Privacy Risks in Connected Vehicles: Profiling Threats and Mitigation Strategies

Marco De Santis[1(✉)], Christian Esposito[1], and Michele Mastroianni[2]

[1] University of Salerno, Fisciano, Italy
{mdesantis,esposito}@unisa.it
[2] University of Foggia, Foggia, Italy
michele.mastroianni@unifg.it

Abstract. The increasing connectivity of modern vehicles enables advanced services but also raises serious privacy concerns. Continuous data collection from sensors and V2X communications can lead to detailed user profiling and potential misuse, such as tracking, discrimination, or identity theft. This work presents a preliminary methodology for analyzing and mitigating privacy risks in connected vehicles. It combines a Privacy Impact Assessment (PIA) with misuse-case-based threat modeling to identify critical scenarios involving unauthorized access, data tampering, and data loss. We propose targeted technical and organizational mitigation strategies, taking into account the real-time and resource constraints of automotive systems. A re-evaluation of the PIA demonstrates a notable reduction in the likelihood and impact of these risks. Our results highlight the value of structured risk assessments and practical safeguards in protecting user privacy. Beyond enhancing privacy posture, the proposed approach supports alignment with increasingly strict European regulations such as the GDPR and the AI Act, promoting the compliant and responsible deployment of connected vehicle technologies.

Keywords: Cybersecurity · Threat Modelling · Privacy · Connected Vehicles · Data Protection · Profiling Risks · Privacy Impact Assessment (PIA)

1 Introduction

Connectivity is profoundly transforming the automotive sector, redefining not only the driving experience, but also the interaction between vehicles, infrastructure, and users. Connected vehicles equipped with Vehicle-to-Everything (V2X) systems continuously communicate with other vehicles, road infrastructure, pedestrians, and smart devices through advanced wireless technologies such as DSRC, LTE, and emerging 5G/6G networks. This connectivity is supported by a wide range of sensors: GPS, radar, LiDAR, cameras, and microphones that continuously gather data from the surrounding environment [1,12],

© The Author(s), under exclusive license to Springer Nature Switzerland AG 2026
O. Gervasi et al. (Eds.): ICCSA 2025 Workshops, LNCS 15893, pp. 285–302, 2026.
https://doi.org/10.1007/978-3-031-97645-2_19

making these vehicles key components in the development of Intelligent Transportation Systems (ITS) [3]. The connected vehicle ecosystem is the result of joint efforts by automakers, technology providers, standardization bodies, public authorities, and research institutions [1]. Recent deployments in smart cities and Advanced Driver-Assistance Systems (ADAS) have shown tangible benefits, including reduced traffic congestion and improved road safety, thus increasing public interest in these technologies [9,19]. Beyond mobility, connected vehicles enable advanced services such as high-quality infotainment, remote diagnostics, and emerging applications like health monitoring. Real-time integration of sensor data allows dynamic responses to road conditions, improving comfort and contributing to traffic management and environmental sustainability [8,14]. However, these technological capabilities also introduce critical privacy challenges. Connected vehicles collect sensitive data such as location, driving behaviour and user preferences which, when aggregated, can create detailed profiles of individuals' habits [8,10,12]. For instance, GPS and telematics data can track frequent routes, while audio and video recordings may capture private conversations. Without proper safeguards, such data may be exposed to unauthorized entities. One of the most pressing concerns is user profiling. While personalization can improve driving experience, correlating diverse data streams may inadvertently reveal sensitive information. Malicious actors could exploit these profiles for identity theft, phishing attacks, or manipulative advertising [6]. The risk of re-identification from anonymized datasets becomes especially relevant when multiple sources are combined, potentially leading to discrimination in services or insurance pricing [13]. This study presents a Privacy Impact Assessment (PIA) tailored to the connected vehicle context, enriched by an approach based on misuse case modeling. Our contribution lies in the systematic identification of profiling risks arising from the interconnection of multiple vehicular data streams. Unlike generic approaches, our methodology models realistic threats and enables quantitative evaluation of proposed mitigations. The approach combines a literature review with practical misuse case modeling. By simulating realistic attack scenarios, we analyze current system vulnerabilities and assess technical countermeasures, such as encryption, anonymization, and differential privacy, alongside organizational measures such as data minimization, user consent management, and regulatory compliance. This work provides a dual contribution: It improve understanding of privacy risks in connected vehicles and offers practical guidance for developing more secure systems. The proposed framework aims to build trust and promote the responsible deployment of connected technologies. Finally, this preliminary study lays the groundwork for future research toward automated tools supporting PIA in compliance with current regulations, helping bridge the gap between innovation and privacy protection in the automotive domain.

2 Related Work

The increasing connectivity of modern vehicles has raised significant privacy concerns for both users and manufacturers. Connected vehicles continuously collect

and process sensitive data such as location, driving habits, and user preferences. This section reviews existing approaches to privacy risk assessment and mitigation, highlighting key gaps that motivate our preliminary work.

