of Security:** PET are capable of giving users a false sense of security, making them believe that their personal data are protected in STS systems, when in reality they could still be accessible due to misconfiguration or unauthorized access.

Additionally, PET could impact the usability, speed and efficiency of STS as they **need to be tailored to the system's requirements**, taking into account the type of data collected and analysed, the level of privacy that is required and the regulations that have to be complied with. There are still additional challenges with STS to overcome as complexity of integration decentralized PET solutions on existing systems, **balancing act between data privacy and system functioning** and implementation cost with ongoing support.

3.2 Types of PET

PET could be divided into three groups including statistical, cryptographic and other types. [130]

Cryptographic PET

To protect sensitive data, cryptographic PET use data encryption and decryption techniques. Even if the data are intercepted by an unauthorized party, these technologies guarantee that the data remains confidential and protected. **Homomorphic Encryption** (HE), **Secure Multi-Party Computation** (SMPC), **Zero-Knowledge Proof** (ZKP), **Private Information Retrieval** (PIR) and **Group and Ring Signatures** (GRS) are just a few examples of cryptography tools. [135]

- **Homomorphic Encryption:** A cryptographic technique which allows useful computations on encrypted sensitive data without first decrypting them. A homomorphic encryption technique known as **somewhat homomorphic encryption** (SHE) only allows addition or multiplication operations to be performed on encrypted data [136]. Algorithms **ElGamal** is multiplicative in its homomorphism. $\alpha \epsilon Z_p^*$ where p is a prime, α is a generator of Z_p^*. α and β are chosen to $\beta \equiv \alpha^a$. Variables p, α, β are public, a is private. Secret random number is $r \epsilon Z_{p-1}$. Then the following statement is valid:

$$Enc(x, r) = (\alpha^r \ mod \ p, x * \beta^r \ mod \ p)$$

  The more sophisticated technique is **fully homomorphic encryption** (FHE), which allows any computations to be performed on encrypted data same as on non-encrypted data. FHE is an efficient tool for preserving private information while allowing its processing by third parties, such as in cloud computing systems. Currently developed FHE protocols include Microsoft SEAL, PALISADE or openFHE. FHE continues to be a **subject of ongoing research**, therefore it is not yet easily available for use in everyday scenarios. [137]

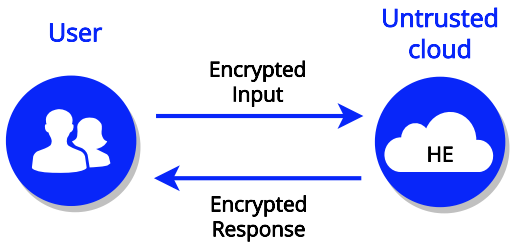


Fig. 3.1: Outsourcing computation to an untrusted third party is a typical implementation of FHE.

- **Secure Multi-Party Computation:** A cryptographic technique which allows multiple parties to perform computations on their inputs without revealing their personal inputs to each other. This method comes in useful when parties lack full confidence in other parties but still have to collaborate together to compute a function.

$$F(x_1, x_2, x_3) \;=\; (y_1, y_2, y_3)$$

Regarding privacy protection, collaboration and robustness, SMPC has a number of advantages. But it also comes with disadvantages in terms of computational complexity, scalability and requirements for skill. SMPC includes **Shamir Secret Sharing, Yao's Garbled Circuits, Oblivious Transfer and other FHE techniques**. [138]

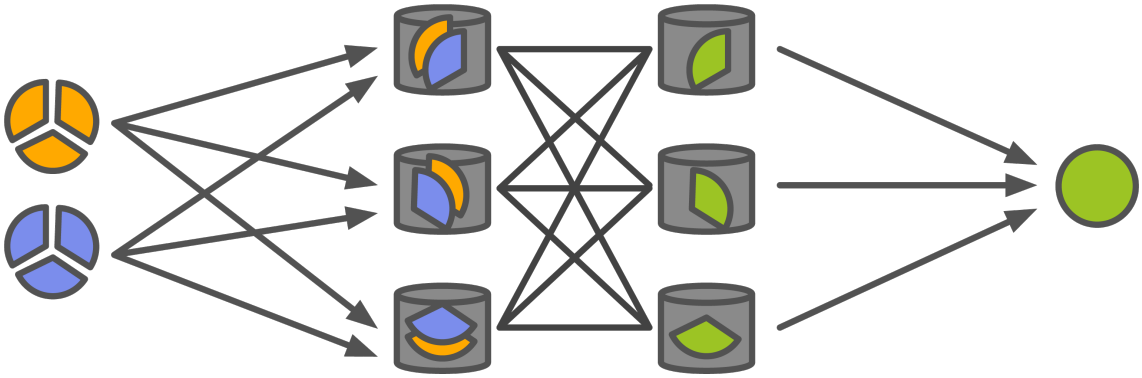


Fig. 3.2: Using the MPC protocol, two values are secretly shared across three separate nodes, which together create the result [139].

- **Zero-Knowledge Proof:** A cryptographic technique which allows a prover to demonstrate knowledge of a fact to a verifier without revealing any information about the fact itself. The verifier is convinced that the prover knows the information, but does not learn nothing else. **The preservation of privacy, the high level of security and quick deployment** represent some of ZKP's main advantages. The limitations are side-channel attacks vulnerabilities, high complexity, which requires special knowledge and limited application. ZKP could be used for user validation, access control, voting systems, digital rights protection or any knowledge proof. **Interactive, non-interactive and statistical proofs are main ZKP categories.** [140, 141]

Mathematical expression of an interactive proof where Alice wants to prove Bob that she knows a secret x without giving any information about x. Bob already knows $f(x)$. Alice could make $f(x)$ public and then prove that she knows x through an interactive exchange with anyone.

$$
\begin{aligned}
&A : publishes\ f(x)\ =\ g^x\ mod\ p \\
&A : chooses\ r \\
&A : sends\ u\ =\ f(x) \\
&B : could\ not\ verify \\
&B : sends\ e\ ==\ 0\ ||\ 1 \\
&A : verifies\ if\ e == 0\ :\ v\ =\ r;\ e == 1\ :\ v\ =\ r + x \\
&B : verifies\ if\ e == 0\ :\ Bob\ has\ random\ r \\
&B : u == g^x\ mod\ p \\
&B : verifies\ if\ e == 1\ :\ u * f(x)\ =\ g^x\ mod\ p
\end{aligned}
$$

At the entrance of a cave with two separate entrances leading to two distinct paths (A and B), Alice and Bob find themselves. Both paths are connected by a door inside the cave, but it requires a secret code to open. Bob (the tester) owns this code, and Alice (the verifier) wants to acquire it, but she first wants to be certain that Bob is telling the truth.

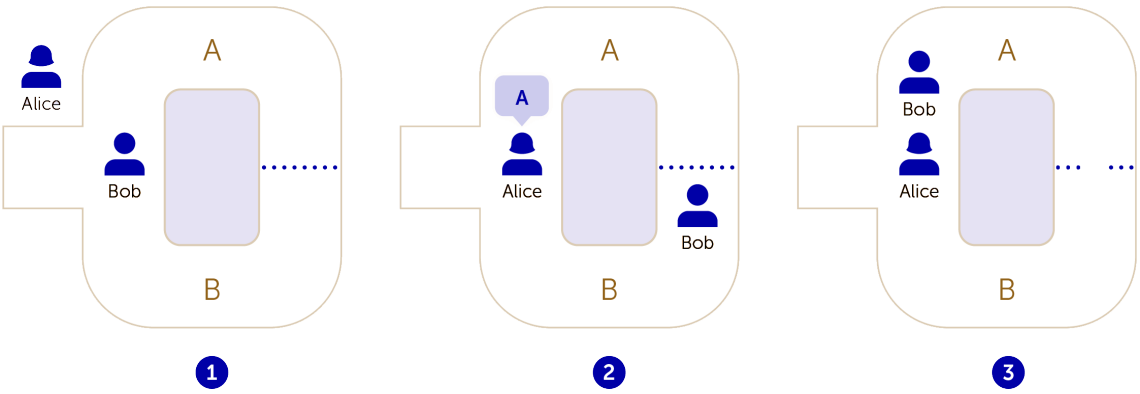


Fig. 3.3: Using the example of the cave to illustrate the Zero Knowledge Proof [141].

- **Private Information Retrieval:** A cryptographic technique which allows users to access databases without revealing any information about the data being accessed or the query being executed. PIR has disadvantages, which include a high computational cost and the **requirement of a trustworthy third party to facilitate the process.** Data analytics, finance and health care are just some of the industries where PIR has numerous uses. [142]
- **Group and Ring Signatures:** A cryptographic technique which allows users to sign a message or document anonymously or on behalf of a group to provide anonymity and privacy. Any member of the group could use the group private key to sign a message or document in anonymity. However, if necessary, the group manager could trace the signature back to the specific member. Similar to group signatures, ring signatures do not require a group manager. Instead, a user could select a group of public keys from a pool of available keys and any key in the group could have been used to sign the message or document. Therefore, the signature is unable to be linked to the initial user as a result. As opposed to potential misuse, which is the main disadvantage, advantages include anonymity, hidden identity, and privacy protection. There are a variety of real-world applications for this technique, including **anonymous online voting systems, anonymous digital contracts or transactions and whistleblowing.**

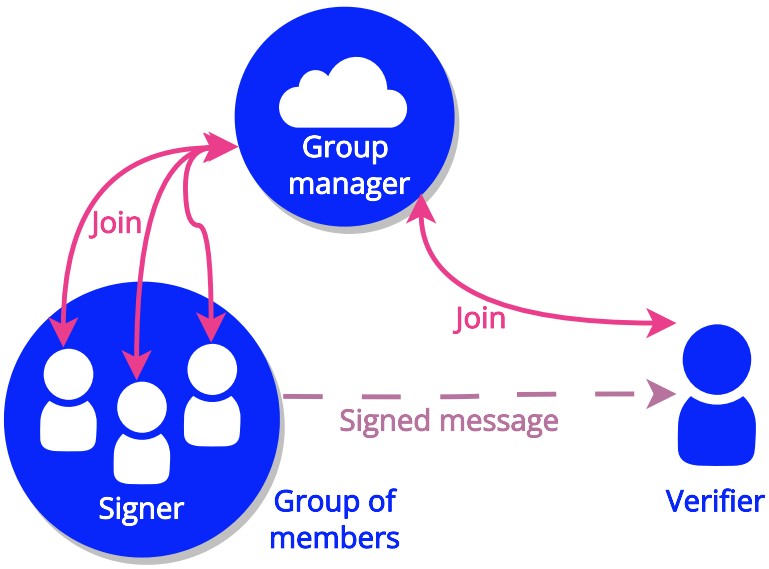


Fig. 3.4: Group Signatures with the manager for individual signature key management. The verifier does not know who in the group has signed the message.

Tab. 3.1: Selected Cryptographic PET.

Technology	Protocols and Frameworks
Homomorphic Encryption	ElGamal [119], Goldwasser–Micali [120], OpenFHE frameworks [121], SEAL [122], Lattigo[123]
Secure Multi-Party Computation	Shamir's secret sharing [124], Yao's Garbled circuit, Oblivious transfer [125]
Zero-knowledge proofs	zk-STARK [126], Libra [127], Aurora [128]
Group and Ring Signatures	BBS [129], RSA [150]

Statistical PET

Using the statistical techniques, statistical PET could anonymize and obfuscate data while still allowing the mining of valuable knowledge. In applications including medical research or marketing analysis, these technologies are frequently used to exchange data while still preserving privacy. Techniques as **Differential privacy** (DP) **Pseudonymization**, **Anonymization**, **Synthetic data generation** (SDG) and **Federated learning** (FL) are covered in statistical PET. [130]

- **Differential Privacy:** A statistical technique, which preserves individual data privacy while allowing valuable insights that could be gathered from the data. The primary goal of differential privacy is providing a mathematical guarantee that the data released from a dataset does not expose any private information about any of the individuals in the dataset. It works by **adding random noise into the dataset**, making it difficult for an hacker to identify whether some individuals are in the dataset. Original data are not changed using this technique. In order to be sure that it does not compromise the data's overall utility, the noise is carefully adjusted. A parameter called epsilon, which controls the amount of noise inserted to the dataset, determines the level of privacy protection.

  The probability that $f(D)$ will return a value in S for any subset S of the output range of the query function f is ϵ times the probability that $f(D')$ will return a value in $S+\delta$ for two datasets D and D' that differ by a single record.

This has the following mathematical expression:

$$P[f(D)\ \epsilon\ S]\ \leq e^{\epsilon}\ *P[f(D')\ \epsilon\ S]\ +\ \delta$$

Differential privacy offers the advantage of being able to provide **high levels of privacy while also allowing insightful data analysis.** It is a flexible technique that could be used in a variety of scenarios. On the other hand, it additionally considers into account computing complexity and technical expertise, which could make it challenging to implement in some scenarios. Online advertising and health care research are examples of real-world applications for differential privacy.

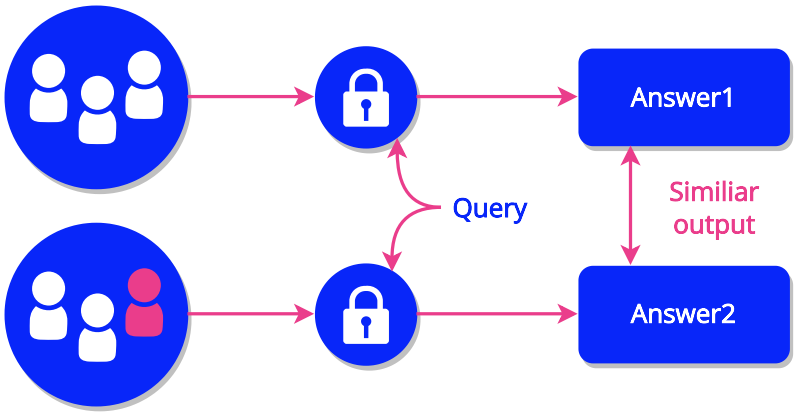


Fig. 3.5: Due to the near indistinguishability of answers 1 and 2, DP guarantees that anyone viewing the outcome of a differentially private analysis will come to the same result.

- **Pseudonymization:** A statistical technique, which involves replacing identifying personal data with pseudonyms or identifiers, allowing **data to be linked without revealing the identity** of the individual and making it challenging to trace data back. This technique could be also considered as cryptographic PET as it involves the use of encryption, hash function or HMAC to protect the identifiers. Other statistical techniques are counter, random number generator (RNG).

$$pseudonym\ =\ hash(name\ +\ date\ +\ salt)$$

Pseudonymization has the same advantages as differential privacy, but a major disadvantage is the **possibility of re-identification attacks**, in which hackers could associate pseudonymized data to a specific individual. [131, 132]

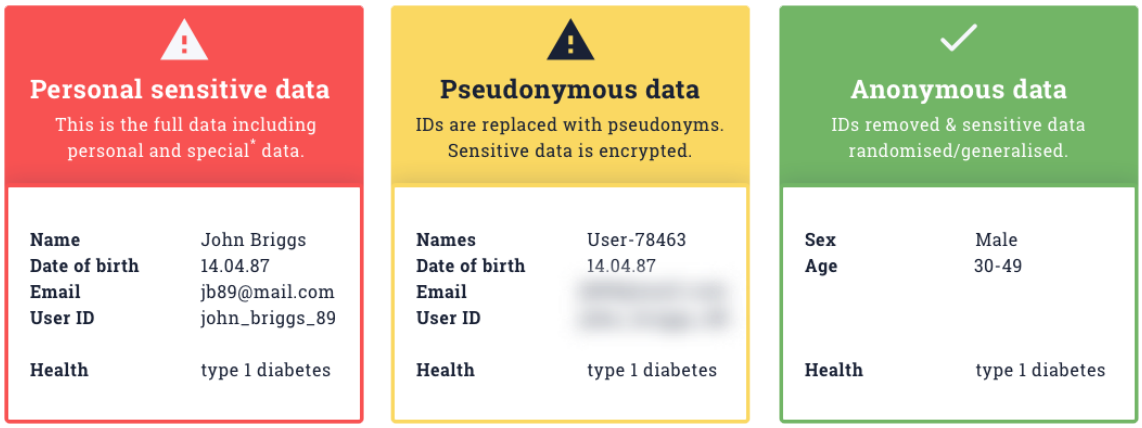


Fig. 3.6: The Data Pseudonymization and Anonymization techniques are also supported by GDPR [133].

