Privacy Impact Assessment of Cyber Attacks on Connected and Autonomous Vehicles

Sakshyam Panda
s.panda@greenwich.ac.uk
University of Greenwich
London, UK

Emmanouil Panaousis
e.panaousis@greenwich.ac.uk
University of Greenwich
London, UK

George Loukas
g.loukas@greenwich.ac.uk
University of Greenwich
London, UK

Konstantinos Kentrotis
k.kentrotis@exus.ai
Exus
Athens, Greece

ABSTRACT

Connected and autonomous vehicles (CAVs) are vulnerable to security gaps that can result in serious consequences, including cyber-physical and privacy risks. For example, an attacker can reconstruct a vehicle's location trajectory by knowing the speed and steering wheel position of the vehicle. Such inferences not only lead to safety issues but also significantly threaten privacy. This paper assesses the privacy impacts of cyber threats on vehicular networks. We augment the Privacy Risk Assessment Methodology (PRAM), proposed by the National Institute of Standards and Technology, with cyber threats, with cyber threats, which are, in practice, mapped to PRAM impact metrics. We demonstrate the practical application of the enhanced PRAM methodology through a use case that highlights attacks leading to privacy risks in CAVs. The consideration of cyber attacks for privacy risk assessment addresses a major gap in current practices, which is to integrate privacy risk into cyber risk management.

CCS CONCEPTS

• **Security and privacy** → **Human and societal aspects of security and privacy**; • **Applied computing** → Enterprise computing; • **General and reference** → **Evaluation**.

KEYWORDS

Privacy risk assessment, Cyber threats, Connected and autonomous vehicles

ACM Reference Format:
Sakshyam Panda, Emmanouil Panaousis, George Loukas, and Konstantinos Kentrotis. 2023. Privacy Impact Assessment of Cyber Attacks on Connected and Autonomous Vehicles. In *The 18th International Conference on Availability, Reliability and Security (ARES 2023), August 29-September 1, 2023, Benevento, Italy*. ACM, New York, NY, USA, 9 pages. https://doi.org/10.1145/3600160.3605073

ARES 2023, August 29-September 1, 2023, Benevento, Italy

ACM ISBN 979-8-4007-0772-8/23/08…$15.00
https://doi.org/10.1145/3600160.3605073

1 INTRODUCTION

Connected and autonomous vehicles (CAVs) have been envisioned to revolutionise the transportation industry by integrating many advanced technologies such as sensors, communication systems and artificial intelligence to create a safer, more efficient and more convenient mode of transportation with the potential to reduce environmental damage. Lately, we are seeing the emergence of connected vehicles with an array of sensors and smart onboard units to assist with cruise control, platooning and parking [36, 38, 52]. Connected vehicles which are permanently connected through various communication technologies to the internet can interact with any entity capable of doing so, such as vehicle-to-pedestrian, vehicle-to-devices, and vehicle-to-grid. With the application of artificial intelligence in conjunction with sophisticated sensors, and improved infrastructures and communication technologies, it is expected that the CAVs market will steadily grow to reach $7 trillion by 2050 [52]. However, the increased connectivity and automation of CAVs have led to a larger threat landscape with growing privacy and security risks, leading to cyber-physical impact. These risks include attacks such as GPS spoofing, replay attacks and injection attacks that could compromise the privacy, safety and security of the passengers and other road users.

Besides security, privacy is a key aspect of CAVs. Privacy ensures that the collected information is only used for the intended purpose and is free from interference or unwanted surveillance. The leakage of information in CAVs is a huge concern that could lead to exposure of location data (home address, workplace etc), passengers' identity data, passengers' medical data (heart rate, medical conditions etc), traffic density, HD maps, or user behaviour data (fatigue, habit) among others [21, 25, 52, 59]. As CAVs become more widespread, it is important for individuals, manufacturers, and policymakers to be aware of these risks and to take steps to mitigate them.

Privacy risk assessment, also known as data protection impact assessment or privacy impact assessment, is a crucial process to identify and evaluate privacy risks [56]. Better management of privacy risks and effective solutions to protect individuals' privacy when designing or deploying systems, products and services can help build customer trust. The process can also help understand and prioritise privacy risks within a broader profile of enterprise risks and drive comprehensive risk management approaches to promote better resource allocation and decision-making. Such approaches can lead to effective cyber risk management practices through protection [10, 47], mitigation [19, 24, 46, 54] as well as support forensic investigations [7, 39] and obtain evidence to take legal actions or support cyber insurance [18, 45, 48] to contain the risks and exposure.

In this paper, we analyse and extend the NIST Privacy Risk Assessment Methodology (PRAM) to perform a privacy impact assessment of attacks on CAVs and identify potential privacy concerns for individuals and the associated enterprise risks. We begin by identifying cyber attacks (threat scenarios) on key components of CAVs that would impact the confidentiality and integrity of data by reviewing existing literature. Besides attacks affecting the confidentiality of data, we have also selected attacks that affect the integrity of data. Integrity prevents unauthorised modification of data and guarantees that all data are accurate, reliable, verifiable and consistent. Firstly, failure to assure integrity can lead to severe safety issues as the data and depending services can no longer be trusted. Maliciously manipulated data could lead to adverse decisions and potentially life-threatening situations. Secondly, if an attacker tampers with CAV's data, it can lead to sensitive personal information being disclosed without the individual's consent. For example, the attacker could access biometric data such as facial recognition or voice prints to identify the individual or manipulate the data to create false information that could be used in a discriminatory way.