The evolution of PIA frameworks in the automotive domain shows a growing move toward specialized and tailored methodologies. General standards like ISO 27005 have been adapted for vehicular systems but often lack the required specificity. Bella et al. [4] combined ISO 27005 with STRIDE threat modeling, while Panda et al. [15] extended NIST PRAM with cybersecurity considerations for autonomous vehicles. Stingelová et al. [17] and Wu et al. [18] propose integrated methods combining STRIDE and LINDDUN, although these often address isolated phases of the analysis process. Another approach may be found in Di Martino et al. [7], in which data processing activities (i.e. business processes involving personal data) have been represented in BPMN notation and the DPIA has been carried out using ontologies. Attack modeling research identifies recurring threats, such as spoofing, tampering, and disclosure [4,15]. Carlton and Malik [5] focus on persistent user profiles in infotainment systems. However, these works often lack a direct link between threats and measurable privacy impacts. Data profiling risks have been discussed in relation to vehicle telemetry [2,11,16], especially regarding the potential for re-identification when combining multiple data sources. While these contributions provide detailed threat characterization, they generally do not include structured tools for assessing the effectiveness of mitigation measures. Mitigation strategies include technical controls like encryption, multi-factor authentication, and Privacy Enhancing Technologies (PETs) such as anonymization and differential privacy [15,18]. Some solutions, like the VIPR system [5], focus on specific components. However, many approaches remain conceptual and do not fully consider the implementation challenges in constrained automotive environments.

To address these limitations, our work presents a preliminary solution aimed at analyzing privacy risks in connected vehicles through a structured and systematic approach. The proposed methodology combines privacy impact assessment with realistic attack modeling, incorporating both technical and organizational considerations. Particular emphasis is placed on understanding the operational context, identifying profiling-related risks, and evaluating the effectiveness of mitigation strategies. This study serves as an initial step toward developing practical tools for privacy-aware system design, aligned with the constraints of automotive environments and recent regulatory developments.

This study provides a foundational step toward developing practical tools for privacy assessment in connected vehicles, offering initial insights that align with current regulatory trends and operational constraints.

3 Methodology

Our methodology consists of seven sequential phases, designed to assess privacy risks in connected vehicles in a structured and iterative manner, from data analysis to risk mitigation and validation.

1. Context: Overview, Data, Processes & Supporting Assets. We first define the operational scope of connected vehicles, mapping key data sources (e.g., GPS, telematics, cameras, radars, LiDAR, biometric sensors, V2X systems), associated processes, and supporting assets (software, hardware, protocols).

2. Fundamental Principles: Proportionality, Necessity & Controls. We assess whether collected data is proportionate and necessary for system functionality. This includes evaluating compliance with privacy principles and regulations (e.g., GDPR, ISO/SAE 21434) and documenting existing safeguards such as data minimization, encryption, and pseudonymization.

3. Risks: Identification & Assessment. We identify privacy threats in four categories: unauthorized access, data tampering (unwanted modification), data loss (disappearance), and a consolidated risk overview. Each threat is evaluated based on its likelihood and potential impact.

4. Attack Modeling: Misuse Cases. We simulate realistic attack scenarios—such as man-in-the-middle, injection, or insider threats—to understand how vulnerabilities could be exploited and validate the relevance of identified risks.

5. Mitigation Strategies: Technical & Organizational Measures. To address the risks, we define targeted countermeasures including end-to-end encryption, differential privacy, and RBAC at the technical level, and data minimization policies, consent frameworks, and audits at the organizational level.

6. PIA Update: Risk Reduction. We re-assess the risks by updating the Privacy Impact Assessment. This step quantifies the effectiveness of the mitigations, ensuring that residual risks are acceptable and compliant with legal thresholds.

7. Results & Discussion: Visualization & Evaluation. We evaluate pre- and post-mitigation outcomes, using visual comparisons and analysis to validate the overall effectiveness and adaptability of the methodology.

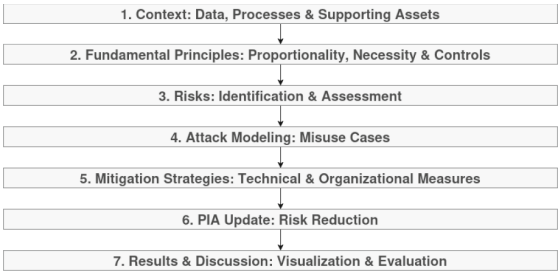

Fig. 1. Workflow overview of the proposed methodology.

This structured process provides a practical foundation for privacy-aware design in connected vehicles. Its iterative nature, especially the feedback loop

between mitigation and reassessment, makes it adaptable to evolving threats and technologies.

4 Privacy Risks Analysis in Connected Cars

The increasing interconnectivity of vehicles has opened a new frontier in transportation, where large amounts of data are continuously generated and processed. While these data streams enable significant advancements, such as enhanced road safety, improved traffic management, and personalized user services, they also introduce critical privacy challenges. In particular, the risk of profiling, where personal data is aggregated to infer sensitive information about drivers, is of growing concern.

4.1 Data Sources for Profiling

Connected vehicles are equipped with multiple subsystems that generate various types of data. The table below maps key data sources, describes the nature of the information collected, indicates whether the data can be used for profiling, and qualitatively assesses the associated privacy risk.

Table 1. Mapping of Data Sources in Connected Vehicles and Their Profiling Risk

Data Source	Description	Profiling	Privacy Risk
GPS	Provides precise location data, route history, and travel times	Yes	High
Telematics	Records driving behavior such as speed, acceleration, braking, and engine performance	Yes	High
Cameras	Capture images of the environment, driver, and in-cabin activities	Yes	High
Radar	Measures distances and detects obstacles in real time	No	Limited
LiDAR	Generates 3D maps of the surrounding environment	No	Limited
Infotainment Systems	Logs user interactions, app usage, and multimedia preferences	Yes	High
Biometric Sensors	Collects data for authentication	Yes	High
V2X Communications	Exchanges information with other vehicles and infrastructure	Yes	High