- **Anonymization:** A statistical technique, which involves removing or altering identifying information in a dataset in order to preserve individual privacy and confidentiality. **Generalization, suppression and randomization are some of the techniques** which could be applied to achieve it. When something is generalized, a specific value is replaced by a more broad one. For example, the exact age is replaced by the age range. Suppression is the process of deleting specific data from the dataset, such as names or addresses. By adding noise or random values to the dataset, randomization refers to this technique.
  The key benefits of anonymization are the **preservation of individual privacy, the ability for data exchange while preserving privacy and compliance with data protection regulations.** The potential loss of data utility, an increase in the computation complexity and the possibility of certain de-anonymization and homogeneity attacks are some its disadvantages. Examples of real-world applications for anonymization include demographic research, financial analysis and medical research. **Anonymization is also recognized by GDPR as a key method of protecting personal data and the regulation actively promotes its use.**
- **Synthetic Data Generation:** A statistical technique, which involves generating new data, which are statistically equivalent to the original data but do not contain any personally identifiable information in it. Synthetic data are categorized as a type of data transformation tool using techniques of data masking and anonymization. The primary objective of synthetic data is to **allow researchers and analysts to use real data for testing, modeling and analysis without compromising the privacy** of the individuals whose data are included in the original dataset.

Statistical algorithms are used to analyze the relationships and patterns using the original data in the synthetic data technique, after which new data are produced that **mimics the observed relationships and patterns**. The benefits of synthetic data include its ability to protect individual privacy while still allowing the use of real data for research and study. Additionally, it is relatively simple to create synthetic data and it could be applied in a variety of scenarios. Some of the disadvantages of synthetic data is the possibility of biases or mistakes in the data that are generated, which could affect the accuracy of any models or studies based on synthetic data. [134]

- **Federated Learning:** A statistical technique, which allows multiple parties to collaboratively learn, train and share machine learning models without sharing raw data. It **operates by storing the data locally on each involved party and just exchanging model modifications**, not the raw data itself. Federated learning could be categorized as a cryptographic as well as statistical PET as it involves the use of multiple PET tools. The benefits of federated learning include its **ability to preserve data privacy while still enabling cooperative machine learning model training.** Since raw data is not shared between parties, it reduces the possibility of data breaches or leaks. Federated learning also makes it possible to train models more quickly as computing could be split across multiple machines. Federated learning comes with certain disadvantages, including its complexity and demand for specialized infrastructure. Using consistent data and model versions across all parties involved could be difficult as well. [134]

Tab. 3.2: Summary of statistical PET.

Technique	**Method**	**Use**
Differential privacy	Adding random noise to the real data to not exposing any private information from real data.	Healthcare, Social media, Location-based services
Pseudonymization	Using pseudonyms and identifiers with link to the real data.	E-commerce, Finance, Research studies
Anonymization	Removing real data using generalization, suppression or randomization to preserve private information.	Healthcare, Government, Research studies
Synthetic data	New data generation based on relationship and connection analysis on the real data.	Machine learning model training, Testing software, Simulation
Federated learning	Multiple parties collaboration on machine learning model without revealing real data.	Energy industry, Manufacture, Transportation

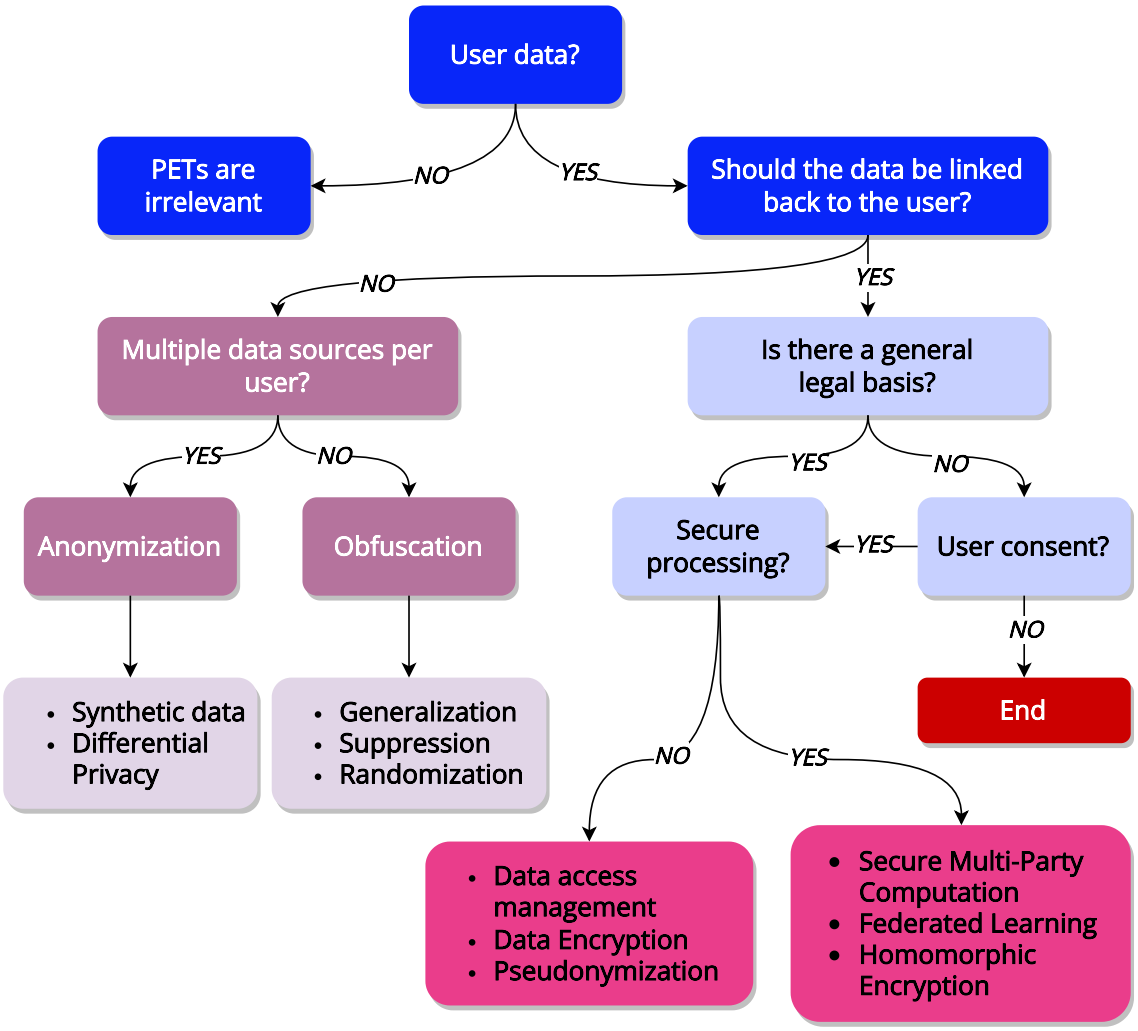


Fig. 3.7: A diagram of the classification of PET by specific use.

3.3 Applications using PET

Smart Parking Services

Smart parking services take advantage of a variety of technologies which increase parking efficiency overall, improve traffic flow and optimize parking management. Closer details in the Section 1.6. While enabling the efficient functioning of these services, the use of PET could be useful in preserving user privacy. The use case of a SPS allows for the implementation of both cryptographic and statistical PET in the ways described below.

- **HE:** Encryption of user data, such as payment information, vehicle type or vehicle number plates.

- **SMPC:** Authorization for multiple parties, such as parking lot operators and local authorities, to collaborate on parking operations or parking fee calculation.
- **ZKP:** User identity authentication, such as proving that a driver has a valid parking permit.
- **PIR:** Allowing users to access parking availability information without revealing their current vehicle location.
- **GRS:** Allowing users to authenticate anonymously to parking lot operators or local authorities about ownership of the parking permit.
- **DP:** User privacy protection while allowing analysis of parking usage patterns to improve parking management using PET as pseudonymization or anonymization.
- **SD and FL:** Application for creating parking management machine learning models without revealing real user data to exposure. FL decentralized technique could be used for training.

Car Sharing Services

In recent years, CSS have been increasing in popularity as a cost-effective and sustainable mode of transportation. More details about CSS in the Chapter 2. A number of PET could be used to overcome concerns about the collection and processing of personal data while still allowing the service to operate efficiently. Various statistical and cryptographic PET could be used in a CSS, including:

- **HE:** Allows secure processing of user data, including payment and personal information.
- **SMPC:** Employing to determine the fair rental price for without revealing any personal information about the user.
- **ZKP:** Verifying that a user is at least 18 years old without revealing the user's actual age.
- **PIR:** Obtaining information about available vehicles without revealing the user's precise location.
- **GRS:** Confirmation if a user has agreed to the CSS's terms and conditions without revealing their identity.
- **DP:** Guarantee that no user's personal information are exposed while analyzing vehicle usage patterns for service improvement.
- **Pseudonymization:** Replacing a user's real name with a pseudonym in a database of vehicle reservations.
- **Anonymization:** The radius could be expanded to a nearby neighborhood while still preserving a user's precise pick-up and drop-off locations.

- **SD and FL:** Creating and improving a model that predicts demand for vehicles in various scenarios. Training a model that uses user data to predict the availability of vehicles in different locations without requiring the data to be shared with a centralized server.

Additional applications

There are several other applications in STS that could benefit from PET:

Tab. 3.3: Additional applications in STS with possibility of using PET.

Scenario	Technique	Use
Intelligent Traffic Management	PIR, DP, Anonymization	Real-time Traffic updates
Public Transportation Services	HE, Anonymization	Real-time Travel times
Personalized Travel Planning	SMPC, DP, FL	Personalized trip recommendations, Users' travel behavior
Anonymous Delivery	HE, Anonymization	Secure e-commerce deliveries

3.4 Legal Status of PET

Many international human rights treaties and conventions recognize **the right to privacy as a fundamental human right.** The right to privacy requires the **ability to control an individual's personal data and regulate who has access to it.** By limiting the collection, processing, storage and use of personal data, the data protection legislation tries to protect this data. The legal status of PET **varies from country to country as there is no universal regulations**. However, as long as they comply to current legislation about data privacy and security, PET are usually accepted as legal and accepted.

Data Protection using PET

Data protection is driven by fair data processing. Fair data processing refers to the **collection, processing, storage and use** of personal data in a way that is open, legal and respects the rights of data subjects. Data minimization, purpose limitation, accuracy, storage limitations and transparency are same of the suitable data protection principles:

- **Lawfulness, Fairness, Transparency:** Personal data have be processed lawfully, fairly and transparently. Therefore, service operators **need to have a legal basis for the processing** of the user personal data and have to inform them about the collection, use and sharing. The legal basis could be consent, a contractual demand, a legitimate interest or compliance to a regulation. The processing also needs to be fair, which means that user should not be harmed from unreasonable or unexpected consequences as a result of it. Transparency requires providing user a **clear and easy-to-understand summary** of how their personal data are processed, including who is handling them, the reason, what types of data are being processed and how long they will be stored.
- **Data Minimization:** According to the principle of data minimization, personal information needs to be adequate, relevant and limited to a minimum considering the purposes for which they are processed. This means that service operator should **only collect and process the minimal amount of personal data required to fulfill the purpose** for which they were collected.
- **Purpose Limitation:** The principle of purpose limitation requires that personal data have be collected for specified, explicit and legitimate purposes and **may not be further processed in a way that is beyond those purposes**. As a result, service operators are required to have a specific, legitimate reason for collecting and using users' personal information. If a service operator needs to use the data for a new purpose, they requires to obtain **additional user consent** or have a legal basis for it.
- **Accuracy:** Personal information have to be accurate and kept up-to-date and any information that is incorrect or incomplete needs to be modified or deleted in accordance with the principle of accuracy. Therefore, service operators must implement appropriate steps to ensure the accuracy of personal data and set techniques in place for handling with any errors or inconsistency.
- **Storage Limitation:** The principle of storage limitation specifies that personal information have to only be maintained in a form that allows a possibility to identify data subjects for as long as is required to fulfill the purposes for which they are being processed. If personal data are no longer required for its original purpose, service operator should have mechanisms in place to delete or anonymize data.

Current Laws and Regulations

In May 2018, the European Union (EU) adopted the **General Data Protection Regulation** (GDPR), which regulates how personal data of individuals within the EU and the European Economic Area (EEA) are processed. Every company, re-

gardless its location that processes personal data of individuals within the EU and EEA is subject to the GDPR. The key principles of data protection, individual rights, data breach reporting and the idea of the data protection officer (DPO) are some of the GDPR's most important requirements. Before collecting and processing a person's personal data, companies are obligated by the GDPR to obtain the individual's explicit and informed consent. Additionally, organizations must provide people certain rights, including the ability to access and correct their data as well as the right to be forgotten or data portability.

In California, a privacy law named the **California Consumer Privacy Act** (CCPA) came into effect in January 2020. Any company that collects, uses or sells personal information about California residents and generates a certain amount of revenue is subject to the CCPA's regulations. The rights of California people, reporting of data incidents and the requirement to provide privacy notices are just a few of the key clauses in the CCPA. Residents of California have similar rights to GDPR under the CCPA, including the right to access their data, the right to know what personal data is being collected, the right to have their data deleted and the right to refuse to have their data sold.

3.5 Preserving Privacy in Commercial Solutions

Specific Factors for CSS

In terms of the legal status of using PET in CSS, the general data protection laws including above mentioned apply to it. Additional rules about the protection of personal data in the development of a privacy first software business are explained in greater detail here [143].

1. The Service Operator must comply with the **current applicable legislation**, including data protection legislation, in the area of the service providing.
2. The Service Operator must ensure that they obtain **the explicit consent from users** before collecting and processing their personal data or payment information.
3. The Service Operator must also provide users with **transparent information** about the types of data that are being collected and how data will be further processed.
4. Personal data provided by users are usually shared by the service with third-party service operators, such as payment gateways or insurance companies. Service operator must regularly reviewing and assessing **the compliance of their third-party service operators** with applicable data privacy protection laws and regulations.

5. The Service Operator must take appropriate **data safety measures**, such as choosing the right PET, executing regular backups and testing to protect user data from various attacks.
6. The Service Operator must establish appropriate **data retention periods** based on the service purposes.

Current market leaders in CSS are mentioned in the section 2.1. **Reviewing the Privacy Policy guidelines** posted on these Service Operators' websites is the only method for discovering more about how these CSS handle users personal information. Since none of the chosen CSS offer open source access to the source code, it is not possible to verify their claims in any other way.

Zipcar

The Zipcar states on their Privacy Policy website these claims that they take privacy protection seriously. It also provides users with details on how their vehicles are tracked while they use the service, in addition to collecting personal data and information from calls made to Zipcar services.

By using the Zipcar service, users must accept that their collected personal data could be processed outside of their home country, even outside of the European Union (if they are European customers). Additionally, they have no alternative but to stop using this service if they would like to change the processing method.

The Zipcar service informs users about the sharing of their personal data with multiple third parties, but their names are not mentioned. They describe the purposes for sharing the information, such as applying student reductions to fees for membership, identity verification services, insurance or vehicle repairs. Also mentioned purpose: *"when we have a good faith belief that there is an emergency that poses a threat to the safety of you or another person."* [144] is described in very broad words.

Advertising and marketing is a significant part of Zipcar's Privacy Policy. The Service, together with other third parties, collects, analyzes and sends various user data for the purpose of targeting personalized advertising on multiple advertising platforms. The user has the option to opt-out. If the user requests a full copy of the collected data, Zipcar may charge for this service.