We then analyse (i) the potential impact of the threat scenario on the NIST Privacy Engineering Objectives, namely Predictability, Manageability and Disassociability; and (ii) the effect of PRAM problematic data actions on these objectives. These mappings aid in identifying problematic data actions for a threat scenario and the privacy concerns for individuals that the threat scenario could lead to. Finally, we calculate the enterprise risk for a threat and problematic data action pair leading to privacy concerns for an individual.

The remainder of the paper is structured as follows. Section 2 discusses relevant work and positions our contribution. Section 3 presents the attacks on CAVs and possible privacy impacts. Next, Section 4 lays out the use case scenario under investigation and the privacy impact assessment leading to risk scores. Finally, Section 5 concludes the paper.

2 RELATED WORK

Privacy risk analysis methods are essential for minimising or avoiding privacy breaches. It aims to identify events leading to a risk of harm to the fundamental rights of data subjects for any data collection and processing activity and assess appropriate measures to properly manage the risks. However, quantifying risk is a challenging task and many approaches have resorted to estimating the risk based on more tangible factors such as the estimated likelihood of a feared event and projected impact. Methods have been developed to measure privacy risk based on the number of records stored in the system [22], system architecture [5, 30], organisational characteristics [34] or based on privacy risk assessment frameworks and guidelines [13].

To protect privacy, various regulations have been put-forth such as the European General Data Protection Act (GDPR) [56], the California Consumer Privacy Act (CCPA) [3], the UK Data Protection Act [4], the Privacy Rule of the Health Insurance Portability and Accountability Act (HIPAA) [40] among others. In the meanwhile, several guidelines and frameworks have been proposed to assess privacy impact and protect data privacy. The NIST PRAM [41] applies the NISTIR 8062 [11] risk model to identify and prioritise privacy risks. While NIST FAIR Privacy [15] incorporates the principles of FAIR [20] into privacy management practices enabling organisations to achieve a balance between data access and privacy protection. The FAIR approach has also been extended by Sion et al. [50] for privacy threat modelling. From a threat modelling perspective, LINDDUN framework [58] assesses seven privacy threats which are Linkability, Identifiability, Non-repudiation, Detectability, Disclosure of information, Unawareness and Non-compliance. Other privacy impact assessment frameworks include CNIL PIA [1], ISO/IEC 29134:2017 [2] and ICO DPIA [42]. Bisztray and Gruschka [9] present a questionnaire-based evaluation of LINDUNN, CNIL PIA and ISO/IEC 29134:2017. Alongside these frameworks, Tang et al. [53] presents a list of existing mechanisms and approaches offering privacy risk analysis. Table 1 presents an overview of existing privacy impact assessment approaches highlighting their general characteristics such as skills required to implement them, whether the analysis method is quantitative or qualitative, the kind of risk assessment method employed and whether they propose controls to manage the privacy risks, to assist practitioners in choosing the right assessment approach based on available skills and business objectives.

3 ATTACKS ON CAVS AND PRIVACY IMPACTS

Advanced autonomous driving has the potential to revolutionise transportation in urban areas. Autonomous driving which relies on advanced sensors and algorithms to navigate vehicles without human intervention, can enhance safety and efficiency by eliminating the need for human drivers altogether. This form of driving allows human operators to control vehicles from a remote location improving safety and efficiency while reducing the risk of human errors. It also enables faster response times to unexpected events.

Connected and autonomous driving can enable a wide range of innovative transportation services in urban areas, such as on-demand mobility, last-mile delivery, and public transportation. For example, autonomous shuttles and buses can provide safe and efficient transportation for commuters, whereas autonomous delivery vehicles can improve the speed and efficiency of last-mile logistics. This paper builds upon one of the use cases for the use of autonomous vehicles for transportation.

3.1 Vehicular Data, Attacks and Privacy Impacts

CAVs continuously collect data from the surrounding environment, road facilities and passengers to enhance user experience and road safety. The collected data is used to perceive objects in the surrounding (e.g., pedestrians, vehicles) and traffic rules (e.g., road edges, speed limit, traffic signals), and to plan driving trajectory and motion control of the vehicle. The collected data usually carries personal and potentially sensitive information such as location data, passengers' identity data, passengers' medical data (heart rate, medical conditions etc), traffic density, HD maps, or user behaviour data (fatigue, habit) among others [21, 59]. In general, the data collected are necessary for vehicular systems to improve performance,

	Template/ Framework	Skills required	Severity of harm	Analysis method	Risk assessment method	Controls recommended
CNIL PIA [1]	1/0	Low	✓	Qualitative	control-based	×
NIST PRAM [41]	0/1	High	×	Qualitative	control-based	×
ICO DPIA [42]	1/0	Low	✓	Qualitative	control-based	✓
NIST FAIR [15]	0/1	High	✓	Quantitative	threat-based	×
LINDDUN [58]	0/1	High	×	Qualitative	threat-based	×

Table 1: Comparison of privacy impact assessment approaches

personalise services, intelligent recommendations, and enhance traffic flow and safety.

However, attacks on these systems can affect the overall services and operations of CAVs and may lead to significant cyber-physical risks as well as privacy risks. For example, Gazdag et al. [21] were able to re-identify a driver from the raw, unprocessed CAN data with 97% accuracy and reconstruct the vehicle's complete location trajectory knowing only its speed and steering wheel position. Unauthorised access to vehicular data can impact privacy at an individual level (information leakage about individuals), population level (information leakage leading to inferences on the behaviour or characteristics of a group) and/or proprietary level (information leakage on proprietary usage of CAVs) [59]. Below, we list out various types of cyber attacks on vehicular networks that could breach the confidentiality and integrity of data leading to potential privacy leakage.