As shown in Table 1, certain data sources, such as GPS, telematics, cameras, infotainment systems, and biometric sensors, are directly linked to user profiling and pose a high privacy risk. These data streams provide detailed and continuous insights into individuals' habits, routines, and behaviors. Other sources, like radar and LiDAR, are less directly linked to personal identification but may still

contribute to privacy risks when combined with other data. V2X communications, although valuable for real-time coordination and safety, can also expose sensitive behavioral patterns if not properly secured. Their associated risk is considered limited only if strong access control and encryption mechanisms are implemented. In the absence of such protections, even data originally designed for cooperative driving can be exploited for profiling purposes. In this context, data protection strategies are not optional safeguards, but essential components in determining the actual level of privacy risk. Without technical countermeasures, such as end-to-end encryption, pseudonymization, and strict role-based access policies, even seemingly innocuous data can contribute to invasive profiling. Furthermore, when advanced AI techniques such as clustering, classification, or behavioral prediction are applied to these datasets, the privacy implications are significantly amplified. These models can reveal commuting patterns, frequent destinations, or even personal preferences, transforming raw data into detailed and sensitive user profiles. The combination of high-resolution data and predictive analytics underscores the need for rigorous risk assessment and proactive mitigation.

4.2 Data Protection Impact Assessment (DPIA)

A Data Protection Impact Assessment (DPIA) is a crucial tool for systematically identifying and mitigating privacy risks associated with the processing of personal data in connected vehicles. Under GDPR and related standards, the DPIA process ensures that the design and operation of data processing systems adhere to privacy by design and by default principles.

Our DPIA framework evaluates privacy risks based on two key dimensions: the likelihood of a risk occurring and the severity of its impact. For example, the probability of an attacker intercepting unencrypted V2X communications is assessed alongside the potential consequences, such as unauthorized tracking or data manipulation. Risk levels are classified using a scale from Negligible to Maximum. Table 2 provides a summary of the risk classification criteria used in this study.

Table 2. Risk Classification Scale for DPIA

Risk Level	Description
Negligible	Minimal risk with little or no impact on privacy; effective technical and organizational controls are in place
Limited	Risk exists but with low impact; mitigations reduce the likelihood or severity of a breach
Significant	Noticeable risk where data exposure could lead to moderate privacy violations; requires prompt mitigation actions
Maximum	High risk with potential for severe impact on individuals' privacy, possibly leading to significant legal and reputational consequences

Within our DPIA, we systematically identify and assess several critical categories of privacy risk. These include the risk of illegitimate access, where unauthorized interception or breaches of data may occur; the possibility of unwanted modification, which refers to tampering or alteration of data that could result in inaccurate or even fraudulent profiling; and the threat of data disappearance, involving the loss of information due to system failures, malicious deletion, or ransomware attacks. In addition to these specific risks, we also construct an overall risk overview that provides a comprehensive picture of all potential privacy threats across the connected vehicle ecosystem. This broader perspective enables us to analyze how different vulnerabilities may interact and compound one another, ultimately offering a more complete foundation for mitigation strategies.

Figure 2 illustrates the comprehensive risk overview derived from our DPIA. In this figure, you can observe the distribution of potential impacts, threats, and sources. For example, under the *Illegitimate Access* category, the diagram highlights the risk of unauthorized surveillance and data theft through vulnerabilities such as weak API authentication and insufficient encryption. Similarly, the *Unwanted Modification* category underscores risks associated with data tampering that can distort user profiles, while the *Data Disappearance* segment indicates the impact of losing critical data due to ransomware or insider actions.

The comprehensive mapping of data sources (Table 1) and the DPIA risk classification (Table 2) together provide a robust framework to assess, quantify, and ultimately mitigate privacy risks in connected vehicles. This integrated approach enables stakeholders to identify vulnerable areas, implement effective countermeasures, and continuously monitor the performance of the system against evolving threats.

5 Attack Modeling with Misuse Cases

Based on our risk assessment, we identified several critical attack scenarios that pose significant threats to the privacy of connected vehicles, particularly with respect to user profiling. Drawing from a comprehensive overview of the risks (see Fig. 2), we focused on modeling attacks that present high severity and a high probability of occurrence. Our analysis is driven by the need to understand how an attacker can exploit vulnerabilities in the system and the resultant damage that such attacks can cause. These attacks, which allow the profiling of both the vehicle and the driver, represent some of the most pressing privacy risks in connected vehicles.

The three key scenarios we have modeled are Behavioral Profiling via Telemetry, Unauthorized Access to Sensitive Infotainment System Data, and Surveillance via Internal and External Cameras. These scenarios were chosen because they represent attacks that allow an attacker to exploit critical components of a connected vehicle, enabling them to profile both the vehicle and the driver. In each of these cases, the attacker can gather and misuse sensitive data, leading to severe privacy breaches.

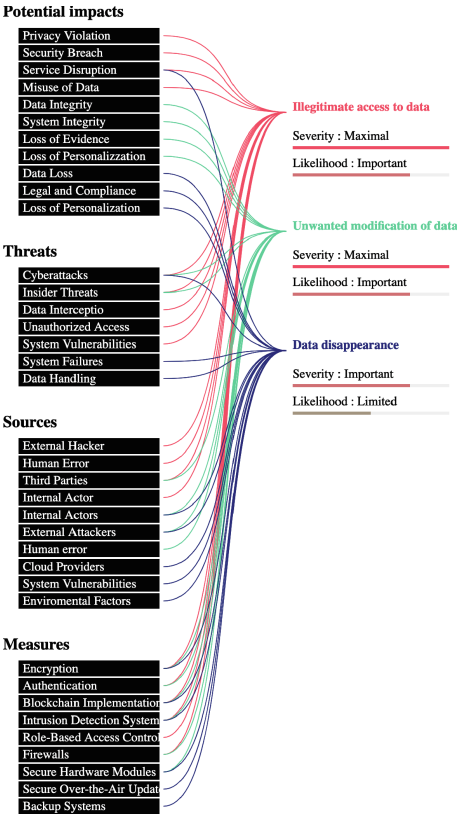

Fig. 2. Risk Overview from the DPIA. This diagram maps potential impacts, threats, and sources in connected vehicle systems.