The Privacy Policy informs about the use of *"reasonable steps to make sure your information is protected from unauthorised use, access, disclosure, alteration, destruction or loss."*, in addition to *"We take security extremely seriously but as no system is 100% secure, we can't completely guarantee the protection of your personal information, any more than any other organisation can."* [144]. In the end, it is the

user's responsibility to protect his Zipcar service account with a secure password and not reveal it to anybody else.

Turo

Turo provides Peer-to-Peer method of CSS. Ordinary car owners are able to rent their vehicles via Turo as long as they are not using them. As a result, Turo acts as a middleman between the user and the car owner.

The Privacy Policy also describes which personal data of the user and owner of the vehicle are collected and processed. These include vehicle information such as insurance number and vehicle condition, payment details as well as personal identity verification data. In order for the service to operate properly, the CSS collects usage data, location information (including precise location if the user permits it), information about the device, trip information and vehicle tracking data. CSS only uses, stores and further processes the obtained data if necessary to preserve service functionality, comply with the terms of the service agreement or protect the safety of users and properties.

The users are also warned by Turo that their rented vehicle could be monitored by a third party device that has been installed in a owner's car. In this situation, the privacy of the user shall be guaranteed by the device owner.

The Privacy Policy mentions transmitting personal data that has been encrypted and anonymized with third parties. In terms of data security, Turo uses: *"technical, physical and organizational measures designed to protect information against unauthorized access, destruction, or alteration while it is under our control. However, no method of transmitting or storing information can be 100% secure and we cannot guarantee the security of your personal information."* [146]. Since Turo operates from the United States, it is forced to transfer user data out of the country in which it operates (UK, Australia). This cross-border data transfer is further explained and Turo *"apply additional safeguards to your personal information under data protection laws. For example, by implementing the applicable standard contractual clauses."* [146].

Considering the type of CSS offered by Turo, the Privacy Policy is described in a rather brief way and constantly referred to the obtaining of additional information by contacting their specific email address.

ShareNow

ShareNow provides its CSS inside the borders of the EU member states, so as a result, its Privacy Policy is strictly regulated by the GDPR.

By registering, the service users consent to provide their personal data, as well as the purposes behind their data gathering and storage, which are clarified in more detail in the Privacy Policy. If the personal data entered by the user are not needed for any other processes of the service, they will be deleted.

ShareNow allows the registration of other smaller companies and individuals who could use this service to offer their vehicle rental services and thus increase user satisfaction. However, these personal data are processed automatically using the contact form on the website and handled to databases of CRM tool, which processes these personal data on US territory.

Therefore: *"Appropriate safeguards may not currently exist for data transfers to the US. There are restrictions on the protection of personal data resulting from the fact that, under US law, security authorities can access data transferred from the EU to the US and use it without restriction to what is strictly necessary. As a data subject without US citizenship, you cannot take legal action against such use."* [145], which means that in case of any legitimate interest of the higher US authorities, they can access and further use those personal data of a user from a state of the European Union. In this case, the GDPR regulation is no longer applicable because it primarily involves payment activities.

An interesting feature is the SHARE NOW Rewards program, which rewards users for using the service frequently by collecting points. While it is an optional feature and has no impact on the main ShareNow services, this service is outsourced. As opposed to this, ShareNow directly runs a very similar service named as Friend Referral program.

ShareNow is committed to preserving users' private data safe by taking security measures. They accomplish this by using organizational and technical tools that are frequently modified and updated. At the same time, they raise awareness to the user's responsibility, which involves taking the identical measures to protect his data and his personal information [145].

As a consequence of providing the service inside the European Union, the ShareNow service presents a far stronger and more understandable Privacy Policy.

4 Implementation Proposal

Data privacy concerns in Car Sharing Services have been drawing more and more attention in recent years. The demand for Privacy Enhancing Technologies has increased as a result of the expansion of the sharing economy and the massive amount of personal data that users generate. As explained in the previous Chapters 2 and 3, implementing PET tools in CSS could help ensure that private user data are preserved and user privacy is respected.

4.1 Reference Scenario in CSS

Imagine a city where many people are looking for a **cost-effective and efficient way to travel** to work, run errands or meet friends. The service operators offer a solution, where users could rent a vehicle for a specific period of time, drive it to their desired destination and drop-off it in the designated service area. They also manage the fleet of vehicles and ensures that they are in good condition and ready for use.

In the proposed scenario, we take into consideration a **One-way free moving Car Sharing Service** with multiple parking spots in the city, where the service operator offers a fleet of vehicles to users in compliance with set rules, including vehicle availability, users' legal status, the pick-up and drop-off location and rental duration. Users who comply with the service operator's Terms and Conditions are allowed to sign up for the Car Sharing application, where they are required to submit valid documentation in order to receive Trusted Authority (TA) approval.

The Car Sharing application is straightforward to use and user-friendly. The user-selected search criteria are used to show the vehicles which meet the criteria. The service operator, who validates both the characteristics of the vehicle and the user's competence to drive the vehicle, has to approve or deny the user's preference for a specific vehicle. After confirmation, a passkey is issued to the user's application where he or she is able to unlock the vehicle using the criteria they have selected. As a deposit for the vehicle during the rental time, the service operator will also charge the user the selected amount using her or his payment option.

The rental of a vehicle is performed in accordance with the agreed-upon Terms and Conditions of vehicle operation, which have to be fulfilled by both the user and the service operator. In order to protect assets and prevent any criminal activity during the rental period, multiple data are collected and stored in the vehicle and via the user's application. The process of calculation the final price of the rental is initiated when the User locks the vehicle and finishes the rental through the application. After that, the user confirms the calculated price of rental and uses the

chosen payment method to make the payment. All legal documentation and payment receipts are automatically generated and sent to the user using the application.

The aim of our proposal is to **select specific CSS processes, which are adopted by users** in the current commercial CSS and with the use of **PET tools to improve data and privacy protection** for all involved parties without significant restrictions on the functionality of the CSS. This section of the thesis further describes the individual components of the model, the phases of the model and multiple requirements to the proposed model. The following **five phases adequately propose the use of PET tools and techniques in the Car Sharing process**. Each phase is presented with a description of the problem, the current solution, the proposed technical solution and a verification of the implementation. The outcomes are presented in the last section, where they are expanded with further possibilities for future development.

4.2 Model Proposal

Model Components

The proposed model consists of several components, each with a specific role in the CSS. These components are as follows:

- **Users:** Individuals who want to use the CSS are identified as users. Users of the service have to comply with specific parameters set by the legislation and the specific CSS.
- **Service Operator:** The component responsible for running the CSS using Car Sharing application is identified as the service operator. Their responsibilities include fleet management, vehicle maintenance, customer service and preserving confidentiality as well as privacy of user data.
- **Application:** A platform known as Car Sharing application allows users to access the CSS. Based on their selected search preferences, the application allows users to search for available vehicles, book and access them. Also, it provides the option to pay for the CSS by linking to payment gateways or contacting the service operator for help or to report a problem with the vehicle.
- **Vehicle:** Users could rent vehicles from the service operator using Car Sharing application. In order to protect the assets of the service operator, vehicles may be equipped with GPS or monitoring devices which allow real-time monitoring of the location, speed, fuel level and other vital components of the vehicle.

- **Trusted Authority:** The component in charge of providing the security and privacy of user data is known as the Trusted Authority. It is in the position of overseeing secure communication between system components and is also in charge revoking user access in the event of a security violation or misuse of the service.

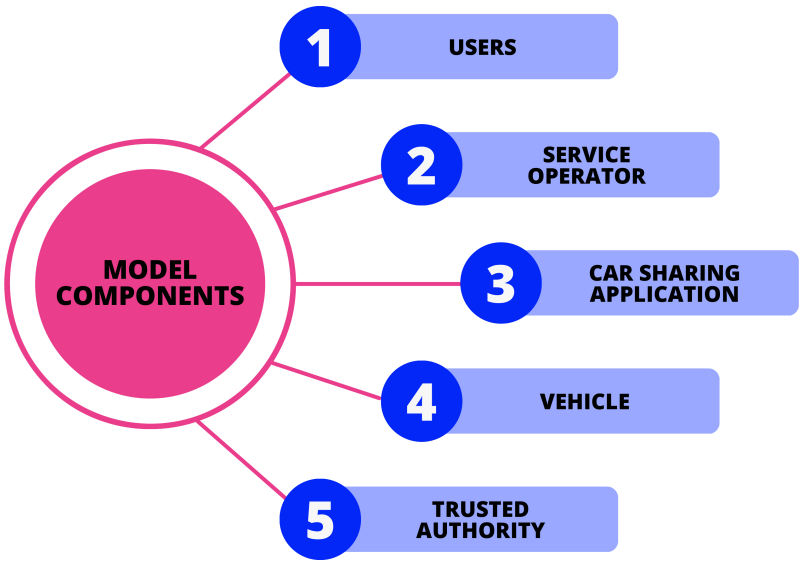


Fig. 4.1: Model consists of 5 interconnected components in the CSS.

Model Phases

The typical Car Sharing process could be divided into the following five phases:

- **User Registration and Verification:** The user creates an account in the Car Sharing application and provides personal data including name, email address and payment information based on user's voluntary consent to the Terms of service. The service operator confirms the user's identity and checks their driving history to make sure they are qualified to use the service.
- **Vehicle Selection and Reservation:** After the successful verification, the user chooses a preferred vehicle from the database, specifying the pick-up and drop-off locations as well as a time. The Car Sharing application validates the reservation and provides the user the relevant details, including the exact location of the vehicle, an access code, pick-up and drop-off instructions.
- **Vehicle Access and Monitoring:** Once the user has arrived at the specified pick-up location, they use their mobile device with Car Sharing application to unlock the vehicle. After entering, the user follows the instructions to start the vehicle and set off on their trip. The user is responsible for driving the vehicle safely and legally during the rental period. This includes following all traffic

regulations, preserving the vehicle in good condition and fuelling as required. Any incidents, breakdowns or other problems should be reported by the user to the service operator.

- **Trip Calculation and Vehicle Return:** After finishing their trip, the user returns the vehicle to the designated drop-off location, where they then follow the instructions to lock up the vehicle and end the rental. Based on agreed Terms of Service including rental duration and additional fees, such as extra distance or fuel costs, the CSS calculates the final fee. The Car Sharing application issues a receipt with a summary of the rental to the user.
- **Secure Payment** The most important step in CSS is making a secure payment, which guarantees a secure financial transaction between the service operator and the user using the Car Sharing application. The service operator store only the minimum necessary payment information about the user, such as payment method and trip receipt. The Car Sharing application's secure payment gateway handles transaction execution and authorization. In the event of non-payment or other illegal behaviour, the service operator could contact the Trusted Authority revoke the user's access to the CSS using the payment gateway response.

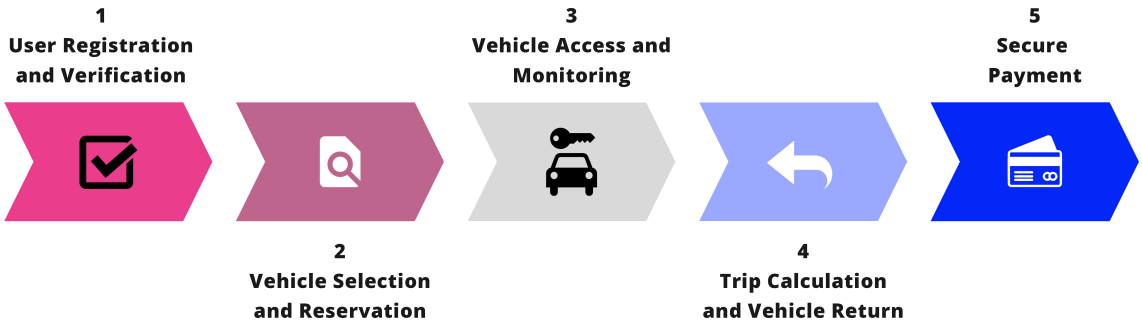


Fig. 4.2: CSS model consists also of 5 phases.

Model Requirements

Security requirements are essential for ensuring the data security of the Car Sharing system. Table 4.1 describes the security requirements.

Tab. 4.1: Security Requirements for CSS.

Requirement	Description
Data Integrity	Ensure that data are not changed or affected without detection.
Authentication	Validate that users have appropriate permissions to access the system and are exactly who they claim they are.
Confidentiality	Ensure sure that private data are protected from unauthorized access.
Unlinkability	Ensure that users are not linked to their data or patterns without their permission.
Revocation	Make ensuring that access to the system or data could be revoked if needed.
Conditional Traceability	In the case of a security incident or legal issue, make sure that collected data and behavior are possible to monitor.

Privacy requirements for ensuring that the CSS respects user privacy and autonomy where users could trust the service to handle their personal data. Table 4.2 describes the privacy requirements.

Tab. 4.2: Privacy Requirements for CSS.

Requirement	Description
Transparency	Information about data collection, processing, and sharing should be provided in a clear and understandable way.
Anonymity	Allow users to use the service without sharing their identities or personal data, unless absolutely necessary.
Data Minimization	Just the bare minimum amount of data necessary for providing the service should be collected and stored.
Purpose Limitation	Use the collected data only for the intended purpose and with user consent.
User Control	Provide users access to their data and an option to modify or delete it.

Functional requirements are mandatory for ensuring that the Car Sharing system meets the needs and expectations of users and that the service is efficient, sustainable and user-friendly way. Table 4.3 describes the functional requirements.

Tab. 4.3: Functional Requirements for CSS.

Requirement	Description
User Registration	Allow users to create accounts and authenticate themselves to access the service.
Vehicle Reservation	Allow users to reserve vehicles based on predetermined reservation details (availability, time, price, location).
Vehicle Access	Allow users to access the reserved vehicle in a secure and easy-to-use method.
Vehicle Status Monitoring	Information about the location, status and condition of the vehicle should be collected and displayed in real-time to the user.
Payment Processing	Allow users to conveniently and securely pay for the service.
Customer Support	Provide users a way to get in touch with customer service for assistance or help.
Trustee Third Party Control	Use a trustee third party to provide users additional security and privacy controls.

4.3 Phase 1: User Authentication

Problem Description

User registration and authentication is a initial phase of the CSS to ensure secured and authorized user's access to the service. However, **using personally identifiable information such as a name, email address, phone number, age or user's driving licence** for conventional methods of registration and authentication raises privacy concerns. Data leaks and user identity theft are risks which could be raised by the storing and processing these data and could result in serious consequences.

Current Solution

The user authentication process used by CSS operators currently combines a variety of techniques. Users have to create an account by providing personally identifiable

information. In most CSS, uploading a selfie and a scan of a user's current driving license is also required for identity verification.

A verification code is used by CSS to verify the user account. To the extent that users' private information is cross-checked against databases and national driving licence registries[1] for any unwanted entries. Additionally, the payment option is checked against card/banking institutions if CSS requests an authorized payment method during the user registration process.

Proposed Solution

PET tools including **Pseudonymization** and **Attribute-Based Credentials** (ABCs) are suitable to solve these concerns. By replacing users' personally identifiable information with **pseudonyms**, it is possible to verify users without disclosing their true identities. On the other hand, ABCs allow users prove attributes such age or driving license status **without revealing unnecessary personal information**. The Car Sharing application then stores and processes the user's personal data which have been modified using these tools.

We assume that provided data are validated and secured against attacks using input fields. Additionally, we assume that the user provided consent for the data processing needed to utilize the CSS, allowing it to process additional data. The user was clearly informed about the way how PET tools work and what type of data are preserved.

The proposed solution is developed using **Python 3.9.7** programming language with the **hashlib** library and Post Quantum resistant hash algorithm **SHA3_256**, which is the NIST-recommended [147, 148]. The Post Quantum signature algorithm **CRYSTALS - Dilithium** is also used for signing and verifying processes in the **pqcrypto** library [149].

Implementation Verification

The proposed implementation consists of two CSS main components, which are **Service Operator and User**.

User class has defined attributes for name, email, phone, age and driving license status. `Get_attributes()` method returns a dictionary of entered users attributes. `Pseudonymize()` method takes user data (only name, email and phone) and returns pseudonyms for the each value by generating a random string of the same length using `SHA3_256` (KECCAK) hashing function.