3.1.1 Attacks on CAVs Affecting Data Integrity: Integrity ensures that the content of a message or signal is not tampered with during transmission, thus preventing unauthorised creation, modification and deletion of data. This category only considers integrity attacks with the potential to manipulate the data.

Illusion Attack: An illusion attack involves altering the data from sensors or RSU that creates a false or deceptive perception of the vehicle's surroundings or behaviour. For example, an attacker could use a false traffic sign or road marking to deceive other vehicles causing it to take an unintended route or behaviour leading to an action that undermines the integrity of the vehicle's systems or data [31].

Injection Attack: An injection attack involves the insertion of malicious code or software to manipulate or steal data. For example, attackers can gain entry to the in-vehicle network through OBD-II ports, compromised ECUs or infotainment and telematics systems [29, 35]. Injection attacks could also potentially breach the confidentiality of CAV data.

3.1.2 Attacks on CAVs Affecting Data Confidentiality: Confidentiality guarantees that only the authorised entity is able to access the data.

Eavesdropping Attack: An eavesdropping attack involves unauthorised access to vehicular messages. For example, the attacker gains access to FlexRay protocol and interprets communications [23] and identifies patterns in legitimate CAN frames [29].

Man-in-the-middle Attack: A man-in-the-middle attack involves interception and manipulation of information. For example, an attacker could pose as a legitimate vehicle, such as the owner or a trusted third party, to eavesdrop, modify sensor readings, steal personal information and inject false information [17, 29].

GPS Trailing Attack: A GPS trailing attack involves monitoring and intercepting GPS data to track a vehicle. For example, a GPS trailing attack could be used to trace the trajectory of the vehicle and obtain private information through tracking the vehicle [12, 27].

Timing Attack: In a timing attack, a malicious vehicle receiving time-critical updates and traffic information do not forward the message to other vehicles at the right time, instead it analyses the information and adds extra delay in transmission. A timing attack could potentially lead to a breach of confidentiality if sensitive information could be extracted from analysing the messages. For example, an attacker listens to the message transmission and then analyses its frequency and duration to gather the response pattern of the vehicle [8].

Note that this list does not cover every attack on vehicular networks, but rather provides a subset of attacks that affect confidentiality and/or integrity resulting in a direct privacy breach. Practitioners should consider all attacks (including attacks that affect availability) that could potentially impact privacy. For example, a Denial of Service (DoS) attack on a CAV might disrupt the vehicle's communication leading to a breakdown in the privacy protections that are provided by the system. Carsten et al. [12] demonstrate a DoS attack where the attacker repeatedly sends high-priority messages to block other messages and take control of the vehicle. However, DoS attacks are usually performed as a decoy attack to divert attention, making it easier to launch a separate attack to gain access to the vehicle's data or control systems. Since attacks that affect the availability of data do not necessarily have a direct impact on privacy, these attacks are excluded from the analysis.

4 USE CASE AND PRIVACY IMPACT ASSESSMENT

A service provider offers self-driving taxi services in a facility through a smartphone application (let's call it CAVRide). CAVRide allows users to book a ride by specifying a pickup location, time and destination. It also allows users to track the self-driving taxi in real time while providing accurate navigation and directions which include traffic updates and alternative routes. The self-driving taxis

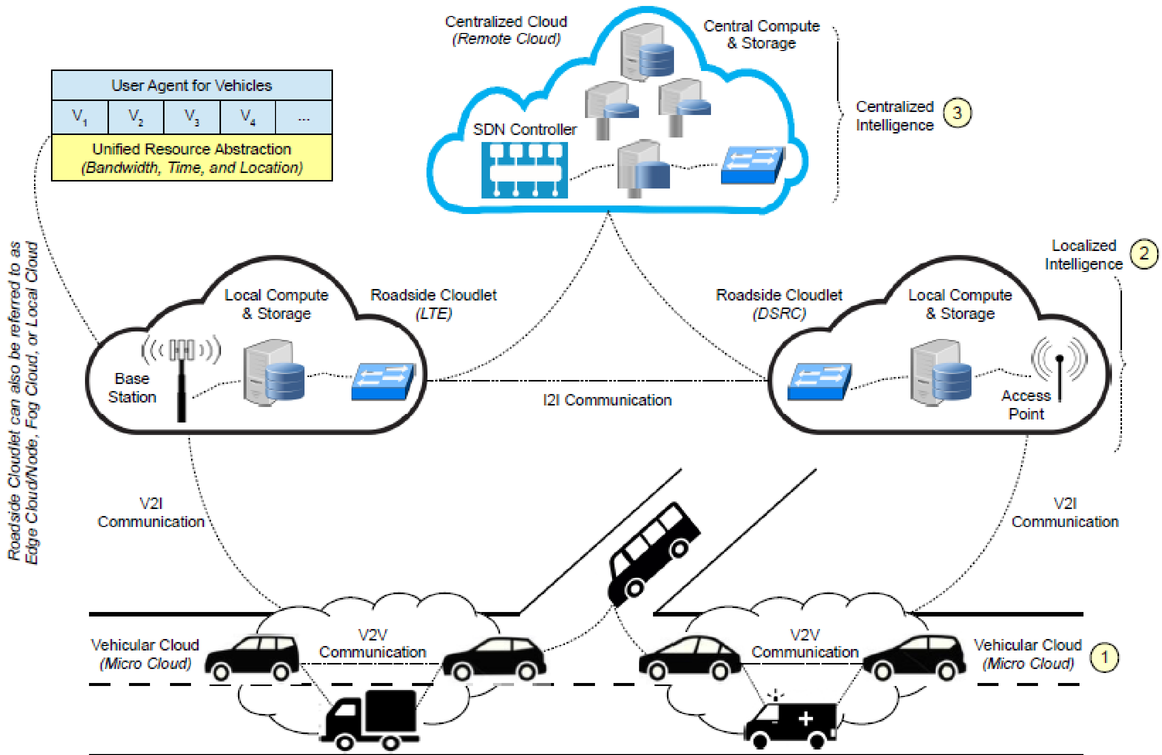

Figure 1: A topological architecture of vehicular network [33].