In the first scenario, an attacker intercepts data from the GPS and the Telematics Control Unit (TCU) of the vehicle, exploiting vulnerabilities in the communication with the Cloud API. This allows the attacker to reconstruct a detailed profile of the driver, including frequently visited routes, driving times, and habits. By gaining access to this data, the attacker can track the driver in real time, exposing their private movements and daily routines. The impact on privacy is significant, as this data could be used for unauthorized tracking, targeted advertising, or even discriminatory practices, such as manipulation of insurance premiums or advertising targeting. This type of attack is particularly concerning because it allows continuous surveillance of the driver without their consent, making it a critical risk in terms of privacy and data security. Figure 3 illustrates the Behavioral Profiling via Telemetry misuse case, showing how an attacker can exploit vehicle communication systems to collect detailed profiling data.

The second scenario focuses on unauthorized access to sensitive infotainment system data. In this case, the attacker exploits vulnerabilities in the infotain-

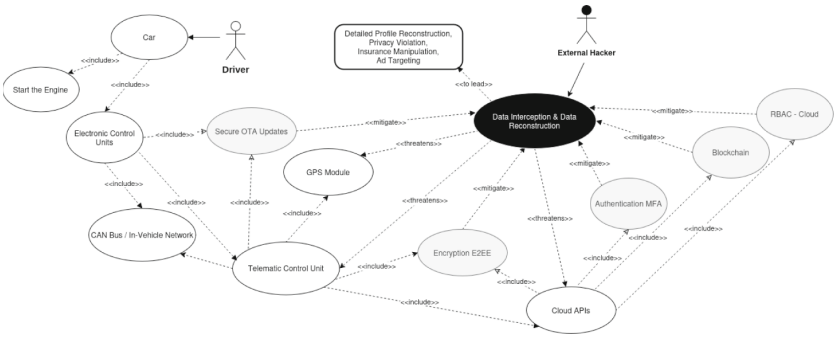

Fig. 3. Behavioral Profiling via Telemetry misuse case

ment system or in the Bluetooth/Smartphone Sync connections to gain access to sensitive information such as contacts, call logs, multimedia preferences, and even audio recordings through the vehicle's microphone. The attacker may monitor and intercept these data streams, allowing them to eavesdrop on private conversations and gain access to the vehicle user's personal information. This unauthorized access can lead to severe privacy violations, as the attacker can listen to private conversations and gather personal data without the driver's knowledge. The risks associated with this type of attack include identity theft, invasive profiling, and phishing attacks. Given the widespread use of Bluetooth and mobile device connections, this type of vulnerability is particularly concerning in the context of connected vehicles, as it opens the door to significant privacy breaches and potential exploitation of sensitive information. Figure 4 provides a UML diagram that models this scenario, illustrating the methods through which an attacker can access the infotainment system.

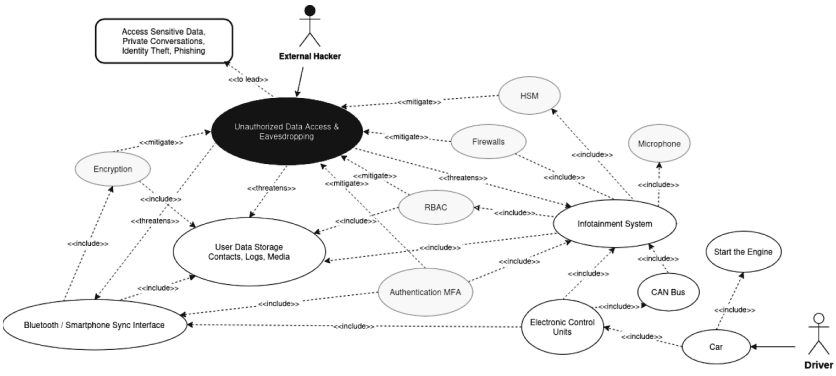

Fig. 4. Unauthorized access to sensitive infotainment system data misuse case

The third scenario involves surveillance via internal and external cameras. In this scenario, the attacker gains remote access to the vehicle's cameras, either internal or external, by exploiting vulnerabilities in the camera management systems or wireless connections. The internal cameras can be used to monitor the driver's behavior and emotional state, while the external cameras can track the vehicle's movements. This type of surveillance allows the attacker to continuously monitor the vehicle and its occupants without consent, potentially gathering intimate details about the driver's emotional responses and daily interactions. The external cameras also provide the attacker with the ability to track the vehicle's location and movement patterns, which could be used for malicious purposes. The impact of this attack is profound, as it compromises the privacy of the driver and passengers, making it a significant security concern. Figure 5 visually represents this misuse case, showing how surveillance via both internal and external cameras can be exploited by an attacker.