ABC class represents an ABC system including: issuer, a set of attributes and signature. Signature consist of the **entity** (issuer) and **attributes** (credentials) to

[1] Acts as Trusted Third Party

prevent to any tampering attacks. `CRYSTALS-Dilithium` post quantum algorithm is used to sign and verify the signature. In this implementation we assume an ABC to be a part of **ServiceOperator** component.

ServiceOperator class has defined attribute of name and `verify()` method where user age and driving license status are both verified. **If conditions are valid, user is correctly verified.** Also verifies issuer name and ABC signature.

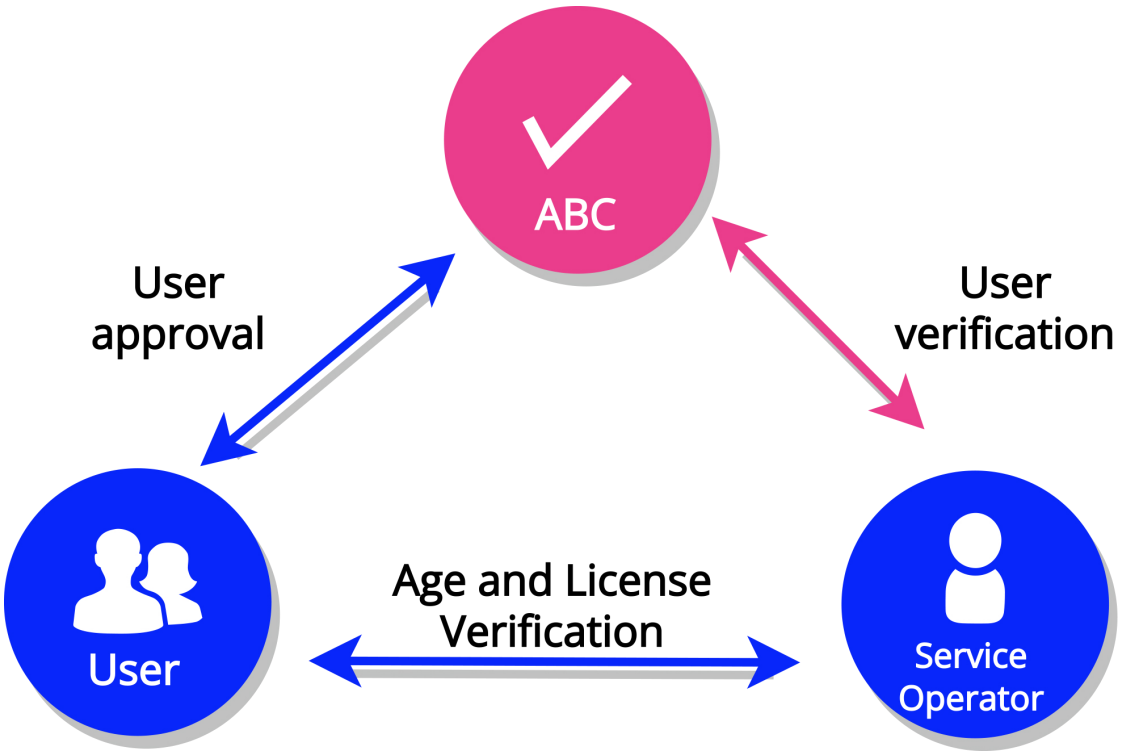


Fig. 4.3: Phase 1 Component and communication design.

Listing 4.1: Code snippets from Phase 1 Implementation

```
import hashlib
from pqcrypto.sign.dilithium import generate_keypair,
   sign, verify

class User:
def pseudonymize(self):
    name_pseudonym = hashlib.sha3_256(self.name.encode())
       .hexdigest()

class ABC:
def sign(self, secret_key):
    h = f"{self.issuer}:{self.attributes}"
    m = hashlib.sha3_256(h.encode()).digest()
    self.signature = dsign(secret_key,bytes(m))

class ServiceOperator:
def verify(self, user):
    user.pseudonymize()

    if not abc.verify(self.public_key):
        print(f"Invalid signature.")

    if user.age >= 18 and user.license == 'valid':
        print(f"Verification successful for user {user.
           name} by service {self.name}.")
```

4.4 Phase 2: Vehicle Selection

Problem Description

The second phase of selection a vehicle is important for the Car Sharing process as it specifies the selected vehicle based on its availability and fit for the user's needs. CSS offer a range of vehicles with various features, engine power and size. Additionally, **considering user demand, maintenance schedules and other factors**, the fleet of vehicles available for rental could constantly change. For the user to pick a vehicle, the location of the available vehicles needs to be known. If a hacker is successful in eavesdropping the user's communication with the CSS and accessing the location data, it could result in serious consequences.

Current Solution

In the current CSS, **vehicle location cloaking and clustering** is already implemented in the vehicle selection phase of the Car Sharing process. When a user searches for available vehicles, the system uses a cloaking approach to hide the locations of the vehicles, making sure that the user is not able to locate where the vehicle is precisely until they reserve it. It also avoids other users from discovering the precise location of the vehicle and possibly stealing or interfering with it.

To provide users with an adequate selection of available vehicles on the map in the application while preserving their privacy, **location clustering and location cloaking techniques are combined**. The user is presented with a sufficient number of possibilities that are close enough to their desired location due to this grouping, which is done without revealing the exact location of any specific vehicle.

Proposed Solution

Vehicle cloaking is another PET tool, which involves obscuring the location data of the available vehicles so they could not be linked to a specific area, is a solution to this problem. A additional PET tool for improving vehicle privacy is **location clustering**, which groups vehicles according to their locations into clusters and only shows user the cluster instead of the precise location of each vehicle. Both PET tools are considered to be **Data Minimization techniques**, which enhance the security of the service operator vehicle-fleet by making it more difficult for attackers to obtain sensitive location data.

We assume the fact that vehicle location database is securely stored and that the Car Sharing application's back-end implements techniques for clustering and obscuring location data. Additionally, we are not taking into consideration other

factors of the vehicle, such as availability or its technical condition, which could affect the vehicle's availability.

The proposed solution is developed using **Python 3.9.7** programming language with the **sklearn, numpy, pandas and random** libraries for vehicle location obscuring and clustering. **Matplotlib** is used to plot the final results.

Implementation Verification

Only the **Vehicle** CSS component is included in this proposed implementation.

Firstly, modules `pandas` and `random` randomly **generates a vehicle csv-type database** with valid attributes, which contains data about the vehicle name, plate and current location in area of the city Vienna. The latitude and longitude data of these vehicles are perturbed by **adding random noise**, which makes it more challenging to determine the precise location of each vehicle. It should be noted that this technique only adds small amount of noise the latitude and longitude data, which may not be sufficient to provide adequate privacy guarantees, especially in the less densely populated areas of the CSS.

Secondly, the `pandas DataFrame` is used to process the vehicle csv-type database. It uses latitude and longitude columns to perform `K-Means` clustering. Each vehicle has a new unique cluster to which the mean value of latitude and longitude is calculated. This mean location will be shown to users in the Car Sharing application during vehicle selection process. The **ideal number of clusters is determined** using the `Silhouette score` as part of further privacy protection, which means that the number of clusters will be different each time.

In the end, the clusters with preserved vehicle locations are **illustrated on the plot** using `matplotlib` module to provide a better representation of this implementation.

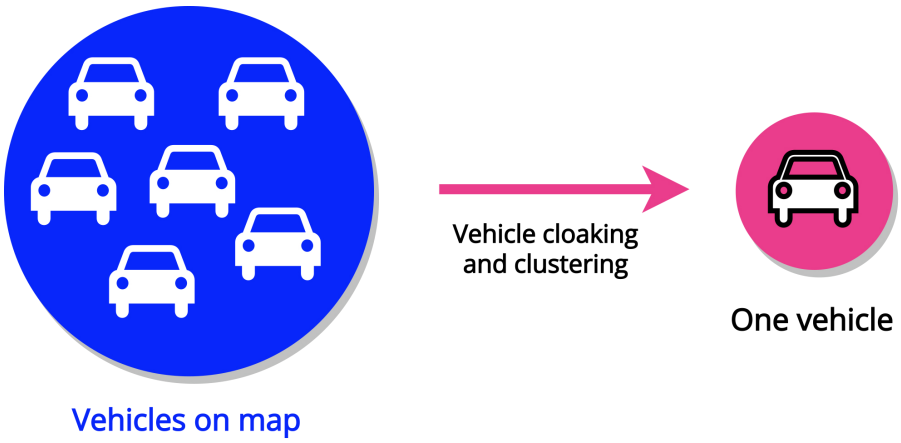


Fig. 4.4: Phase 2 Vehicle cloaking and clustering.

Listing 4.2: Code snippets from Phase 2 Implementation

```
import random
import numpy as np
import matplotlib.pyplot as plt
from sklearn.cluster import KMeans
from sklearn.metrics import silhouette_score

for i in range(100):
    data.loc[i] = [random.choice(["BMW","Mercedes",...),
    f"vehicle_{i+1}",
    random.uniform(48.1, 48.3),
    random.uniform(16.3, 16.6)
data.to_csv("vehicle_locations.csv", index=False)

vehicle_df["latitude"] = vehicle_df["latitude"] + np.rand
   om.normal(scale=0.01, size=len(vehicle_df))
vehicle_df["longitude"] = vehicle_df["longitude"] + np.r
   andom.normal(scale=0.01, size=len(vehicle_df))

sil_score = silhouette_score(vehicle_df[["latitude","
   longitude"]],kmeans.labels_)
n_clusters = np.argmax(sil_scores) + 2

kmeans = KMeans(n_clusters=n_clusters, random_state=42)
kmeans.fit(vehicle_df[["latitude","longitude"]])
vehicle_df["cluster"] = kmeans.labels_

for cluster in range(n_clusters):
    vehicles = vehicle_df[vehicle_df['cluster'] ==
       cluster]
    center_lat = vehicles["latitude"].mean()
    center_lon = vehicles["longitude"].mean()
    for _, row in vehicles.iterrows():
        print(f"Vehicle {row['vehicle_number']}: {row['br
           and_name']} at ({row['latitude']},{row['
           longitude']})")

plt.scatter(vehicles["longitude"],vehicles["latitude"],s
   =50,alpha=0.5,c=[color],label=f"Cluster {cluster}")
plt.show()
```

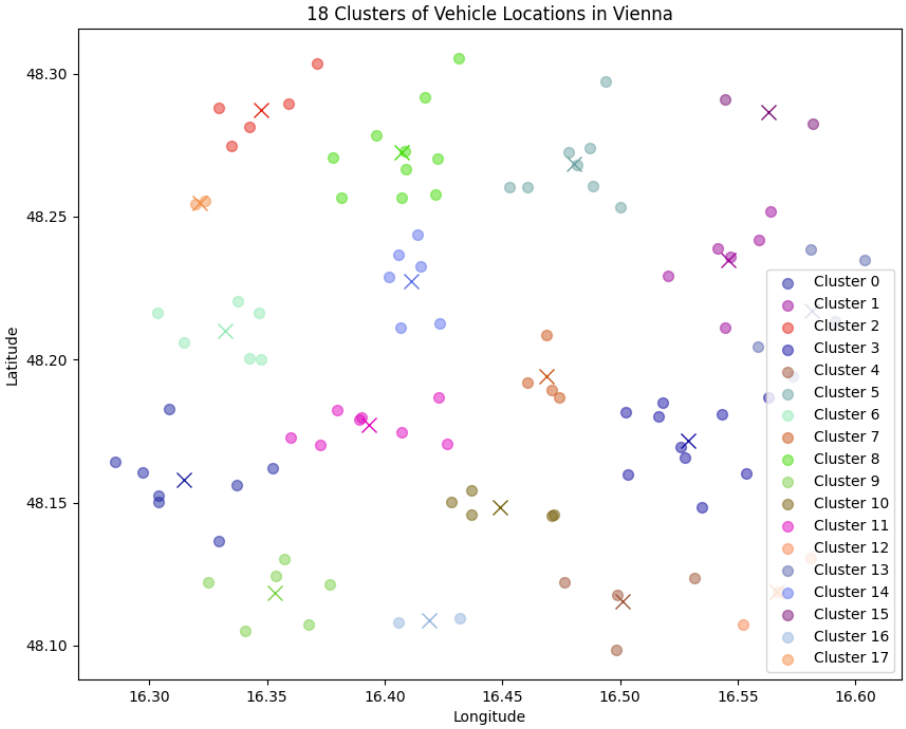


Fig. 4.5: Vehicle clustering with centeroids in the city of Vienna.

4.5 Phase 3: Vehicle Access

Problem Description

The next important phase of Car Sharing process is accessing a vehicle, which allows the user to use the reserved vehicle. Car Sharing application usually offer using a **unique access key**, which could be used by the user to unlock the vehicle while it is the close proximity using Bluetooth and GPS technologies. Preserving user anonymity while providing access to the vehicle creates a significant privacy challenge. When the user accesses the vehicle, the precise location becomes visible in the Car Sharing application, which compromises the user's privacy.

Current Solution

Current methods for accessing a vehicle in a CSS involve using a physical key, remote OBU device or an application-based unlocking technique that requires the user to provide their identity. These techniques compromise user privacy by revealing it to the vehicle.

Proposed Solution

Group Signatures are one techniques of PET tools which could be used to solve this privacy concern. They are considered to be the PET category of **Anonymous Credentials** techniques. Group Signatures **provide users anonymous access to the vehicle** as verification that they have consent to use it, without revealing their identities. Only authorized users are allowed to access the vehicle. A RSA-based signature technique could be implemented in the context of CSS to provide confidentiality and anonymity during the vehicle accessing process. This technique allows the service operator to **issue a vehicle-fleet group signature** that the user could verify without revealing the user's identity and connection to the specific vehicle. The complete mathematical proof of RSA Group Signatures is described in more detail in [150].

We assume that when a user approaches a vehicle in close proximity, the vehicle has been already signed by the service operator. In order to use this technique, we also assume that the user validates the correct public key associated with the vehicle-fleet using a compatible device.

The proposed solution is developed using **Python 3.9.7** programming language with the **PyCryptodome** library for **RSA** Group Signatures generation and **SHA3_256** hash algorithm [151].

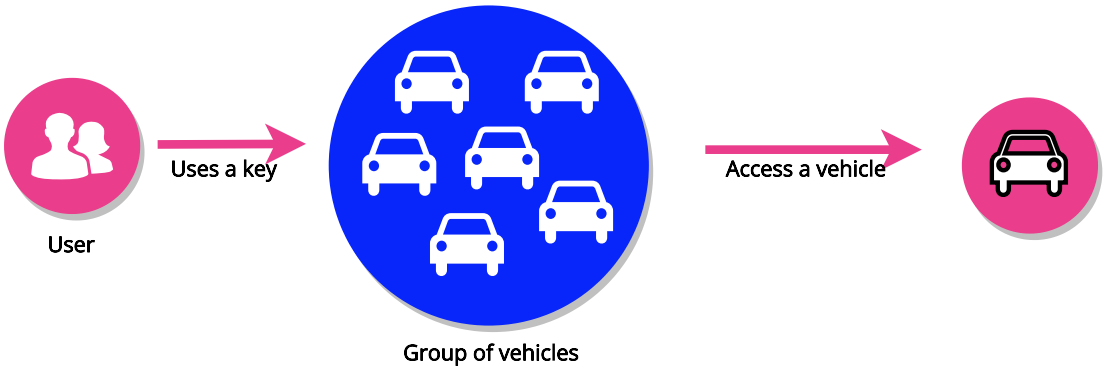


Fig. 4.6: Phase 3 Vehicle Access principle using Group Signatures.

Implementation Verification

The proposed implementation consists of two main CSS components, which are **Vehicle and User**.

Vehicle class represents each vehicle in the fleet. Class contains variables as vehicle brand name and number plate. Two methods are also implemented. Method `sign()` is using hashing function to create hash and using a private RSA key is generated a signature for each vehicle. The `verify()` method of the class checks the user's signature against the multiple public RSA keys of vehicles. RSA key uses a larger key size of **4096 bits** for the encryption. For hashing functions is used Post Quantum resistant `SHA3-256` (KECCAK) hash algorithm.