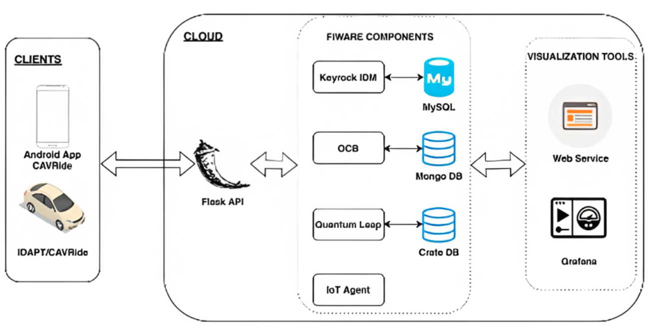

Figure 2: An example architecture of CAVRide for HE TANGO[1] use case

on the other hand, continuously update their location and availability status on the cloud server that is accessed by CAVRide. A user requests a pickup service using CAVRide on their smartphone. The user request is evaluated (for authenticity) based on predefined logic on the cloud server and on success is forwarded to the available self-driving taxi. Once the taxi receives and acknowledges the request, the server transmits information about the taxi to the user. The user through the CAVRide can access the taxi's current location, speed, estimated arrival time and other telemetries. Authentication, acknowledgement and interactions between the user, taxi and server continue till the user reaches the destination. In addition, the data gathered through the sensors on the taxi is processed and uploaded to the server by the onboard unit to enhance services. Figure 1 presents an overview of the topology and communication between the endpoints of the CAV network. Figure 2, on the other hand, presents the topology architecture of CAVRide and the cloud server (marked as Centralised Intelligence in Fig. 1).

Considering the detailed scenario, let us begin by applying the NIST PRAM to assess privacy risk for the CAV use case. In general, NIST PRAM is a high-level framework to identify privacy risks and develop mitigation to counteract possible impacts from the risks. The methodology is a cycle of iterative steps that includes framing business objectives and an organisational privacy governance plan, assessing privacy risks based on system design, selecting privacy controls and monitoring change. NIST PRAM consists of four key steps. **Step 1** focuses on identifying business objectives and organisational privacy governance requirements. **Step 2** focuses on defining privacy risks and contextual factors that lead to problematic data actions. **Step 3** supports the assessment and prioritisation of privacy risks based on the likelihood and risk estimates for the identified problematic data actions. Finally, **Step 4** deals with identifying controls and considerations to address the privacy risks.

[1]HE TANGO Project: https://cordis.europa.eu/project/id/101070052

4.1 Step 1:

The first step looks into framing business objectives and defining the privacy goals. For the use case scenario, the objective is to provide seamless service to users based on varieties of telemetries collected during the journey while ensuring user privacy. The overall privacy goal is to ensure that the NIST Privacy Engineering Objectives [11], which are Predictability, Manageability and Disassociability, are met to reduce privacy risks and protect privacy at scale. NIST IR 8062 defines *Predictability* as the ability that enables reliable assumptions about individuals, owners, and operators based on the processing of personal information; *Manageability* as the ability that enables granular administration of personal information including alteration, deletion, and selective disclosure; and *Disassociability* is enabling the processing of personal information or events without associating them to individuals or devices beyond the operational requirements.

4.2 Step 2:

Next, we identify and catalogue inputs required to perform the privacy risk analysis. We begin by identifying data flows, processes, data stores, entities and endpoints that help with mapping data flows and generating a Data Flow Diagram (DFD) of the system. Table 2 highlights key DFD element types and the components that fall under each type for the use case. Identification of key element types defines the scope of the privacy assessment while applying NIST PRAM.

Once the DFD elements are identified, we then analyse each data flow to identify the personal data it uses and summarise potential threat scenarios. Note that we consider a data flow uses some form of sensitive data which if breached would impact privacy. Practitioners might choose to consider the data types and additional factors such as duration or frequency of each data activity, degree of sensitivity of data and relation between system and operation purposes with respect to data. Table 3 presents attack scenarios against critical elements for a few selected data flows of the use case.

The attack scenarios against critical elements in each data flow have been identified by reviewing existing literature. **Considering cyber attacks for privacy risk assessment addresses a major gap in current practices which is to integrate privacy risk assessment with cyber risk management.** Viewing cyber threats from a privacy lens can help organisations understand and prioritise risks promoting better resource allocation and decision-making. Next, we identify the potential repercussions of each attack scenario on the three NIST Privacy Engineering Objectives. For example, let us consider the attack scenario **T2** which expresses the "exploitation of CAN vulnerability that allows an attacker to present as a legitimate node". Such an impersonation attack, belonging to the man-in-the-middle attack class, would allow the attacker to intercept, manipulate and transmit information to mislead other recipients. Through this attack, the attacker can preclude reliable assumptions regarding the participants (affecting predictability), have granular administration of the data (affecting manageability) and can confidently associate information regarding the participants (affecting dissociability). Similarly, attack scenario "**T8**: attacker identifies the response pattern by analysing the timing of the vehicle's response", a timing attack, would allow the attacker to make reliable prediction about a participant. Thus affecting only the predictability metric (see the last row of Table 3).