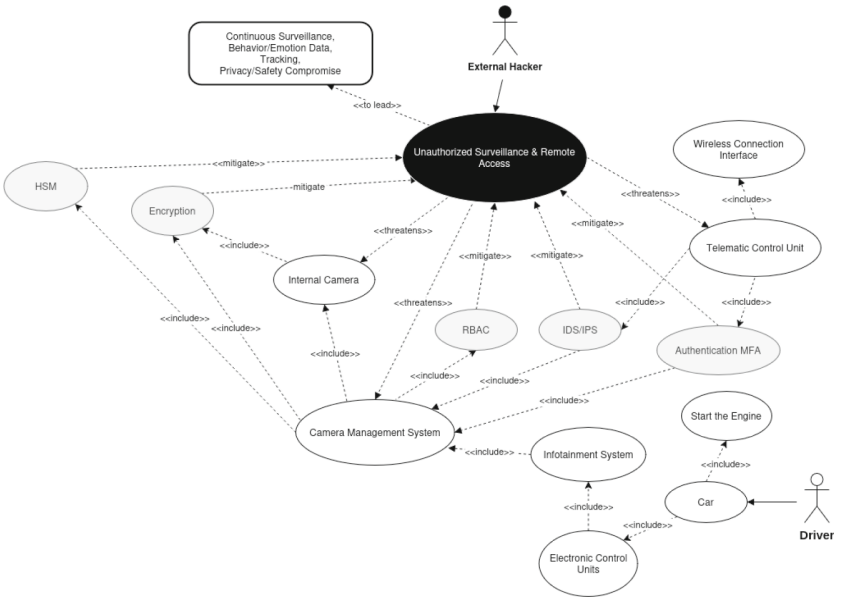

Fig. 5. Surveillance via internal and external cameras misuse case

These three scenarios: Behavioral Profiling via Telemetry, Unauthorized Access to Sensitive Infotainment System Data, and Surveillance via Internal and External Cameras, have been selected because they capture the most critical and relevant privacy risks in connected vehicle systems. Each of these attacks involves exploiting vulnerabilities in key vehicle systems, allowing attackers to gather and misuse personal data. By modeling these attacks, we highlight the severe consequences of privacy breaches that can occur when an attacker successfully exploits these vulnerabilities.

In addition to the three primary misuse cases described, there are several other potential threats that could further compromise the privacy of connected vehicle users. Unauthorized profiling data access is one such threat, where an attacker gains unauthorized access to profiling data through weak access controls or vulnerabilities in the data storage systems. This could allow the attacker to gather and misuse detailed personal data about the driver's habits and preferences. Another potential threat involves tampering with driver profiling data, where an attacker deliberately alters the data associated with the driver's profile, such as falsifying driving behavior or modifying driving logs. This could be achieved through methods such as data injection or exploiting cloud database vulnerabilities. The goal of such attacks could be to manipulate insurance premiums or obscure risky driving behavior.

Profiling data erasure attacks represent another critical risk, where an attacker deletes or makes critical profiling data inaccessible, either through ransomware or by exploiting weaknesses in backup and recovery systems. The loss of this data could impair personalized services, disrupt data retention compliance, or even expose the vehicle owner to legal consequences. Finally, the extraction of geolocation data for surveillance is a growing concern. In this case, an attacker exploits vulnerabilities in cloud APIs or intercepts unsecured V2X/GPS communications to continuously harvest location data. This data could be used to reconstruct detailed movement patterns, providing the attacker with sensitive information about the user's whereabouts and daily habits.

These additional potential threats reinforce the diverse ways in which an attacker can compromise the privacy of connected vehicle users. Together with the three primary misuse cases, they highlight the need for robust security measures to protect user data and prevent unauthorized access, manipulation, or loss of sensitive information. By thoroughly modeling these attack scenarios, we provide a clearer understanding of the critical risks and the need for strong countermeasures to safeguard the privacy of connected vehicle users.

6 Mitigation Strategies and PIA Update

Following the identification of privacy risks and the modeling of potential attack scenarios through misuse cases, our study has analyzed and proposed a set of mitigation strategies aimed at addressing the specific vulnerabilities highlighted in our analysis. The goal of this section is to assess how these strategies, if implemented, could significantly reduce the likelihood and impact of privacy violations related to user profiling in connected vehicles. These strategies include both technical countermeasures that could be integrated into the system architecture and organizational measures that focus on governing data management practices. It is important to note that while we are not directly implementing these solutions, our focus is on evaluating their potential effectiveness in improving security and reducing the privacy risks identified in our analysis. The selection and implementation of these strategies must also consider the specific constraints of the automotive environment, such as real-time processing requirements and limited

computational resources available on the vehicle. Subsequently, we conducted an analytical reassessment of the PIA to quantify the potential effectiveness of these proposed mitigations in reducing the overall risk landscape.

6.1 Technical Countermeasures

To counter the identified threats, such as unauthorized data access, tampering, and potential re-identification from aggregated datasets, we analyzed several advanced technical controls that could be applied in the specific context of connected vehicles. These measures are aligned with the strategies defined in our PIA, including those related to encryption, authentication, and blockchain. While we are not implementing these solutions directly, our analysis shows how they could help mitigate the risks identified.

We recommended the mandatory use of robust End-to-End Encryption protocols, such as TLS, for all data transmissions between the vehicle, backend servers, and any third-party services. The implementation of cryptographic algorithms must balance security with the performance demands of the real-time environment, favoring computationally efficient solutions or leveraging hardware acceleration where available. Our analysis highlights that this measure directly addresses the risk of data interception during transit, as shown in the misuse cases involving V2X communication sniffing or interactions with cloud APIs. Furthermore, we discussed the need for encryption for data at rest, ensuring that stored profiling information (e.g., location history, driving behavior logs) is protected in the event of a storage system compromise, while adhering to performance constraints.