User class has only one method `verify_vehicle()` for verifying the selected vehicle. Method takes a user's selected vehicle, a list of signatures and the public key. The method verifies the signature of the selected vehicle against the public key using the verify method. If the verification is successful, it returns True and User's access has been approved. If no signature matches to the all signatures, returns False and user has no access to any of the vehicle from the fleet.

Listing 4.3: Code snippets from Phase 3 Implementation

```
from Cryptodome.Hash import SHA3_256
from Cryptodome.PublicKey import RSA
from Cryptodome.Signature import pkcs1_15

class Vehicle:
def sign(self, key):
    h = SHA3_256.new()
    h.update(f"{self.brand_name}:{self.number_plate}".
       encode())
    signature = pkcs1_15.new(key).sign(h)

def verify(signature, key):
    try:
        pkcs1_15.new(key).verify(h, signature)
        return True
    except ValueError:
        return False

class User:
    def verify_vehicle(signatures, key):
        for signature in signatures:
            try:
                pkcs1_15.new(key).verify(h, signature)
                return True
            except ValueError:
                continue

gk = RSA.generate(4096)

signs = []
for vehicle in fleet:
    s = vehicle.sign(gk)
    signs.append(s)
sv = fleet[5]

if user.verify_vehicle(sv, signs, gk.publickey()):
    print("Access has been approved.")
```

4.6 Phase 4: Vehicle Monitoring

Problem Description

The next phase of the Car Sharing process involves monitoring the vehicle while it is being rented for a variety of reasons, includes monitoring the its precise position, compliance with road regulations, correct parking and monitoring safety features of the vehicle. This **vehicle monitoring process represents a number of privacy issues**, as private information about the user's driving habits and location could be collected, transmitted and processed between the user's device, vehicle and the Car Sharing application. Preserving these data confidential and secure during the monitoring process is the primary challenge.

Current Solution

The current approach of vehicle monitoring in CSS typically includes the **use of telemetries OBU devices installed inside the vehicle** to collect various data. These data are then transmitted on the CSS servers, where they are stored and analyzed. Data are also used to further **profiling the users** with the aim to increase CSS usage and boost revenue.

Proposed Solution

The data from the vehicle, user's device and Car Sharing application could be safely collected and processed using **Secure Multi-Party Computation** (SMPC) techniques. Multiple parties could compute an equation on their inputs using SMPC without disclosing any of their personal information. The approach guarantees that data privacy remains preserved while allowing the required monitoring to happen. Sharemind is a database and analysis solution that preserves privacy and allows to integrate and analyze personal information without ever seeing the actual data. It also enables the enforcement of data usage policies by data owners and other interested parties. [152]

The **Sharemind MPC software** could be operated on three separate Sharemind hosts. The three Sharemind Hosts receive the data which Data Owners share, creating a distributed database. Only with the permission of enforcers who verify that the query complies with the data usage policy could analysts query this database. The Sharemind MPC SDK provides a **SecreC programming language** to develop applications which preserve user privacy using SMPC methods.

We assume that the user has installed the current version of the Car Sharing application on their device with SMPC SDK support. We also assume that all other infrastructure including the vehicle and Car Sharing application has also properly

implemented the individual components of its SMPC SDK. The SMPC SDK works in the background of the Car Sharing application and does not require the user intervention in this activity. We assume that the user is following the correct procedure for using the CSS.

The proposed solution is developed using **Sharemind MPC SDK created by Cybernetica**. For connection with **Python 3.9.7** programming language is used module **ShareProm** which allows the communication between SecreC programming language and Python [153]. This proposed solution is time consuming to initialize. To run this solution it is necessary to have specific technical knowledge with creating a connection between Virtual Machine where Sharemind MPC SDK is running and final source code developed in Python.

Implementation Verification

The proposed implementation consists of three major CSS components, which are **User, Vehicle and Car Sharing application**.

In this implementation, each party generates or calculate a specific value as their secret input, **representing the distance, price per kilometer and additional costs** for the CSS. The final price for the user is calculated from these inputs on the basis of the specific algorithm of the particular CSS. Without disclosing any of the individual inputs to the other participants, the sum of these secret inputs is safely computed using the Sharemind MPC architecture.

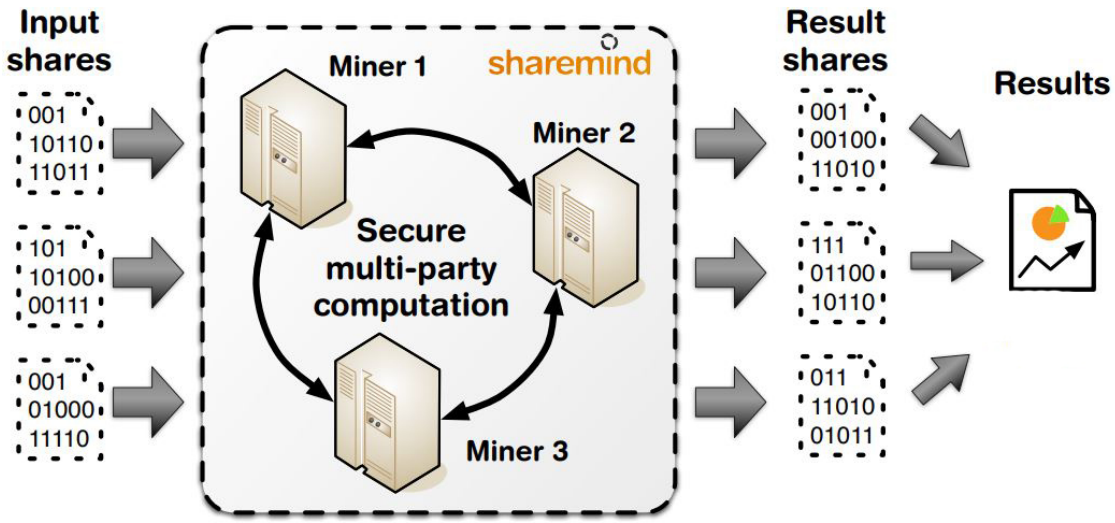


Fig. 4.7: Phase 4 Vehicle Monitoring principle using Secure Multi-Party Computation [152].

Listing 4.4: Code snippets from Phase 4 Implementation

```
import sharemind
import shareprom

with sharemind.Connection('localhost', 12345) as conn:
    with conn.session() as session:
        vehicle_miles = 10
        session.input(vehicle_miles)

        received = session.input_from("C",output)
        result = session.output(received)

        print("The calculated result of the three inputs
           is:", result)
```

Using `localhost` on the same system, the `Connection()` function connects the Virtualized Sharemind MPC SDK server with the Python code. For each new session, a manager is created using `Session()` function. The `Secret()` function is used by each involved party to define their secret inputs. Operation for multiplication and function for sum are used to calculate the final value of the secret inputs. The `Reveal()` function is used to expose the result to the Car Sharing application. Based on this value, the final rental price for the user is calculated.

$$f(user * vehicle + application) = finalprice$$

Please keep in mind that this implementation offers an easy example of how to use SMPC techniques properly. Additional security procedures have to be implemented in the real world to ensure the confidentiality and integrity of transmitted data.

Listing 4.5: Pseudocode snippets from Phase 4 Implementation

```
#include <sharemind.h>

void main() {
    smd_connection_t conn = smd_create_tcp_connection("
       localhost", 12345);
    smd_session_t session = smd_create_session(conn);

    smd_input_t input1 = smd_receive_input(session);
    smd_sint_t secret1 = smd_get_input_sint(input1);

    smd_sint_t mul = smd_mul_sint(secret1, secret2);
    smd_sint_t result = smd_add_sint(mul, secret3);

    smd_output_t output = smd_create_output(session);
    smd_set_output_sint(output, result);
    smd_send_output(session, output);

    smd_destroy_input(input1);
    smd_destroy_session(session);
    smd_destroy_connection(conn);
    return 0;
}
```

4.7 Phase 5: Secure Payment

Problem Description

Secure payment is the last and most important phase in the CSS process. The **identity of the parties has to be revealed during a traditional payment** transaction, which could lead to privacy issues. Users' privacy and their behavior could be compromised if their identities are revealed, especially past vehicle rentals or additional service fees, could be tracked. Users could also be exposed to fraudulent activities as a consequence of their personal information being made accessible to third parties. The primary challenge is to preserve the users' financial and private information secure and discrete during the payment process.

Current Solution

Car Sharing applications already accept payments using a variety of secure mechanisms, including credit card transactions and mobile payment providers. But **providing party identities continues to be necessary** for these methods to work.

Proposed Solution

A PET tool known as **Zero-Knowledge Proof** could solve these issues by allowing participants to verify the legitimacy of a transaction without exposing any unnecessary information. As an example, a **user could prove that they have sufficient funds** to complete a transaction without revealing their account balance. Or, could confirm sending the requested payment while keeping the identity hidden. By doing so, the risk of fraud will be reduced while simultaneously guaranteeing the confidentiality of the transaction and identity.

We assume that the user has a **digital wallet** or other payment option that supports the creation and verification of ZKP. We also assume that a secure connection is established between the user and the service operator using Car Sharing application and both parties are authenticated.

To implement Zero-Knowledge Proof technique to ensure Secure Payment in Car Sharing application, the **noknow** library in **Python 3.9.7** programming language could be used [154]. This technique could ensure the integrity of the transaction while providing users a secure and anonymous payment method.

Implementation Verification

The proposed implementation consist of two main CSS components, which are **User and Service Operator.**

The user wants to send a 100-unit payment to the service operator. The implementation allows the user to insert the selected value of the **payment amount**, which is confirmed with user's signature and sent to service operator. The service operator accepts this signature and adds operator's token, which also includes secret operator's knowledge and the token which the was originally sent by user.

As a result, the user receives the token, successfully extracts the value of the payment amount from it and sends the remaining part back to the service operator, who finally verifies, if the sent token has changed. If it has not changed, the service operator has successfully approved that the user knows the value of the payment amount, without revealing any of user's personal or financial information. This complete process is described by the mathematical equations below:

$$\begin{aligned} secret_u &= paymentAmount \\ token_u &= Sig(secret_u) \\ **\ send\ user's\ token_u & \end{aligned}$$

$$\begin{aligned} token_s &= H(\text{"password"}||salt)\ mod\ n; token_s\ \epsilon\ F_n \\ r &= random\ r;\ r\epsilon\ F_n \\ R &= r * G \\ c &= H(token_u||R||salt) \\ m &= r + c * token_s \\ **\ send\ operator's\ prove\ & (c, m) \end{aligned}$$

$$\begin{aligned} M &= m * G \\ C &= c * S \\ **\ proof\ valid\ if\ c == & H(token_u||M - C||salt) \end{aligned}$$

It should be noted that this example code is only intended to illustrate a proof-of-concept and it is not secure for implementation in real applications.

Listing 4.6: Pseudocode snippets from Phase 5 Implementation

```
from noknow.core import ZK

payment_amount = 100

def User():
    signature = user_zk.create_signature(payment_amout)
    proof = user_zk.sign(payment_amout, token).dump()

def ServiceOperator():
    oPassword = "Password"
    oSignature: ZKSignature = operator_zk.
       create_signature(oPassword)
    uSignature = ZKSignature.load(signature)
    user_zk = ZK(uSignature.params)
    token = operator_zk.sign(oPassword, user_zk.token())

if operator_zk.verify(token, oSignature):
    if user_zk.verify(proof, uSignature, token):
        print("Success!")
```

4.8 Testing and Solution Results

To evaluate the performance and functionality of our proof-of-concept implementations is used a **Windows 10 Pro 64-bit** machine equipped with an **Intel i7-6500U** CPU and **16GB of RAM**. Implementations are developed in the programming language **Python 3.9.7** and executed in **Visual Studio Code 1.78.0**. All used libraries and modules are listed in the **Implementation Verification** section of the specific phase.

User Authentication

The first phase evaluates the effectiveness of Pseudonymization and Attribute Base Credentials PET techniques in protecting user identity during the registration and authentication. The user credentials pseudonymization, user credentials signing and user credentials verification tests have been created in order to evaluate the speed of the implementation under realistic conditions. After 10,000 runs, the time necessary to execute out these functions is extremely low. The user credentials signing test took an average of **0.001042 milliseconds**, the user data pseudonymization test **0.000008 milliseconds** and the verification test **0.001188 milliseconds**. From the collected data, it could be assumed that the implementation of these PET tools **would be suitable** for CSS from the perspective of time consumption.

Vehicle Selection

The second phase focuses on the use of vehicle location cloaking and clustering PET techniques in the vehicle selection process to preserve user location privacy. The proposed proof-of-concept generates 100 rows of vehicle data for further processing. Out of 1000 runs, the average time required to generate this csv database is **0.083111 milliseconds**. The generation of random noise following scaling of vehicle location data represent the second method in this phase which is measured. The average time in 100 runs is **0.004344 milliseconds**. For 100 iterations, it took an average of **1.844042 milliseconds** to calculate the random cluster number and then distribute the 100 generated vehicles across these locations. The outcomes from the second phase show how **time-consuming the PET technique** could be for finding the random number of clusters in a certain area. A faster technique for preserving the vehicle's location for secure displaying in the Car Sharing application is adding random noise to the single vehicle location data itself.

Vehicle Access

The third phase examines the use of Group Signatures to ensure vehicle accessing anonymity during the reservation process. The creating and signing of a 100-vehicle fleet requires on average **2.610243 milliseconds** using algorithms such as `SHA3_256` and RSA with a key length of 4096 bits. On the other hand, using a user obtained public key only takes in average **0.251869 milliseconds** out of 100 vehicles to authenticate access to a specific vehicle. The use of this technique is directly **dependent on the number of vehicles** in a signature group.

Vehicle Monitoring

The fourth phase tests the effectiveness of SMPC in protecting vehicle data privacy during the rental period. In this phase, the Sharemind MPC SDK is used, which requires the creation of a virtualized server and its subsequent connection to the implementation using `localhost`, which significantly impacts any testing of connection speeds and calculations. Due to the difficulties to verify the calculation speed or the rate of communication between the host and the server more closely, this fourth phase acts only as a proof-of-concept. The **SyMPC package**, allowing performing SMPC computations directly in Python programming language, is able to develop an implementation, however running it on a single device could have an impact on its functionality [155]. From it could be concluded that the use of the **SMPC PET technique requires a specific environment**, which is beyond the scope of this thesis.

Secure Payment

Fifth, the final proposed phase evaluates the use of ZKP to secure user payment information during the payment phase. The time complexity of signing the payment amount value by user is first verified in the developed implementation. The average duration of time needed to perform 100 runs is **0.005570 milliseconds**. Two methods are then evaluated on the service operator's side. The first method involves signing the service operator token, which consist of the user's token and the operator's secret password. Average time of 100 runs is **0.012300 milliseconds**. The second method involves the service operator's side accurate validation of the hidden payment amount value. The average execution time of the method used to validate secret with 100 runs is **0.010410 milliseconds**. According to the collected average time values, it could be considered that the correct implementation of the ZKP protocol **does not have to significantly slow down the functionality** of the secure payment gateway in the CSS. The only question is if such a possibility could be realistically realized in the context of well-known payment methods today.

The results from each implementation are collected in the table below and a graph showing the **information about time consumption** [ms] in relation to **implementation difficulty** [points] follows. The points are assigned by the author on the basis of his subjective view of the difficulty of implementation in the chosen test bed.

Tab. 4.4: Results of proposed techniques of PET in CSS.