4.3 Step 3:

This step provides the structure for the analysis and risk assessment. Before proceeding with the risk assessment which is to determine the frequency of loss event and the loss magnitude, we must determine the potential harm as a result of a cyber attack. This is achieved by mapping (see Table 4 and Table 5) the NIST Privacy Engineering Objectives to NIST Problematic Data Actions and potential harm from each problematic data action. NIST PRAM identifies nine problematic data actions which include: (i) *Appropriation* (**AP**) includes scenarios in which data is used in ways that exceed individual's expectation or authorisation; (ii) *Distortion* (**DI**) refers to the use or dissemination of inaccurate or misleading data; (iii) *Induced Disclosure* (**ID**) refers to scenarios in which individuals feel compelled to provide information disproportionate to the purpose or outcome of the transaction. Induced disclosure can include leveraging access or rights to an essential (or perceived essential) service; (iv) *Data Insecurity* (**IN**) resulting in a breach of confidentiality and integrity of personal data; (v) *Re-identification* (**RE**) refers to scenarios where data from multiple sources can be associated or identified to a specific individual; (vi) *Stigmatisation* (**ST**) refers to the scenario in which data is linked to an actual identity in such a way as to create a stigma; (vii) *Surveillance* (**SU**) refers to scenarios in which data, devices and individuals are tracked or monitored in a manner disproportionate to the purpose leading to an adverse situation for individuals or groups; (viii) *Unanticipated Revelation* (**UR**) refers to situations in which data in revealed or exposed in unexpected ways; (ix) *Unwarranted Restriction* (**WR**) includes not only blocking access to data or services. but also limiting awareness of the existence of data or its use in ways that are disproportionate to operational purposes.

Mapping NIST Privacy Engineering Objectives to Problematic Data Actions: Problematic data actions such as appropriation (AP) in the context of privacy refers to the unauthorised use of an individual's data for purpose other than those for which the data was originally collected. Unauthorised use of data can allow the attacker to have reliable assumptions about the entity as well as associate events and actions to an entity. Appropriation, thus, can affect predictability and disassociability. Unanticipated revelation (UR) in the context of privacy refers to the unexpected disclosure or exposure of information that was not meant to be shared. The unexpected revelation of information can allow the attacker to have reliable assumptions about the entity's behaviour or characteristics as well as can associate actions with an entity affecting predictability and dissociability. On the other hand, distortion (DI) which refers to the manipulation or modification of information will affect the manageability metric. A similar assessment is performed for all the rest of the problematic data actions and the mapping is presented in Table 4.

A problematic data action can lead to harm. While harm is most often associated with physical or mental injury, it can also be referred to as moral injury or wrongfulness. Daniel Solove's [51]

DFD Element Type	Units
End Points	Electronic Control Units (ECU), Controller Area Network (CAN), Local Interconnect Network (LIN), GPS, Central computer, Video Camera, Bluetooth, Radio, Network infrastructure, Mobile phones, cloud etc
External Entity	Passengers, Owners, Pedestrians, Service providers
Processing Units	CAV central computer unit, Service provider, Network provider, Mobile phones
Data Flow	In-vehicle (i.e OBD II port and CAV central computer), vehicle-to-infrastructure (i.e sending GPS to server through network provider), vehicle-to-user (i.e sharing current location and estimated time of arrival to the user), vehicle-to-vehicle (i.e sharing current trajectory)
Data Store	CAV database, Service provider database, mobile phone database, network provider database

Table 2: DFD Element Types and CAV Components

Data Flow	Critical Elements	Attack Scenario	NIST Privacy Engineering Objectives		
			Predictability	Manageability	Disassociability
In-vehicle	OBD II port, CAN	T1. Replacing an unauthorised ECU programme with an illegitimate, malicious programme and connecting the CAN bus with an unauthorised device [55].	×	✓	✓
		T2. Exploiting CAN vulnerability that allows attacker to present as a legitimate node [14, 29].	✓	✓	✓
		T3. Attacker gains access to CAN's broadcasting transmission allowing to eavesdrop on CAN transmissions [29].	✓	×	✓
	OBD II port, FlexRay	T4. Attacker gains access to FlexRay protocol and interprets communication [23].	✓	×	✓
		T5. Attacker interprets FlexRay communication and injects messages [37].	×	✓	✓
V2I	GPS	T6. Attacker obtains users' private information through locating and tracking their vehicles [27]	✓	×	✓
V2V	Vehicle	T7. Influence other vehicles' behaviour by disseminating false information [31, 52].	✓	✓	×
		T8. Attacker identifies the response pattern by analysing the timing of the vehicle's response [8].	✓	×	×

Table 3: Data flows with attack scenarios for CAVs

NIST Privacy Engineering Objectives	Problematic Data Actions								
	AP	DI	ID	IN	RE	ST	SU	UR	WR
Predictability	✓	×	✓	✓	×	✓	✓	✓	×
Manageability	×	✓	×	✓	×	×	✓	×	×
Disassociability	✓	×	✓	✓	✓	✓	✓	✓	✓

Table 4: Mapping NIST Privacy Engineering Objectives and NIST Problematic Data Actions.