In line with the Anonymization of Data strategy outlined in the PIA, we analyzed the application of robust Pseudonymization and Anonymization techniques throughout the data lifecycle. Where feasible, particularly for large-scale analysis or research purposes, we evaluated techniques such as k-anonymity, l-diversity, or t-closeness, taking into account the computational overhead these may introduce. Our analysis demonstrated that these techniques are effective in preventing re-identification when datasets are combined or released, thereby mitigating the risks associated with correlating behavioral and infotainment data.

For scenarios requiring aggregated user data analysis (e.g., traffic pattern analysis, service enhancement), we assessed the use of Differential Privacy mechanisms. By adding carefully calibrated noise to query results, differential privacy allows valuable insights to be extracted from collective data without disclosing sensitive information about individual users. Our evaluation indicated that differential privacy can effectively protect against inference attacks, while maintaining the utility of the data for analysis.

To counter threats such as unauthorized access to profiling data by insiders or external attackers (Fig. 3), we analyzed the implementation of strict Role-Based Access Control (RBAC) policies, as part of the PIA's Role-Based Access Control mitigation strategy. These policies ensure that access to sensitive profiling data is granted according to the principle of least privilege, reducing exposure and limiting the attack surface. We also evaluated the integration of multi-factor

authentication for privileged access, selecting methods that are feasible in the vehicular environment.

Finally, to address the misuse case of tampering with driver profiling data (Fig. 4), we analyzed the use of cryptographic techniques such as digital signatures or Hash-based Message Authentication Codes to guarantee the Integrity and Authenticity of collected data. For critical logs, we explored the feasibility of using blockchain or distributed ledger technologies to create immutable records. While blockchain solutions are resource-intensive, our analysis suggests that they could be feasible in specific cases, such as ensuring the integrity of critical vehicle logs.

These technical measures, though not directly implemented in our study, were assessed for their potential integration into the connected vehicle's architecture and associated backend systems, forming the first line of defense against privacy threats, while considering specific operational constraints.

6.2 Organizational and Legal Measures

Technical solutions alone are insufficient without solid organizational policies and adherence to legal frameworks. Therefore, we analyzed the integration of these technical countermeasures with organizational and legal measures, which are in line with the PIA's Privacy by Design and Privacy by Default strategy. We established guidelines promoting a Data Minimization Policy, supporting the collection of only the data strictly necessary for the intended purpose. This involved reviewing every data point identified in Table 1 and evaluating its necessity, thereby reducing the total volume of sensitive data processed and stored. We also proposed the creation of a transparent and user-friendly Consent Management Framework, in line with the Explicit Consent for Data Collection mentioned in the PIA. This framework provides users with granular control over what data is collected, how it is used, and with whom it may be shared. Our analysis confirmed that such a framework would ensure compliance with GDPR requirements by providing clear explanations of the privacy implications for each data category, while also offering mechanisms for easy consent withdrawal. To ensure ongoing Compliance and Governance with relevant regulations such as GDPR, and industry standards like ISO/SAE 21434 (Cybersecurity Engineering for Road Vehicles), we recommended regular internal and external audits, staff training programs, and protocols for data breach notification and response. Furthermore, we emphasized the importance of integrating privacy and security considerations throughout the vehicle and system development lifecycle (Secure Development Lifecycle - SDL), incorporating the principles of "Privacy by Design" and "Security by Design" from the early requirement stages through to deployment and maintenance.

These organizational measures, when paired with technical countermeasures, aim to create a culture of privacy awareness and responsibility, ensuring that data management practices align with legal requirements and user expectations.

6.3 PIA Reassessment

Following the implementation of the technical and organizational mitigation strategies, we conducted a reassessment of the PIA to evaluate the extent to which these interventions reduced the previously identified privacy risks. The objective was to quantify how the measures influenced both the likelihood and the severity of each risk scenario.

Our focus remained on the three core threats identified earlier: unauthorized data access, unwanted modification of data, and data disappearance. Each of these risks was re-evaluated by re-estimating its probability of occurrence and its potential impact on user privacy. For example, the adoption of End-to-End Encryption and RBAC significantly lowered the likelihood of unauthorized access, while techniques such as pseudonymization and data minimization effectively reduced the severity of the resulting impact.

This reassessment was carried out using the same qualitative risk classification scale as the initial PIA (Negligible, Limited, Significant, Maximum). The comparison between pre- and post-mitigation assessments revealed a noticeable shift in risk levels. In particular, risks initially considered significant, such as persistent access to sensitive data or the silent loss of information—were downgraded to more acceptable levels.

To visually illustrate this reduction in risk, we performed a comparative analysis represented in Fig. 6. The figure shows how many of the assessed risks have moved from higher-risk zones (typically characterized by high likelihood

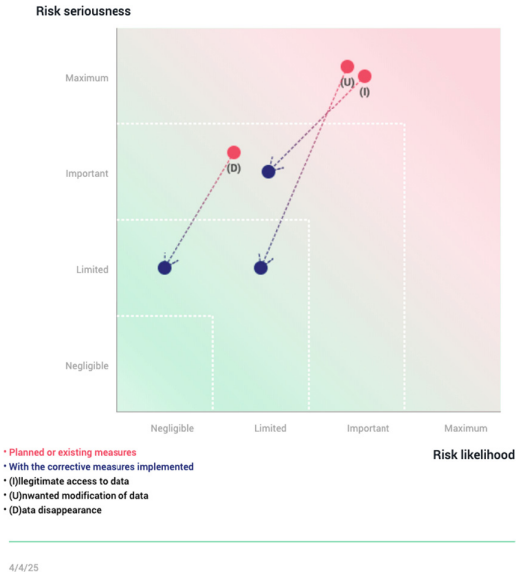

Fig. 6. Graphical representation of risk severity and likelihood estimation pre- and post-mitigation for privacy threats in connected vehicle profiling.

and high impact) to lower-risk quadrants, confirming the overall effectiveness of the proposed mitigation strategies.