Technique	**Phase of CSS process**	**Average time [ms]**
Pseudonymization	Registration	0.000008
ABC	User Verification	0.001188
Data Minimization	Vehicle Selection	0.004344
Vehicle Clustering	Vehicle Selection	1.844042
Group Signature	Accessing Vehicle	2.610243
Group Signature	Opening Vehicle	0.251869
ZKP	Secure Payment	0.010410

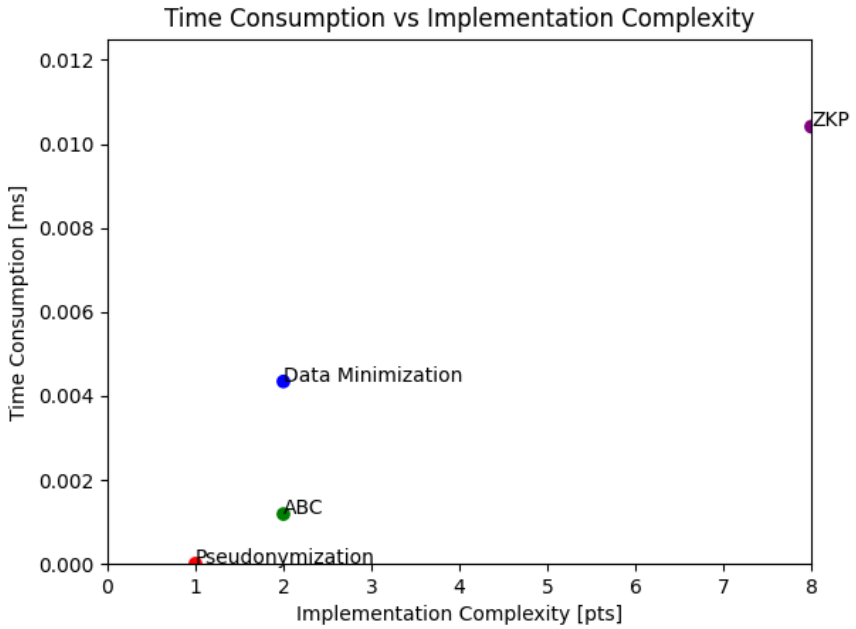


Fig. 4.8: Graph representation of collected results (narrow view).

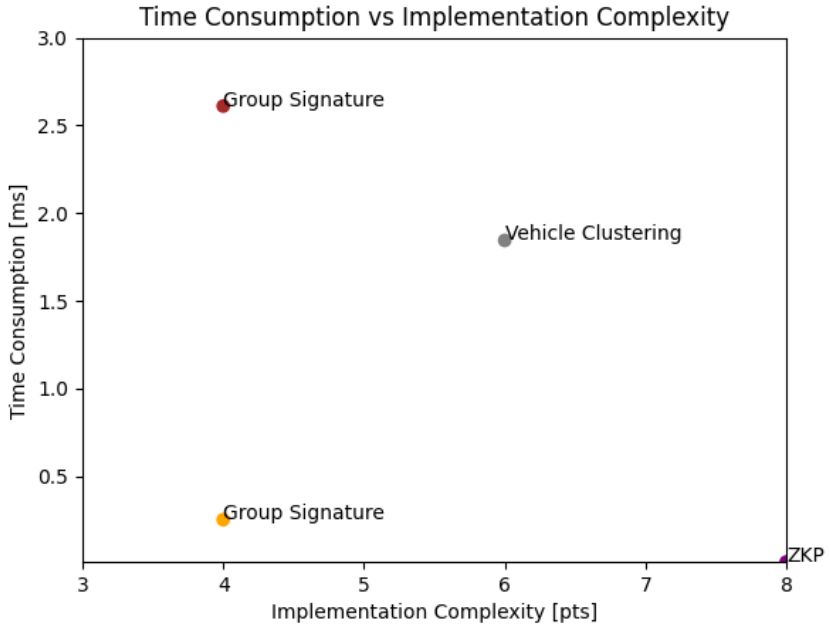


Fig. 4.9: Graph representation of collected results (wide view).

4.9 Evaluation and Future Work

The implementation of PET in CSS could significantly boost user privacy and security. **Pseudonymization and ABCs** are examples of PET that could efficiently protect user identity and personal information during registration and authentication. In order preserve user privacy in the vehicle selection process, **vehicle location cloaking and clustering** could be used. User anonymity could be preserved by **group signatures** during vehicle access and monitoring. **ZKPs and SMPC** could both be used to securely exchange and process sensitive data during transactions.

However, there are also some challenges with PET as well. Pseudonymization is required to guarantee the **uniqueness** of the pseudonyms provided to the users. Nevertheless, this requires a complicated implementation which has to been properly tested for any potential implementation problems which could lead to security vulnerabilities. **Achieving the right level of use** for vehicle location cloaking and clustering to preserve user or vehicle privacy without impacting the service's usability is always a challenge.

There are several challenges with using Group Signature during the accessing process to the selected vehicle. One challenge is **preserving user anonymity** while maintaining responsibility for any malicious actions. Another challenge could be **collusion attacks**, in which multiple users work together to bypass the group signature system. Therefore, future research could focus on implementing modern

cryptographic techniques to improve the system's overall security.

Secure Multi-Party Computation is an excellent PET tool for preserving user data secure, but on the other hand, there is a possibility for **performance issues as multiple parties collaborate to compute a function**. Additionally, there is still an opportunity to improvement in the ability to use SMPC directly on devices with limited processing power and no network connection.

The primary challenge in using Zero-Knowledge Proofs is **ensuring the correctness and completeness of the proofs** provided by users without revealing any additional information. Due to the ZKP protocols' complexity, there could potentially be performance problems and additional computational overhead.

The possibility of using these techniques for the preservation of User and data privacy is still lacking after an individual analysis of each phase using PET tools in CSS and their deployment in complex systems creates a number of risks from both the perspective of the users and the functionality of the system itself as well as from the perspective of reliability and security against different types of attacks. The adoption of new PET would require massive infrastructural and technological investments, which could not be achievable for smaller services.

Future research might concentrate on developing more **user-friendly and effective PET** as well as researching **modern cryptographic methods** including Post Quantum algorithms and additional PET tools to smoothly and inexpensively integrate PET into CSS. In order to promote PETs' widespread adoption in the CSS, additional efforts could be made to increase the general awareness of their characteristics and their advantages.

Conclusion

In conclusion, the primary goal of the theoretical part of this thesis was to provide a comprehensive description of current Smart Transportation Services and their security threats, attacks and countermeasures. These services offer numerous advantages, such as reducing traffic congestion, improving transportation efficiency and promoting sustainable transportation. Real-world use cases of STS were analyzed and it was found that these services are being used globally in various sectors, including public transportation and personal transportation. However, there are also various challenges associated with the implementation of STS, including cybersecurity threats and the need for appropriate infrastructure. The thesis highlighted the importance of cybersecurity in STS, as the interconnections of these systems makes them vulnerable to cyberattacks.

The thesis dealt in depth with the specific Smart Parking Services and Car Sharing Services, which have gained popularity due to their convenience and cost-effectiveness. The sections showed advantages and benefits of CSS, different types of CSS and multiple requirements for running a operation with overlap to regulatory area and legal status. In addition, the thesis identified various security threats in CSS, such as data and privacy threats, cybersecurity threats or physical threats, which could be mitigated by implementing appropriate security measures. Therefore, the use of Privacy Enhancing Technologies was proposed as well as evaluated a correct application to improve the data security and privacy protection of CSS users.

The practical part of the thesis involved proposing a reference scenario of CSS and implementing the five phases in Car Sharing process using some of the PET techniques. Implemented phases consisted of basic user verification and authentication, vehicle selection, vehicle access, vehicle monitoring and secure payment. The proposed solutions were prepared in the chosen programming language – Python. Functional demonstration of the proposed security and privacy protection methods was tested and analyzed, meeting all the research objectives of the thesis assignment.

Overall, this thesis contributes to the understanding of the advantages and challenges of STS, the various components of CSS and the application of PET to preserve data security and protect user privacy in CSS. The thesis successfully achieved its goals by providing an in-depth analysis of these areas and proposing a basic verification implementation to enhance the security and privacy of CSS users. The actual contribution of the work was also the participation in the EEICT 2023 conference, in which the paper was successfully accepted and published in the journal proceedings. All the stated goals of the thesis have been accomplished.

Bibliography

[1] *Intelligent transport systems: Mobility and Transport.* European Commission [online]. 2023 [cit. 2023-05-01]. Available from: https://transport.ec.europa.eu/transport-themes/intelligent-transport-systems_en

[2] XU, Hansong, Jie LIN a Wei YU. *Smart Transportation Systems: Architecture, Enabling Technologies, and Open Issues.* Secure and Trustworthy Transportation Cyber-Physical Systems [online]. Singapore: Springer Singapore, 2017, 2017-10-17, 23-49 [cit. 2023-05-01]. SpringerBriefs in Computer Science. ISBN 978-981-10-3891-4. Available from: https://link.springer.com/chapter/10.1007/978-981-10-3892-1_2/

[3] MAZUR, Steve. *An Introduction to Smart Transportation: Benefits and Examples.* DIGI [online]. Digi International, 2020, 12-09-2020 [cit. 2023-05-01]. Available from: https://www.digi.com/blog/post/introduction-to-smart-transportation-benefits

[4] CELONA, Team. *What Is Smart Transportation & What Are the Benefits?*. Celona [online]. CELONA, 2020, 10-14-2020 [cit. 2023-05-01]. Available from: https://www.celona.io/5g-lan/smart-transportation

[5] *Ertico* [online]. Brussels, Belgium: ERTICO - ITS Europe [cit. 2023-05-01]. Available from: https://ertico.com/

[6] *INRIX* [online]. INRIX [cit. 2023-05-01]. Available from: https://inrix.com/

[7] *Communication Solutions for Intelligent Transportation Systems.* Siemens [online]. Siemens [cit. 2023-05-01]. Available from: https://new.siemens.com/us/en/products/automation/industrial-communication/industrial-network-topics/transportation-networks/intelligent-transportation-systems.html

[8] *Commsignia* [online]. Commsignia [cit. 2023-05-01]. Available from: https://www.commsignia.com/

[9] *Traffic Management: Smart Solutions - for today and in the future!* [online]. [cit. 2023-05-01]. Available from: https://www.swarco.com/solutions/traffic-management

[10] *Park. Pay. Go.* [online]. ParkMobile, LLC. [cit. 2023-05-01]. Available from: https://parkmobile.io/

[11] *ParkMe Brno* [online]. INRIX [cit. 2023-05-01]. Available from: https://www.parkme.com/map#Brno

[12] *Waymo: The World's Most Experienced Driver* [online]. Waymo LLC. [cit. 2023-05-01]. Available from: https://waymo.com/

[13] *Quuppa* [online]. [cit. 2023-05-01]. Available from: https://www.quuppa.com/

[14] *BlaBlaCar* [online]. Comuto [cit. 2023-05-01]. Available from: https://www.blablacar.cz/

[15] *Uber Pool: Share the ride. Share the savings.* [online]. Uber Technologies [cit. 2023-05-01]. Available from: https://www.uber.com/au/en/ride/uberpool/

[16] *C-ROADS: C-ITS system* [online]. Brno, 2016 [cit. 2023-05-01]. Available from: https://www.bkom.cz/chytre-mesto/c-roads/about-the-project-c-roads-174

[17] MAURA, Giorgia. *South Moravian Fire Service's Intelligent Transport System Rewarded At Annual Firefighting Awards.* In: BRNO Daily [online]. 10-28-2021 [cit. 2023-05-01]. Available from: https://sitemaps.brnodaily.com/2021/10/28/brno/south-moravian-fire-services-intelligent-transport-system-rewarded-at-annual-firefighting-awards/

[18] *TRANSPORTATION TECHNOLOGY THAT CONNECTS PEOPLE: Advancing Mobility Together* [online]. Cubic Transportation Systems [cit. 2023-05-01]. Available from: https://www.cubic.com/transportation

[19] *Thales: Transport* [online]. Thales [cit. 2023-05-01]. Available from: https://www.thalesgroup.com/en/markets/transport

[20] PISANO, Paul, Lynette GOODWIN a Andrew STERN. *Surface Transportation Safety and Operations: The Impacts of Weather within the Context of Climate Change* [online]. 20 [cit. 2023-05-01]. Available from: https://www.transportation.gov/sites/dot.gov/files/docs/pisano_Surfact_Trans_Safety_Oper_Impact_Weather_Context_CC.pdf

[21] *Transportation Management. SAP* [online]. [cit. 2023-05-01]. Available from: https://www.sap.com/products/scm/transportation-logistics.html

[22] *Google Maps* [online]. [cit. 2023-05-01]. Available from: https://www.google.com/maps

[23] CARRESE, Filippo, Stefano CARRESE, Sergio Maria PATELLA, Marco PETRELLI a Simone SPORTIELLO. *A Framework for Dynamic Advanced Traveler Information Systems.* In: Future Transportation [online]. 2021, s. 590-600 [cit. 2023-05-01]. ISSN 2673-7590. Available from: https://www.mdpi.com/2673-7590/1/3/31

[24] *Raising safety and throughput with smarter ATC systems.* ADB SAFEGATE [online]. [cit. 2023-05-01]. Available from: https://adbsafegate.com/what-we-do/tower/

[25] *ALSTOM* [online]. ALSTOM Holdings [cit. 2023-05-01]. Available from: https://www.alstom.com/

[26] *Intelligent street lighting.* InteliLIGHT [online]. [cit. 2023-05-01]. Available from: https://intelilight.eu/intelligent-street-lighting-control/

[27] JAN, Bilal, Haleem FARMAN, Murad KHAN, Muhammad TALHA a Ikram Ud DIN. *Designing a Smart Transportation System: An Internet of Things and Big Data Approach.* IEEE Wireless Communications [online]. 2019, 26(4), 73-79 [cit. 2023-05-01]. ISSN 1536-1284. Available from: https://ieeexplore.ieee.org/document/8809663

[28] KARAMI, Zahra a Rasha KASHEF. *Smart transportation planning: Data, models, and algorithms.* Transportation Engineering [online]. 2020, 2 [cit. 2023-05-01]. ISSN 2666691X. Available from: https://doi.org/10.1016/j.treng.2020.100013

[29] CHOUDHARY, Mahashreveta. *What is Intelligent Transport System and how it works?*. In: GEOSPATIAL MEDIA AND COMMUNICATIONS [online]. 01/15/2019 [cit. 2023-05-01]. Available from: https://www.geospatialworld.net/blogs/what-is-intelligent-transport-system-and-how-it-works/

[30] FRANCIS, Judy. *Supporting Intelligent Transportation Systems: Public Roads* [online]. In: . 04-01-2017 [cit. 2023-05-01]. Available from: https://highways.dot.gov/public-roads/marchapril-2017/supporting-intelligent-transportation-systems

[31] *Transportation Sustainability Research Center*. UC Berkeley: Institute of Transportation Studies [online]. [cit. 2023-05-01]. Available from: https://tsrc.berkeley.edu/topics/intelligent-transportation-systems

[32] *What is an OBU (on-board unit)?* [online]. PTOLEMUS Consulting Group [cit. 2023-05-01]. Available from: https://www.ptolemus.com/what-is-an-obu-on-board-unit/

[33] *Intelligent On-board Unit (OBU) 2.0* [online]. Changsha Intelligent Driving Institute Ltd. [cit. 2023-05-01]. Available from: http://www.cidi.ai/index.php/content/228

[34] YUEN, Desmond. *The Future Begins with The Road Side Unit: Edge computing is so much more fun.* In: Medium [online]. 10-08-2020 [cit. 2023-05-01]. Available from: https://medium.com/predict/edge-computing-is-so-much-more-fun-ac2a8a23e696

[35] *Yunex Connected Vehicle Roadside Unit (RSU)* [online]. Mobotrex, Inc. [cit. 2023-05-01]. Available from: https://www.mobotrex.com/product/siemens-connected-vehicle-roadside-unit/

[36] GUERRERO-IBÁÑEZ, Juan, Sherali ZEADALLY a Juan CONTRERAS-CASTILLO. *Sensor Technologies for Intelligent Transportation Systems.* Sensors [online]. 2018, 18(4) [cit. 2023-05-01]. ISSN 1424-8220. Available from: https://www.mdpi.com/1424-8220/18/4/1212

[37] *Leddar™ T16 – Solid-State LiDAR Traffic Sensor* [online]. LeddarTech Inc. [cit. 2023-05-01]. Available from: https://leddarsensor.com/solutions/leddar-t16-traffic-sensor/