Taxonomy of Privacy harms provides an elaborate and granular list of social norms that could be considered as harms resulting from privacy breaches. NIST PRAM defines seven categories of potential problems that the at-risk individual or group could experience as the result of a loss event. These are: (i) *Dignity Loss* that includes embarrassment and emotional distress; (ii) *Discrimination* that covers unfair or unethical differential treatment of individuals or at-risk

Problems for Individuals	Problematic Data Actions								
	AP	DI	ID	IN	RE	ST	SU	UR	WR
Dignity Loss	×	✓	×	✓	✓	✓	×	✓	×
Discrimination	×	✓	✓	×	✓	✓	✓	✓	×
Economic Loss	✓	×	×	✓	×	×	×	×	✓
Loss of Autonomy	✓	×	✓	×	×	×	✓	✓	✓
Loss of Liberty	×	✓	×	×	×	×	✓	×	✓
Physical Harm	×	×	×	✓	×	×	✓	×	✓
Loss of Trust	✓	×	✓	✓	✓	×	✓	✓	✓

Table 5: Mapping problems for individual (harm) to NIST Problematic Data Actions

groups arising from the processing of data; (iii) *Economic Loss* that includes direct financial losses as the result of identity theft or the failure to receive fair value in a transaction; (iv) *Loss of Autonomy* that includes losing control over determinations about information processing or interactions with systems, products or services, as well as needless changes in ordinary behaviour, including self-imposed restrictions on expression or civic engagement; (v) *Loss of Liberty* that covers impacts from incomplete or inaccurate data which can lead to improper exposure to arrest or detainment and/or improper exposure or use of information to abuse governmental power; (vi) *Physical Harm*; and (vii) *Loss of Trust* that includes the breach of implicit or explicit expectations or agreements about the processing of data which could lead to diminishing morale or leave individuals reluctant to engage in future transactions potentially creating larger economic or civic consequences. Table 5 presents a mapping between problematic data actions and potential problems which are achieved from NISTIR 8062 [11]. This mapping enables us to establish a relation between attack scenarios and potential problems (i.e. attack scenario → NIST privacy objective principles → problematic data action → potential problems).

Once the problematic data actions and respective problems for individuals for an attack scenario are identified, the next step is to determine the likelihood and loss impact. This paper considers the likelihood and loss magnitude (including different categories) as random variables. Practitioners might consider a database of previous incidents (if available) or Monte Carlo simulations to generate the likelihood of impact. Note that identifying the probabilities and impact values is beyond the scope of this paper and will be considered in future work. The final output of Step 3 is a risk score for each <**threat scenario, problematic data action, problems for individual**> tuple. Table 6 presents the privacy impact assessment for attack scenario T1. The Likelihood of Impact (*FI*) represents the probability of a successful event leading to the violation of privacy and causing specific harm to the individual or group. Loss Magnitude (*L*) expresses the potential business impact from an adverse event. It is composed of five categories of impact factors: (i) Non-compliance Cost; (ii) Direct Business Cost; (iii) Reputation Cost; (iv) Internal Culture Cost; and (v) Other Associated Costs. These factors capture the impact on a business due to an event leading to harm.

The loss magnitude can be obtained by adding the factors altogether.

$$L = \sum \Big\{ \text{Non-compliance Cost, Direct Business Cost, Reputation Cost, Internal Culture Cost, Other Associated Cost} \Big\} \tag{1}$$

The Risk (i.e., last column) presents the privacy risk which is the likelihood of impact (*FI*) times loss magnitude (*L*). Mathematically, we define risk as the inner product of these two factors.

$$\begin{aligned} \textbf{Risk} &= \langle FI \cdot L \rangle \\ &= [FI_1 \times L_1, FI_2 \times L_2, \ldots, FI_r \times L_r] \end{aligned} \tag{2}$$

The risk quantification process can be found in Algorithm 1.

Note that for better readability of the paper and due to limited space, Table 6 only include the assessment for attack scenario T1.

Algorithm 1 Privacy Risk Quantification

procedure PrivacyRiskQuantification
  for each df in DataFlow **do**
    for each ts in ThreatScenario **do**
      for each pi in ProblemForIndividual **do**
        Risk(ts) = $\sum_{pi} FI_{pi} \times L_{pi}$
      end for
    end for
    Risk(df) = $\sum_{ts}$ Risk(ts)
  end for
end procedure

Practitioners must analyse every identified attack scenario using a detailed approach. One possible direction would be to consider the frequency of loss event (*FE*) along with the likelihood of impact (*FI*). The frequency of loss event (*FE*) represents the frequency of an adverse event that could potentially impact the privacy of an at-risk individual or group. In simpler terms, it represents how often an event occurs over a period (e.g., annually) that has the potential to breach user privacy. These events could be the result of threat actors exploiting vulnerabilities or gaps in the systems, and/or inappropriate data handling practices within an organisation. In practice, this could include alerts or logs of potential security breaches or suspicious activities detected on a system or network. In such as case, the risk could be expressed as:

$$\begin{aligned} \textbf{Risk} &= \langle FE \cdot FI \cdot L \rangle \\ &= [FE_1 \times FI_1 \times L_1, FE_2 \times FI_2 \times L_2, \ldots, FE_r \times FI_r \times L_r] \end{aligned} \tag{3}$$

4.3.1 Step 4: The final step involves prioritisation of privacy risks and identification of controls to address the privacy risks. For example, attacks against CAN bus vulnerabilities (Attack Scenario T2) can be mitigated using network segmentation, encryption and authentication mechanisms [44]. Intrusion detection methods to analyse arbitration identity sequence [16] and specification-based supervised learning on CAN timing [43] could also be used as defensive measures. To prevent location trailing attacks (Attack Scenario T6), methods such as k-anonymity [49], software defined networks, and location perturbation [26] could be used to protect location privacy in vehicular networks. Methods such as anonymisation [6], resource management [57] and trust-based recommendations [28] could be used to prevent eavesdropping attacks (Attack Scenario T3 and T4). Alongside possible defences against cyber attacks on CAV [32, 36, 52], appropriate data protection measures and PETs must be considered to protect privacy. Once the measures have been identified, cyber security investment approaches such as [19, 46] could be used to determine the cost-effective set of measures that optimally reduce the risks.