In addition to these improvements, we analyzed the relative contribution of different mitigation categories. Technical measures proved especially effective in reducing both unauthorized access and unwanted data modification. Organizational controls played a key role in minimizing risks related to data disappearance—particularly through data retention policies and access audits. When combined, these technical and organizational safeguards resulted in a comprehensive risk reduction across all categories.

Finally, we identified the residual risks, those that remain despite the application of mitigation strategies. These were reviewed in light of organizational policy thresholds and relevant regulatory standards, confirming that the remaining risks fall within acceptable bounds.

This PIA reassessment provides a critical validation of our preliminary framework. It demonstrates, through a structured and comparative analysis, that the applied combination of technical and organizational measures meaningfully reduces privacy risks in connected vehicle ecosystems, particularly those associated with user profiling and misuse of vehicular data.

7 Results and Discussion

The application of our integrated methodology, which combines data source analysis, misuse case modeling, and an iterative PIA, has yielded significant results regarding the privacy risks associated with profiling in connected vehicles and the effectiveness of the proposed mitigation strategies.

The main result emerging from our analysis is the quantification of risk reduction achieved through the combined application of the technical and organizational countermeasures proposed in Sect. 6. As illustrated in the comparative analysis (Fig. 6), the most critical risks identified in the initial phase, specifically illegitimate access, unwanted modification, and disappearance of personal data related to profiling, show a notable decrease in both the likelihood of occurrence and the severity of potential impact. The combined effectiveness of End-to-End Encryption techniques (optimized for real-time contexts), pseudonymization, access control (RBAC), integrity verification, together with data minimization policies and transparent consent management, proved fundamental in reducing the overall exposure to profiling risks.

These findings fully support our initial hypotheses: a systematic and multilayered approach, based on the PIA methodology and enriched by threat modeling through misuse cases, is effective not only in identifying critical vulnerabilities but also in validating the impact of countermeasures. The PIA reassessment confirmed that the proposed strategies bring the residual risk within potentially acceptable thresholds, demonstrating the practical validity of the adopted methodological framework.

The implications of these results for the automotive industry and future regulations are manifold. Firstly, they underscore the urgency for vehicle manufacturers (OEMs) and technology providers to proactively adopt “Privacy by Design”

and "Privacy by Default" principles in the development of connected systems. Our study provides an operational framework that can guide this process in a structured manner. Secondly, the results suggest that future regulations (such as updates to GDPR or specific standards like ISO/SAE 21434) should not only require the execution of PIAs but potentially also the quantifiable demonstration of risk reduction achieved through implemented mitigations, before launching new services based on vehicular data.

To adapt to these growing privacy requirements, automotive companies can adopt several strategies. They can use methodologies similar to ours to conduct thorough internal assessments of their current and future systems, identifying and prioritizing mitigation interventions based on quantified risk analysis. It is crucial, as highlighted in Sect. 6, to select and implement technical countermeasures that balance security and privacy robustness with the computational and latency constraints typical of the automotive environment. Furthermore, investing in more transparent and granular consent mechanisms and clearly communicating the adopted protection measures can help strengthen user trust, an increasingly decisive factor for market acceptance. Collaboration within the industry for sharing best practices and adhering to recognized standards (like ISO/SAE 21434) represents another fundamental step.

8 Conclusion

This work introduced a preliminary methodology for identifying and mitigating privacy risks arising from user profiling in connected vehicles. The proposed approach integrates a structured Privacy Impact Assessment (PIA) with threat modeling through realistic misuse cases, enabling the identification of critical vulnerabilities related to the collection, processing, and potential misuse of personal data generated within vehicular systems. The results confirm that profiling risks are particularly acute when data from multiple subsystems—positioning, telemetry, infotainment, or biometric modules—are aggregated without adequate safeguards. Our methodology demonstrates that a coordinated application of technical mechanisms, including encryption, pseudonymization, and access control, together with organizational policies focused on data minimization, consent management, and regulatory adherence, can substantially reduce both the likelihood and the impact of these risks. The structured and iterative nature of the process allows for continuous refinement and validation of privacy protection strategies. Effectively, the execution of the PIA in this study constitutes a complete Data Protection Impact Assessment (DPIA) under the GDPR framework. However, the proposed methodology extends beyond typical compliance exercises by incorporating concrete threat modeling through misuse cases and simulating realistic attack scenarios. This allows not only for early identification of vulnerabilities but also for the quantitative estimation of risk and the evaluation of mitigation effectiveness, thus offering a more operational and risk-driven approach to privacy management. Beyond risk mitigation, this work contributes to aligning system design with the requirements of evolving European regulations,

particularly the General Data Protection Regulation (GDPR) and the Artificial Intelligence Act (AI Act). These frameworks impose strict obligations to ensure data protection and prohibit high-risk practices such as manipulation or exploitation through AI, but often lack prescriptive technical standards. In this context, our methodology offers a structured, adaptable, and replicable baseline that anticipates regulatory expectations while enhancing the trustworthiness of connected vehicle systems. The methodology is especially relevant for embedded and AI-based automotive functions, where the combination of real-time constraints and sensitive data flows creates complex privacy challenges. Early-stage privacy assessments become essential to detect vulnerabilities, reduce attack surfaces, and ensure that user rights are protected by design. This study lays the groundwork for future developments aimed at transforming the proposed methodology into a practical, regulation-ready tool. Key directions for future research include empirical validation through prototyping and real-world deployment, assessment of system performance impacts, and adaptation of the framework to emerging technologies such as cooperative V2X communication, onboard AI inference, and IoT integration. In this perspective, the methodology we propose aligns with and complements regulatory instruments like the DPIA under the GDPR and the Fundamental Rights Impact Assessment (FRIA) introduced in the AI Act. These tools are not only legal requirements but also essential for systematically identifying, evaluating, and minimizing risks associated with data processing and AI deployment. By extending and operationalizing these assessments, our work contributes to the development of automotive systems that are not only compliant but also resilient, transparent, and accountable by design.