[38] *Traffic Control Centres* [online]. PIARC [cit. 2023-05-01]. Available from: https://rno-its.piarc.org/en/network-operations-rno-activities/traffic-control-centres

[39] PERIN, Michel. *Marben Shows its V2X Software on the Latest NXP RoadLINK™ Chipset at the ITS World Congress.* In: CISION PRWeb [online]. 10/05/2015 [cit. 2023-05-13]. Available from: https://www.prweb.com/releases/2015/10/prweb13000268.htm

[40] ISO 13111-2:2022. *Intelligent transport systems (ITS) — The use of personal ITS stations to support ITS service provision for travellers: Part 2: General requirements for data exchange between ITS stations.* Geneva, Switzerland: International Organization for Standardization, 2022. Available from: https://www.iso.org/standard/78863.html

[41] ISO 15638-24:2021. *Intelligent transport systems (ITS) — Framework for collaborative telematics applications for regulated commercial freight vehicles (TARV): Part 24: Safety information provisioning.* Geneva, Switzerland: International Organization for Standardization, 2021. Available from: https://www.iso.org/standard/78358.html

[42] ISO 17419:2018. *Intelligent transport systems (ITS) — Cooperative systems: Globally unique identification.* Geneva, Switzerland: International Organization for Standardization, 2018. Available from: https://www.iso.org/standard/70077.html

[43] ISO/TS 19091:2019. *Intelligent transport systems (ITS) — Cooperative systems: Using V2I and I2V communications for applications related to signalized intersections.* Vol. 2. Geneva, Switzerland: International Organization for Standardization, 2019. Available from: https://www.iso.org/standard/73781.html

[44] ISO 21177:2023. *Intelligent transport systems (ITS): ITS station security services for secure session establishment and authentication between trusted devices.* Geneva, Switzerland: International Organization for Standardization, 2023. Available from: https://www.iso.org/standard/81067.html

[45] ISO 24102-6:2018. *Intelligent transport systems (ITS) — Communications access for land mobiles (CALM): ITS station management — Part 6: Path and flow management.* Geneva, Switzerland: International Organization for Standardization, 2018. Available from: https://www.iso.org/standard/62292.html

[46] *IEEE Standards Activities for Intelligent Transportation Systems (ITS)* [online]. [cit. 2023-05-01]. Available from: https://standards.ieee.org/wp-content/uploads/import/documents/other/its.pdf

[47] IEEE 1609.0-2019. *IEEE Guide for Wireless Access in Vehicular Environments (WAVE) Architecture*: VT/ITS - Intelligent Transportation Systems. IEEE Standards Association, 2019. Available from: https://standards.ieee.org/ieee/1609.0/6792/

[48] IEEE 802.11P-2010. *IEEE Standard for Information technology: Local and metropolitan area networks - Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 6: Wireless Access in Vehicular Environments.* IEEE Standards Association, 2010. Available from: https://standards.ieee.org/ieee/1609.0/6792/

[49] *Intelligent Transport Systems (ITS): Technical Committee (TC).* ETSI [online]. [cit. 2023-05-01]. Available from: https://www.etsi.org/committee/1402-its

[50] KOLAJA, David. *SECURE COMMUNICATION IN THE INTERNET OF VEHICLES* [online]. Brno, 2022 [cit. 2023-05-01]. Available from: https://www.vut.cz/www_base/zav_prace_soubor_verejne.php?file_id=241576. Master's thesis. Brno University of Technology. Supervisor Doc. Ing. Lukáš Malina, Ph.D.

[51] ETSI TS 102 940. *Intelligent Transport Systems (ITS) - Security: ITS communications security architecture and security management.* Release 2. France: ETSI, 2021. Available from: https://www.etsi.org/deliver/etsi_ts/102900_102999/102940/02.01.01_60/ts_102940v020101p.pdf

[52] ETSI TS 102 941. *Intelligent Transport Systems (ITS) - Security: Trust and Privacy Management.* Release 2. France: ETSI, 2022. Available from: https://www.etsi.org/deliver/etsi_ts/102900_102999/102941/02.02.01_60/ts_102941v020201p.pdf

[53] ETSI TS 103 097. *Intelligent Transport Systems (ITS) - Security: Security header and certificate formats.* Release 2. France: ETSI, 2021. Available from: https://www.etsi.org/deliver/etsi_ts/103000_103099/103097/02.01.01_60/ts_103097v020101p.pdf

[54] AL-TURJMAN, Fadi, Hadi ZAHMATKESH a Ramiz SHAHROZE. *An overview of security and privacy in smart cities' IoT communications.* Transactions on Emerging Telecommunications Technologies [online]. 2022, 33(3) [cit. 2023-05-01]. ISSN 2161-3915. Available from: https://doi.org/10.1002/ett.3677

[55] MECHEVA, Teodora a Nikolay KAKANAKOV. *Cybersecurity in Intelligent Transportation Systems.* Computers [online]. 2020, 9(4) [cit. 2023-05-01]. ISSN 2073-431X. Available from: https://doi.org/10.3390/computers9040083

[56] JAVED, Muhammad, Elyes BEN HAMIDA a Wassim ZNAIDI. *Security in Intelligent Transport Systems for Smart Cities: From Theory to Practice.* Sensors [online]. 2016, 16(6) [cit. 2023-05-01]. ISSN 1424-8220. Available from: https://doi.org/10.3390/s16060879

[57] DROZHZHIN, Alex. *Black Hat USA 2015: The full story of how that Jeep was hacked.* In: Kaspersky daily [online]. 08-06-2015 [cit. 2023-05-01]. Available from: https://www.kaspersky.com/blog/blackhat-jeep-cherokee-hack-explained/9493/

[58] *2018 SingHealth data breach.* In: Wikipedia: the free encyclopedia [online]. San Francisco (CA): Wikimedia Foundation, 2001- 2023, 03-29-2023 [cit. 2023-05-01]. Available from: https://en.wikipedia.org/wiki/2018_SingHealth_data_breach

[59] *Cyber security in intelligent public transport: Challenges and Solutions* [online]. United Kingdom: Russell Publishing, 06-20-2016 [cit. 2023-05-01]. Available from: https://www.intelligenttransport.com/transport-articles/19618/cyber-security-intelligent-public-transport/

[60] FREDIANELLI, Luca, Stefano CARPITA, Marco BERNARDINI, Lara Ginevra DEL PIZZO, Fabio BROCCHI, Francesco BIANCO a Gaetano LICITRA. *Traffic Flow Detection Using Camera Images and Machine Learning Methods in ITS for Noise Map and Action Plan Optimization.* Sensors [online]. 2022, 22(5) [cit. 2023-03-09]. ISSN 1424-8220. Available from: https://doi:10.3390/s22051929

[61] SAHARAN, Sandeep, Seema BAWA a Neeraj KUMAR. *Dynamic pricing techniques for Intelligent Transportation System in smart cities: A systematic review.* Computer Communications [online]. 2020, 150, 603-625 [cit. 2023-05-01]. ISSN 01403664. Available from: https://doi:10.1016/j.comcom.2019.12.003

[62] EL HAMDANI, Sara, Nabil BENAMAR a Mohamed YOUNIS. *Pedestrian Support in Intelligent Transportation Systems: Challenges, Solutions and Open issues.* Transportation Research Part C: Emerging Technologies [online]. 2020, 121 [cit. 2023-05-01]. ISSN 0968090X. Available from: https://doi:10.1016/j.trc.2020.102856

[63] DZURENDA, Petr, Carles Anglès TAFALLA, Sara RICCI a Lukas MALINA. *Privacy-Preserving Online Parking Based on Smart Contracts.* The 16th International Conference on Availability, Reliability and Security [online]. New York, NY, USA: ACM, 2021, 2021-08-17, 1-10 [cit. 2023-03-09]. ISBN 9781450390514. Available from: https://doi:10.1145/3465481.3470058

[64] DZURENDA, Petr, Florian JACQUES, Manon KNOCKAERT, Maryline LAURENT, Lukas MALINA, Raimundas MATULEVICIUS, Qiang TANG a Aimilia TASIDOU. *Privacy-preserving solution for vehicle parking services complying with EU legislation.* PeerJ Computer Science [online]. 2022, 8 [cit. 2023-03-09]. ISSN 2376-5992. Available from: https://doi:10.7717/peerj-cs.1165

[65] ALSAFERY, Wael, Badraddin ALTURKI, Stephan REIFF-MARGANIEC a Kamal JAMBI. *Smart Car Parking System Solution for the Internet of Things in Smart Cities* [online]. IEEE, 2018, 2018, 1-5 [cit. 2023-05-01]. ISBN 978-1-5386-4427-0. Available from: https://doi:10.1109/CAIS.2018.8442004

[66] MOUNCE, Richard a John D. NELSON. *On the potential for one-way electric vehicle car-sharing in future mobility systems.* Transportation Research Part A: Policy and Practice [online]. 2019, 120, 17-30 [cit. 2023-03-09]. ISSN 09658564. Available from: https://doi:10.1016/j.tra.2018.12.003

[67] ROBLEK, Vasja, Maja MEŠKO a Iztok PODBREGAR. *Impact of Car Sharing on Urban Sustainability.* In: Sustainability [online]. 2021 [cit. 2023-05-01]. ISSN 2071-1050. Available from: https://doi.org/10.3390/su13020905

[68] NANSUBUGA, Brenda a Christian KOWALKOWSKI. *Carsharing: a systematic literature review and research agenda.* In: Journal of Service Management [online]. 2021, s. 55-91 [cit. 2023-05-01]. ISSN 1757-5818. Available from: https://doi:10.1108/JOSM-10-2020-0344

[69] POLLICINO, Francesco, Luca FERRETTI, Dario STABILI a Mirco MARCHETTI. *Accountable and privacy-aware flexible car sharing and rental services.* 2021 IEEE 20th International Symposium on Network Computing and Applications (NCA) [online]. IEEE, 2021, 2021-11-23, 1-7 [cit. 2023-03-09]. ISBN 978-1-6654-9550-9. Available from: https://doi:10.1109/NCA53618.2021.9685942

[70] HUANG, Cheng, Rongxing LU, Jianbing NI a Xuemin SHEN. DAPA: *A Decentralized, Accountable, and Privacy-Preserving Architecture for Car Sharing Services.* IEEE Transactions on Vehicular Technology [online]. 2020, 69(5), 4869-4882 [cit. 2023-03-09]. ISSN 0018-9545. Available from: https://doi:10.1109/TVT.2020.2980777

[71] AÏVODJI, Ulrich Matchi, Sébastien GAMBS, Marie-José HUGUET a Marc-Olivier KILLIJIAN. *Meeting points in ridesharing: A privacy-preserving approach.* In: Transportation Research Part C: Emerging Technologies [online]. 2016, s. 239-253 [cit. 2023-05-01]. ISSN 0968090X. Available from: https://doi:10.1016/j.trc.2016.09.017

[72] *Car4way* [online]. [cit. 2023-05-01]. Available from: https://www.car4way.cz/carsharing

[73] *HoppyGo* [online]. [cit. 2023-05-01]. Available from: https://hoppygo.com/

[74] *Autonapul* [online]. [cit. 2023-05-01]. Available from: https://www.autonapul.cz/

[75] *Rekola* [online]. [cit. 2023-05-01]. Available from: https://www.rekola.cz/en/

[76] *NextBike* [online]. [cit. 2023-05-01]. Available from: https://www.nextbikeczech.com/en/

[77] *Bolt* [online]. [cit. 2023-05-01]. Available from: https://bolt.eu/

[78] *Lime* [online]. [cit. 2023-05-01]. Available from: https://www.li.me/

[79] *Tier* [online]. [cit. 2023-05-01]. Available from: https://www.tier.app/

[80] *Brno Smart parking* [online]. [cit. 2023-05-01]. Available from: https://www.parkovanivbrne.cz/en/

[81] *MYTO CZ* [online]. [cit. 2023-05-01]. Available from: https://mytocz.eu/en

[82] *TOOL 4 EUROPE* [online]. [cit. 2023-05-01]. Available from: https://toll4europe.eu/en/

[83] *European Electronic Toll Service (EETS)* [online]. [cit. 2023-05-01]. Available from: https://www.asfinag.at/en/toll/go-toll/eets/

[84] *eCall* STMicroelectronics [online]. [cit. 2023-05-01]. Available from: https://www.st.com/en/applications/mobility-services/ecall.html

[85] *Co umí mobilní aplikace DPMB Info?* DPMB [online]. [cit. 2023-05-01]. Available from: https://www.dpmb.cz/co-umi-mobilni-aplikace-dpmb-info

[86] *Route Planning and Optimization: Public Transit.* ESRI [online]. [cit. 2023-05-01]. Available from: https://www.esri.com/en-us/industries/transit/business-areas/route-planning-optimization

[87] *The world's leading transport planning software.* PTV Visium [online]. PTV Planung Transport Verkehr GmbH [cit. 2023-05-01]. Available from: https://www.myptv.com/en/mobility-software/ptv-visum

[88] *Intelligent Mobility Solutions*. Conduent Transportation [online]. Conduent Business Services, LLC. [cit. 2023-05-01]. Available from: https://transportation.conduent.com/intelligent-mobility-solutions/

[89] XIAOLIANG, Zhang, Jia LIMIN a Qi-zhou HU. *Discussion on Optimization of Public Transportation Network Setting considering Three-State Reliability.* In: Journal of Advanced Transportation [online]. 2021, s. 1-7 [cit. 2023-05-01]. ISSN 2042-3195. Available from: https://doi:10.1155/2021/6940263

[90] *What is a digital twin?*. IBM [online]. [cit. 2023-05-01]. Available from: https://www.ibm.com/topics/what-is-a-digital-twin

[91] O'BRIEN, JJ. *The Benefits of Demand-Responsive Transport in Rural Areas.* In: Liftago [online]. 10-09-2020 [cit. 2023-05-01]. Available from: https://www.liftango.com/resources/benefits-of-demand-responsive-transport-in-rural-areas

[92] *Demand-Responsive Transport.* Ridango [online]. Ridango AS ostutingimused [cit. 2023-05-01]. Available from: https://ridango.com/demand-responsive-transport/

[93] KUBITZ, Beate. *Is Demand-Responsive Transport a viable solution?*. In: Smart Transport [online]. Bauer Consumer Media, 12-22-2020 [cit. 2023-05-01]. Available from: https://www.smarttransport.org.uk/insight-and-policy/latest-insight-and-policy/is-demand-responsive-transport-a-viable-solution

[94] *TrafficSmart.cz: Budujeme moderní dopravní řešení* [online]. Traffic Smart [cit. 2023-05-01]. Available from: https://trafficsmart.cz/

[95] MANGIARACINA, Riccardo, Angela TUMINO, Giovanni MIRAGLIOTTA, Giulio SALVADORI a Alessandro PEREGO. *Smart parking management in a smart city: Costs and benefits.* 2017 IEEE International Conference on Service Operations and Logistics, and Informatics (SOLI) [online]. IEEE, 2017, 2017, 27-32 [cit. 2023-05-13]. ISBN 978-1-5090-5847-1. Available from: https://ieeexplore.ieee.org/document/8120964

[96] ALQAZZAZ, Ali, Ibrahim ALRASHDI, Esam ALOUFI, Mohamed ZOHDY a Hua MING. SecSPS: *A Secure and Privacy-Preserving Framework for Smart Parking Systems.* Journal of Information Security [online]. 2018, 09(04), 299-314 [cit. 2023-05-13]. ISSN 2153-1234. Available from: https://www.scirp.org/journal/paperinformation.aspx?paperid=87800

[97] SARKER, Victor Kathan, Tuan Nguyen GIA, Imed Ben DHAOU, and Tomi WESTERLUND. *Smart Parking System with Dynamic Pricing, Edge-Cloud Computing and LoRa* Sensors [online]. 2020, 20(17), 4669 [cit. 2023-05-13]. Available from: https://doi.org/10.3390/s20174669

[98] FERRERO, Francesco, Guido PERBOLI, Mariangela ROSANO a Andrea VESCO. *Car-sharing services: An annotated review.* In: Sustainable Cities and Society [online]. 2018, s. 501-518 [cit. 2023-05-01]. ISSN 22106707. Available from: https://doi:10.1016/j.scs.2017.09.020

[99] NGUYEN, Quyen. *Factors affecting the willingness to use car sharing service: A case study of Stavanger* [online]. Stavanger, 2020 [cit. 2023-05-01]. Available from: https://uis.brage.unit.no/uis-xmlui/bitstream/handle/11250/2690135/Quyen_Nguyen.pdf. Master's thesis. University of Stavanger. Supervisor Associate Professor Gorm Kipperberg.