5 CONCLUSION

The primary contribution of this paper is to enable privacy risk assessment using the NIST Privacy Risk Assessment Methodology (PRAM). In this work, we have extended PRAM and demonstrated its applicability on connected and autonomous vehicle networks. Through the introduction of cyber threats to PRAM, we show how threat categories can lead to privacy harm and consequently to

Data Flow	Critical Elements	Attack Scenario (see Table 3)	Problematic Data Actions	Problems for Individual (see Table 5)	Likelihood of Impact (FI)	Loss Magnitude (L)					Risk ($FI \times L$)
						Non-compliance cost	Direct business cost	Reputation cost	Internal culture cost	Other cost	
In-vehicle	OBD II port, CAN	T1	AP	Economic loss	4	7	6	7	3		92
				Loss of Autonomy	3	7	7	8	5		81
				Loss of Trust	8	7	4	5	3		152
			DI	Dignity Loss	5	7	4	4	3		90
				Discrimination	6	7	7	8	3		150
				Loss of Liberty	5	7	7	5	8		135
			ID	Discrimination	7	7	4	4	3	2	140
				Loss of Autonomy	4	7	5	7	3		96
				Loss of Trust	5	7	8	8	4		135
			IN	Dignity Loss	4	7	7	8	5	1	112
				Economic Loss	9	7	2	4	7		180
				Physical Harm	6	7	5	2	2		96
				Loss of Trust	4	7	8	3	2		80
			RE	Dignity Loss	8	7	6	3	5		168
				Discrimination	3	7	4	4	5		60
				Loss of Trust	6	7	5	7	2		126
			ST	Dignity Loss	7	7	2	6	4	2	147
				Discrimination	5	7	5	4	3		95
			SU	Discrimination	5	7	4	6	5		110
				Loss of Autonomy	8	7	2	8	8		200
				Loss of Liberty	2	7	7	3	3		40
				Physical Harm	4	7	4	2	5		72
				Loss of Trust	5	7	3	7	7	5	145
			UR	Dignity Loss	4	7	6	2	4		76
				Discrimination	2	7	2	5	2		32
				Loss of Autonomy	5	7	3	6	4		100
				Loss of Trust	8	7	5	4	6		176
			WR	Economic Loss	5	7	8	2	6		115
				Loss of Autonomy	2	7	6	3	8	4	56
				Loss of Liberty	6	7	6	3	4	3	138
				Physical Harm	4	7	4	5	6		88
				Loss of Trust	5	7	2	6	2		85
										Attack Scenario T1 Total Risk	3569

Table 6: Privacy Impact Assessment for Attack Scenario T1

enterprise risk. The consideration of cyber threats for privacy risk assessment can lead to robust and comprehensive threat analysis supporting improved prioritisation of risks and determining effective countermeasures. For future work, we will support the methodology with cyber threat intelligence, common vulnerabilities and business impact (from reports) to quantify the privacy risks and support security investment decisions.

ACKNOWLEDGMENTS

This work was supported by European Union's HE TANGO project under the grant agreement number 101070052.

REFERENCES

[1] [n. d.]. CNIL PIA (Privacy Impact Assessment). https://www.cnil.fr/en/privacy-impact-assessment-pia. Accessed: March 25, 2023.

[2] 2017. ISO/IEC 29134:2017 Information technology – Security techniques – Guidelines for privacy impact assessment. https://www.iso.org/standard/66390.html. Accessed: March 25, 2023.

[3] 2018. California Consumer Privacy Act. https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375 California Assembly Bill No. 375, Accessed: March 25, 2023.

[4] 2018. Data Protection Act. https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted. Accessed: March 25, 2023.

[5] Amir Shayan Ahmadian, Daniel Strüber, Volker Riediger, and Jan Jürjens. 2018. Supporting privacy impact assessment by model-based privacy analysis. In *Proceedings of the 33rd Annual ACM Symposium on Applied Computing*. 1467–1474.

[6] Muhammad Arif, Guojun Wang, and Valentina Emilia Balas. 2018. Secure VANETs: trusted communication scheme between vehicles and infrastructure based on fog computing. *Stud. Inform. Control* 27, 2 (2018), 235–246.

[7] Soodeh Atefi, Sakshyam Panda, Manos Panaousis, and Aron Laszka. 2022. Principled data-driven decision support for cyber-forensic investigations. *arXiv preprint arXiv:2211.13345* (2022).

[8] Maria Azees, Pandi Vijayakumar, and Lazarus Jegatha Deborah. 2016. Comprehensive survey on security services in vehicular ad-hoc networks. *IET Intelligent Transport Systems* 10, 6 (2016), 379–388.

[9] Tamas Bisztray and Nils Gruschka. 2019. Privacy impact assessment: comparing methodologies with a focus on practicality. In *Secure IT Systems: 24th Nordic Conference, NordSec 2019, Aalborg, Denmark, November 18–20, 2019, Proceedings 24*. Springer, 3–19.

[10] Nadia Boumkheld, Sakshyam Panda, Stefan Rass, and Emmanouil Panaousis. 2019. Honeypot type selection games for smart grid networks. In *Decision and Game Theory for Security: 10th International Conference, GameSec 2019, Stockholm, Sweden, October 30–November 1, 2019, Proceedings 10*. Springer, 85–96.