Acknowledgements. This work has been partially supported by the Secure Federated Learning for Mobility (SEM) project, funded by the Agreements for innovation in the automotive sector supply chain of the Ministry of Business and Made in Italy and has been partially supported by project PRODIGI (PROcessi decisionali DIGitalizzati per una propulsione ad Idrogeno efficiente ed efficace), CNMS – Centro Nazionale Mobilità Sostenibile – Codice Identificativo CN00000023, SPOKE 12 – SUSTAINABLE PROPULSION – CUP B43C22000440001.

References

1. Abdo, A., Chen, H., Zhao, X., Wu, G., Feng, Y.: Cybersecurity on connected and automated transportation systems: a survey. IEEE Trans. Intell. Veh. **9**(1), 1382–1401 (2023)
2. Aljzaere, H.S.J., Kaladi, R.K., Hardt, W.: Analysis of privacy risks of vehicle telematics. In: 2024 International Conference on Computing, Internet of Things and Microwave Systems (ICCIMS), pp. 1–3. IEEE (2024)
3. Alnasser, A., Sun, H., Jiang, J.: Cyber security challenges and solutions for V2X communications: a survey. Comput. Netw. **151**, 52–67 (2019)
4. Bella, G., Biondi, P., Tudisco, G.: A double assessment of privacy risks aboard top-selling cars. Automot. Innov. **1**, 1–18 (2023)

5. Carlton, J., Malik, H.: Safeguarding personal identifiable information (PII) after smartphone pairing with a connected vehicle. J. Sens. Actuator Netw. **13**(5), 63 (2024)
6. De Vincenzi, M., Moore, J., Smith, B., Sarma, S.E., Matteucci, I.: Security risks and designs in the connected vehicle ecosystem: in-vehicle and edge platforms. IEEE Open J. Veh. Technol. (2024)
7. Di Martino, B., Mastroianni, M., Campaiola, M., Morelli, G., Sparaco, E.: Semantic techniques for validation of GDPR compliance of business processes. In: Barolli, L., Hussain, F.K., Ikeda, M. (eds.) CISIS 2019. AISC, vol. 993, pp. 847–855. Springer, Cham (2020). https://doi.org/10.1007/978-3-030-22354-0_78
8. Ghosh, S., Zaboli, A., Hong, J., Kwon, J.: An integrated approach of threat analysis for autonomous vehicles perception system. IEEE Access **11**, 14752–14777 (2023)
9. He, Q., Meng, X., Qu, R.: Towards a severity assessment method for potential cyber attacks to connected and autonomous vehicles. J. Adv. Transp. **2020**(1), 6873273 (2020)
10. Hossain, S., Senouci, S.M., Brik, B., Boualouache, A.: A privacy-preserving self-supervised learning-based intrusion detection system for 5G–V2X networks. Ad Hoc Netw. **166**, 103674 (2025)
11. Li, H., Ma, D., Medjahed, B., Kim, Y.S., Mitra, P.: Analyzing and preventing data privacy leakage in connected vehicle services. SAE Int. J. Adv. Current Pract. Mob. **1**(2019-01-0478), 1035–1045 (2019)
12. Limbasiya, T., Teng, K.Z., Chattopadhyay, S., Zhou, J.: A systematic survey of attack detection and prevention in connected and autonomous vehicles. Veh. Commun. **37**, 100515 (2022)
13. Mastroianni, M., Palmieri, F., Ficco, M., Kozik, R., Choraś, M.: Privacy risk analysis and metrics in capturing and storing network traffic. In: 2023 24th International Conference on Control Systems and Computer Science (CSCS), pp. 580–585 (2023). https://doi.org/10.1109/CSCS59211.2023.00097
14. Panda, J., Jain, R.D.: Cyber security challenges in V2C and in vehicle network. Technical report, SAE Technical Paper (2024)
15. Panda, S., Panaousis, E., Loukas, G., Kentrotis, K.: Privacy impact assessment of cyber attacks on connected and autonomous vehicles. In: Proceedings of the 18th International Conference on Availability, Reliability and Security, pp. 1–9 (2023)
16. Pesé, M.D., Shin, K.G.: Survey of automotive privacy regulations and privacy-related attacks. SAE Technical Paper (2019)
17. Stingelová, B., Thrakl, C.T., Wrońska, L., Jedrej-Szymankiewicz, S., Khan, S., Svetinovic, D.: User-centric security and privacy threats in connected vehicles: a threat modeling analysis using stride and LINDDUN. In: 2023 IEEE International Conference on Dependable, Autonomic and Secure Computing, International Conference on Pervasive Intelligence and Computing, International Conference on Cloud and Big Data Computing, International Conference on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech), pp. 0690–0697. IEEE (2023)
18. Wu, X., Xu, X., Bilal, M.: Toward privacy protection composition framework on internet of vehicles. IEEE Consum. Electron. Mag. **11**(6), 32–38 (2021)
19. Yoshizawa, T., et al.: A survey of security and privacy issues in V2X communication systems. ACM Comput. Surv. **55**(9), 1–36 (2023)