[100] BERT, Julien, Brian COLLIE, Gang XU a Marco GERRITS. *What's Ahead for Car Sharing?: The New Mobility and Its Impact on Vehicle Sales.* In: Boston Consulting Group [online]. 02/23/2016 [cit. 2023-05-13]. Available from: https://www.bcg.com/publications/2016/automotive-whats-ahead-car-sharing-new-mobility-its-impact-vehicle-sales

[101] ZHOU, Fan, Zuduo ZHENG, Jake WHITEHEAD, Robert K. PERRONS, Simon WASHINGTON a Lionel PAGE. *Examining the impact of car-sharing on private vehicle ownership.* Transportation Research Part A: Policy and Practice [online]. 2020, 138, 322-341 [cit. 2023-05-13]. ISSN 09658564. Available from: https://doi.org/10.1016/j.tra.2020.06.003

[102] XU, Yan, Xuehong JI, Ziniu JIN a TANG. *What travel scenarios are the opportunities of car sharing?.* In: PLOS ONE [online]. 2021 [cit. 2023-05-01]. ISSN 1932-6203. Available from: https://doi:10.1371/journal.pone.0260605

[103] *Car Sharing in Europe: Business Models, National Variations and Upcoming Disruptions.* Monitor Deloitte [online]. 2017 [cit. 2023-05-01]. Available from: https://www2.deloitte.com/content/dam/Deloitte/de/Documents/consumer-industrial-products/CIP-Automotive-Car-Sharing-in-Europe.pdf

[104] *Getaround* [online]. [cit. 2023-05-01]. Available from: https://www.getaround.com/

[105] *Zipcar* [online]. [cit. 2023-05-01]. Available from: https://www.zipcar.com/

[106] *ShareNow* [online]. [cit. 2023-05-01]. Available from: https://www.share-now.com/

[107] *Bolt Drive* [online]. [cit. 2023-05-01]. Available from: https://bolt.eu/en/drive/

[108] *CityBee* [online]. [cit. 2023-05-01]. Available from: https://citybee.lt/en/

[109] *Turo* [online]. [cit. 2023-05-01]. Available from: https://turo.com/

[110] *Autolevi* [online]. [cit. 2023-05-01]. Available from: https://autolevi.ee/

[111] *Enterprise* [online]. [cit. 2023-05-01]. Available from: https://www.enterprise.com/en/home.html

[112] *Hertz* [online]. [cit. 2023-05-01]. Available from: https://www.hertz.com/rentacar/reservation/

[113] Directorate-General for Mobility and Transport. *European Commission adopts new initiatives for sustainable and smart mobility* [online]. 02-02-2022 [cit. 2023-05-01]. Available from: https://transport.ec.europa.eu/news/european-commission-adopts-new-initiatives-sustainable-and-smart-mobility-2022-02-02_en

[114] *Sustainable and Smart Mobility Strategy – putting European transport on track for the future.* EUR-Lex [online]. 12-09-2020 [cit. 2023-05-01]. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020DC0789

[115] KLOSOWSKI, Thorin. *The State of Consumer Data Privacy Laws in the US (And Why It Matters).* In: NY Times [online]. 09-06-2021 [cit. 2023-05-01]. Available from: https://www.nytimes.com/wirecutter/blog/state-of-privacy-laws-in-us/

[116] LEMOS, Robert. *Cybercriminals Take Aim at Connected Car Infrastructure.* In: Dark Reading [online]. Informa PLC Informa UK Limited, 10/29/2021 [cit. 2023-05-14]. Available from: https://www.darkreading.com/attacks-breaches/cybercriminals-take-aim-at-connected-car-infrastructure

[117] KELARESTAGHI, Kaveh Bakhsh, Mahsa FORUHANDEH, Kevin HEASLIP a Ryan GERDES. *Intelligent Transportation System Security: Impact-Oriented Risk Assessment of in-Vehicle Networks.* In: IEEE Intelligent Transportation Systems Magazine [online]. 2021, s. 91-104 [cit. 2023-05-01]. ISSN 1939-1390. Available from: https://doi:10.1109/MITS.2018.2889714

[118] *Privacy Enhancing Technologies – A Review of Tools and Techniques.* Office of the Privacy Commissioner of Canada [online]. 11-01-2017 [cit. 2023-05-01]. Available from: https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2017/pet_201711/

[119] LI, Li, Ahmed EL-LATIF a Xiamu NIU. *Elliptic curve ElGamal based homomorphic image encryption scheme for sharing secret images.* In: Signal Processing [online]. 92. 2012, s. 1069-1078 [cit. 2023-05-15]. ISSN 0165-1684. Available from: https://www.sciencedirect.com/science/article/abs/pii/S0165168411003823

[120] PLEŞCA, Cezar, Mihai TOGAN a Cristian LUPAŞCU. *Homomorphic Encryption Based on Group Algebras and Goldwasser-Micali Scheme.* In: Innovative Security Solutions for Information Technology and Communications [online]. Cham: Springer International Publishing, 2016, 2016-10-05, s. 149-166 [cit. 2023-05-15]. Lecture Notes in Computer Science. ISBN 978-3-319-47237-9. Available from: https://link.springer.com/chapter/10.1007/978-3-319-47238-6_11

[121] *OpenFHE.* Yeti Digital Ltd. [online]. [cit. 2023-05-15]. Available from: https://www.openfhe.org/

[122] *Microsoft SEAL: Build end-to-end encrypted data storage and computation services.* Microsoft [online]. [cit. 2023-05-15]. Available from: https://www.microsoft.com/en-us/research/project/microsoft-seal/publications/

[123] BOSSUAT, Jean-Philippe. *A library for lattice-based multiparty homomorphic encryption in Go* [online]. 03-14-2023 [cit. 2023-05-15]. Available from: https://github.com/tuneinsight/lattigo

[124] KEYLESS TECHNOLOGIES. *A beginner's guide to Secure Multiparty Computation.* Medium [online]. [cit. 2023-05-15]. Available from: https://medium.com/@keylesstech/a-beginners-guide-to-secure-multiparty-computation-dc3fb9365458

[125] MORENO, RYAN. *SECURE MULTI-PARTY COMPUTATION: GARBLED CIRCUITS* [online]. [cit. 2023-05-15]. Available from: https://ryan-moreno.github.io/resources/secure_multi_party_computation_paper.pdf

[126] STARKWARE. *STARK* [online] [cit. 2023-05-15]. Available from: https://starkware.co/stark/

[127] ZHANG, Yupeng, Tiancheng XIE a Jiaheng ZHANG. *Libra: Succinct Zero-Knowledge Proofs with Optimal Prover Computation* [online] [cit. 2023-05-15]. Available from: https://eprint.iacr.org/2019/317.pdf

[128] BEN-SASSON, Eli, Alessandro CHIESA, Michael RIABZEV, Nicholas SPOONER, Madars VIRZA a Nicholas P. WARD. *Aurora: Transparent Succinct Arguments for R1CS* [online]. 05-08-2019 [cit. 2023-05-15]. Available from: https://eprint.iacr.org/2018/828.pdf

[129] TESSARO, Stefano a Chenzhi ZHU. *Revisiting BBS Signatures*. In: Advances in Cryptology – EUROCRYPT 2023 [online]. Cham: Springer Nature Switzerland, 2023, 2023-04-16, s. 691-721 [cit. 2023-05-15]. Lecture Notes in Computer Science. ISBN 978-3-031-30588-7. Available from: https://link.springer.com/chapter/10.1007/978-3-031-30589-4_24

[130] DILMEGANI, Cem. *Top 10 Privacy Enhancing Technologies & Use Cases in 2023*: INFORMATION SECURITY. In: AI Multiple [online]. 12-21-2022 [cit. 2023-05-01]. Available from: https://research.aimultiple.com/privacy-enhancing-technologies/

[131] EUROPEAN UNION AGENCY FOR CYBERSECURITY. *DATA PSEUDONYMISATION: ADVANCED TECHNIQUES & USE CASES: Technical analysis of cybersecurity measures in data protection and privacy* [online]. 01-2021. [cit. 2023-05-14]. ISBN 978-92-9204-465-7. Available from: https://www.enisa.europa.eu/publications/data-pseudonymisation-advanced-techniques-and-use-cases/

[132] *BEST PRACTICES AND TECHNIQUES FOR PSEUDONYMIZATION.* In: (ISC2̂ [online]. 06-14-2021 [cit. 2023-05-14]. Available from: https://blog.isc2.org/isc2_blog/2021/06/best-practices-and-techniques-for-pseudonymization.html

[133] STEVOVIC, Jovan. *Pseudonymization of health data. A visual guide with tips.* In: The Chino.io Blog [online]. 04-20-2019 [cit. 2023-05-14]. Available from: https://blog.chino.io/visual-guide-to-health-data-pseudonymization/

[134] BEHERA, Monik Raj, Sudhir UPADHYAY, Suresh SHETTY, Sudha PRIYADARSHINI, Palka PATEL a Ker Farn LEE. *FedSyn: Synthetic Data Generation using Federated Learning* [online]. 2022 [cit. 2023-05-14]. Available from: https://arxiv.org/abs/2203.05931

[135] *Privacy-Enhancing Cryptography - PEC tools.* NIST: COMPUTER SECURITY RESOURCE CENTER [online]. 04-25-2023 [cit. 2023-05-01]. Available from: https://csrc.nist.gov/Projects/pec/pec-tools

[136] CHUMBLEY, Alex, Christopher WILLIAMS a Alex DUNA. *Homomorphic Encryption: Partially Homomorphic Algorithms* [online]. [cit. 2023-05-14]. Available from: https://brilliant.org/wiki/homomorphic-encryption/

[137] *What is Fully Homomorphic Encryption?.* In: Inpher [online]. [cit. 2023-05-01]. Available from: https://inpher.io/technology/what-is-fully-homomorphic-encryption/

[138] *What is Secure Multiparty Computation.* Inpher [online]. [cit. 2023-05-01]. Available from: https://inpher.io/technology/what-is-secure-multiparty-computation/

[139] *Sharemind Technology* In: Sharemind Developer Zone [online]. [cit. 2023-05-14]. Available from: https://docs.sharemind.cyber.ee/2022.03/prologue

[140] *Zero Knowledge What? An Introduction to Zero Knowledge.* Stanford Code the Change [online]. [cit. 2023-05-01]. Available from: https://codethechange.stanford.edu/guides/guide_zk.html

[141] GARAKH, Iliya. *What is Zero-knowledge Proof?: Wonderful, but how does it REALLY work?.* Passwork [online]. 12-20-2021 [cit. 2023-05-14]. Available from: https://blog.passwork.pro/zero-knowledge-proof/

[142] VITHANA, Sajani, Zhusheng WANG a Sennur ULUKUS. *Private Information Retrieval and Its Applications: An Introduction, Open Problems, Future Directions* [online]. In: . 04-27-2023, s. 13 [cit. 2023-05-01]. Available from: https://doi.org/10.48550/arXiv.2304.14397

[143] ELLIS, Jack. *How to build a privacy-first software business.* In: Fathom Analytics [online]. 10-05-2020 [cit. 2023-05-01]. Available from: https://usefathom.com/blog/privacy-first-business

[144] *Privacy Notice: How we disclose personal information.* Zipcar Group [online]. 01-01-2020 [cit. 2023-05-02]. Available from: https://www.zipcar.com/en-gb/privacy

[145] *Privacy Notice App & Service* Sharenow [online]. 09-01-2021 [cit. 2023-05-02]. Available from: https://www.share-now.com/at/en/legal/#privacy

[146] *Privacy policy.* Turo [online]. 09-01-2021 [cit. 2023-05-03]. Available from: https://turo.com/gb/en/policies/privacy

[147] *Hashlib — Secure hashes and message digests.* Python Software Foundation [online]. 2023 [cit. 2023-05-15]. Available from: https://docs.python.org/3.9/library/hashlib.html

[148] DWORKIN, Morris J. *SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions* [online]. FEDERAL INF. PROCESS. STDS. (NIST FIPS), NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. 08-04-2015 [cit. 2023-05-15]. Available from: https://www.nist.gov/publications/sha-3-standard-permutation-based-hash-and-extendable-output-functions

[149] *Post-quantum cryptography* [online]. 2019 [cit. 2023-05-15]. Available from: https://pqcrypto.org/

[150] CAMENISCH, Jan a Markus MICHELS. *A Group Signature Scheme Based on an RSA-Variant* [online]. Denmark, 1998 [cit. 2023-05-15]. Available from: https://www.brics.dk/RS/98/27/BRICS-RS-98-27.pdf Publication. University of Aarhus.

[151] *PyCryptodome's documentation* [online]. 2023 [cit. 2023-05-15]. Available from: https://www.pycryptodome.org/

[152] *Sharemind MPC (Multi-Party Computation)* [online]. Tallinn, Estonia: Cybernetica, 2023 [cit. 2023-05-15]. Available from: https://sharemind.cyber.ee/sharemind-mpc/

[153] ELKOUMY, Gamal. *Shareprom: A Tool for Privacy-Preserving Inter-Organizational Process Mining* [online]. 09-10-2020 [cit. 2023-05-15]. Available from: https://github.com/Elkoumy/shareprom

[154] GoodiesHQ. *Zero-Knowledge Proof Implementation for Passwords and Other Secrets* [online]. 01-24-2021 [cit. 2023-05-15]. Available from: https://github.com/GoodiesHQ/noknow-python

[155] OpenMinded. *A SMPC companion library for Syft* [online]. 05-15-2022 [cit. 2023-05-15]. Available from: https://github.com/OpenMined/SyMPC

Symbols and abbreviations

STS	Smart Transport Services
ITS	Intelligent Transport Systems
GPS	Global Positioning System
DSRC	Dedicated Short-Range Communications
OBU	On-Board Unit
RSU	Road Side Unit
TCC	Traffic Control Centers
ISO	International Organization for Standardization
IEEE	Institute of Electrical and Electronics Engineers
ETSI	European Telecommunications Standards Institute
V2I	Vehicle-to-Infrastructure
I2V	Infrastructure-to-Vehicle
WAVE	Wireless Access in Vehicular Environments
C-ITS	Cooperative Intelligent Transport Systems
IoT	Internet of Things
AI	Artificial Intelligence
PET	Privacy Enhancing Technology
RBAC	Role-Based Access Control
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
SIEM	Security Information and Event Management
MFA	Multi Factor Authentication
SPS	Smart Parking Services
CSS	Car Sharing Services

GDPR	General Data Protection Regulation
EV	Electric Vehicles
HE	Homomorphic Encryption
SMPC	Secure Multi-Party Computation
ZKP	Zero-Knowledge Proof
PIR	Private Information Retrieval
GRS	Group and Ring Signatures
SHE	Somewhat Homomorphic Encryption
FHE	Fully Homomorphic Encryption
DP	Differential Privacy
SDG	Synthetic Data Generation
FL	Federated Learning
RNG	Random Number Generator
DPO	Data Protection Officer
CRM	Customer Relationship Management

A Content of the digital attachment

- / ..... root folder
  - sources ..... source codes in Python
    - usecase1-solution.py
    - usecase2-solution.py
    - usecase3-solution.py
    - usecase4-solution.py
    - usecase5-solution.py
  - tests ..... test codes in Python
    - usecase1-test.py
    - usecase2-test.py
    - usecase3-test.py
    - usecase5-test.py
    - test-vehicle-locations.csv
  - thesis-lovinger.pdf ..... thesis
  - thesis-presentation.pdf ..... thesis presentation
  - eeict2023-lovinger.pdf ..... EEICT 2023 article