[11] Sean Brooks, Michael Garcia, Naomi Lefkovitz, Suzanne Lightman, and Ellen Nadeau. 2017. *An introduction to privacy engineering and risk management in federal systems.* Technical Report Tech. Rep. NIST IR 8062, Jan. 2017. National Institute of Standards and Technology, Washington, D.C. https://doi.org/10.6028/NIST.IR.8062

[12] Paul Carsten, Todd R Andel, Mark Yampolskiy, and Jeffrey T McDonald. 2015. In-vehicle networks: Attacks, vulnerabilities, and proposed solutions. In *Proceedings of the 10th Annual Cyber and Information Security Research Conference*. 1–8.

[13] Badreddine Chah, Alexandre Lombard, Anis Bkakria, Reda Yaich, Abdeljalil Abbas-Turki, and Stéphane Galland. 2022. Privacy Threat Analysis for connected and autonomous vehicles. *Procedia Computer Science* 210 (2022), 36–44.
[14] Wonsuk Choi, Kyungho Joo, Hyo Jin Jo, Moon Chan Park, and Dong Hoon Lee. 2018. Voltageids: Low-level communication characteristics for automotive intrusion detection system. *IEEE Transactions on Information Forensics and Security* 13, 8 (2018), 2114–2129.
[15] R Jason Cronk and Stuart S Shapiro. 2021. Quantitative Privacy Risk Analysis. In *2021 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*. IEEE, 340–350.
[16] Araya Kibrom Desta, Shuji Ohira, Ismail Arai, and Kazutoshi Fujikawa. 2020. ID sequence analysis for intrusion detection in the CAN bus using long short term memory networks. In *2020 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*. IEEE, 1–6.
[17] Zeinab El-Rewini, Karthikeyan Sadatsharan, Daisy Flora Selvaraj, Siby Jose Plathottam, and Prakash Ranganathan. 2020. Cybersecurity challenges in vehicular communications. *Vehicular Communications* 23 (2020), 100214.
[18] Aristeidis Farao, Sakshyam Panda, Sofia Anna Menesidou, Entso Veliou, Nikolaos Episkopos, George Kalatzantonakis, Farnaz Mohammadi, Nikolaos Georgopoulos, Michael Sirivianos, Nikos Salamanos, et al. 2020. SECONDO: A platform for cybersecurity investments and cyber insurance decisions. In *Trust, Privacy and Security in Digital Business: 17th International Conference, TrustBus 2020, Bratislava, Slovakia, September 14–17, 2020, Proceedings 17*. Springer, 65–74.
[19] Andrew Fielder, Emmanouil Panaousis, Pasquale Malacaria, Chris Hankin, and Fabrizio Smeraldi. 2016. Decision support approaches for cyber security investment. *Decision support systems* 86 (2016), 13–23.
[20] Jack Freund and Jack Jones. 2014. *Measuring and managing information risk: a FAIR approach*. Butterworth-Heinemann.
[21] András Gazdag, Szilvia Lestyán, Mina Remeli, Gergely Ács, Tamás Holczer, and Gergely Biczók. 2023. Privacy pitfalls of releasing in-vehicle network data. *Vehicular Communications* 39 (2023), 100565.
[22] Anthony J Grosso, Gregory W Leffard, and Jeremiah G O'dwyer. 2014. System and method for analyzing privacy breach risk data. US Patent App. 13/683,422.
[23] Zonghua Gu, Gang Han, Haibo Zeng, and Qingling Zhao. 2016. Security-aware mapping and scheduling with hardware co-processors for flexray-based distributed embedded systems. *IEEE Transactions on parallel and distributed systems* 27, 10 (2016), 3044–3057.
[24] Ioannis Kalderemidis, Aristeidis Farao, Panagiotis Bountakas, Sakshyam Panda, and Christos Xenakis. 2022. GTM: Game Theoretic Methodology for optimal cybersecurity defending strategies and investments. In *Proceedings of the 17th International Conference on Availability, Reliability and Security*. 1–9.
[25] Stamatis Karnouskos and Florian Kerschbaum. 2017. Privacy and integrity considerations in hyperconnected autonomous vehicles. *Proc. IEEE* 106, 1 (2017), 160–170.
[26] Xinghua Li, Yanbing Ren, Laurence T Yang, Ning Zhang, Bin Luo, Jian Weng, and Ximeng Liu. 2020. Perturbation-hidden: Enhancement of vehicular privacy for location-based services in internet of vehicles. *IEEE Transactions on Network Science and Engineering* 8, 3 (2020), 2073–2086.
[27] Zi Li, Qingqi Pei, Ian Markwood, Yao Liu, Miao Pan, and Hongning Li. 2018. Location privacy violation via GPS-agnostic smart phone car tracking. *IEEE Transactions on Vehicular Technology* 67, 6 (2018), 5042–5053.
[28] Wei Liang, Jing Long, Tien-Hsiung Weng, Xuhui Chen, Kuan-Ching Li, and Albert Y Zomaya. 2019. TBRS: A trust based recommendation scheme for vehicular CPS network. *Future Generation Computer Systems* 92 (2019), 383–398.
[29] Jiajia Liu, Shubin Zhang, Wen Sun, and Yongpeng Shi. 2017. In-vehicle network attacks and countermeasures: Challenges and future directions. *IEEE Network* 31, 5 (2017), 50–58.
[30] Kun Liu and Evimaria Terzi. 2010. A framework for computing the privacy scores of users in online social networks. *ACM Transactions on Knowledge Discovery from Data (TKDD)* 5, 1 (2010), 1–30.
[31] Nai-Wei Lo and Hsiao-Chien Tsai. 2007. Illusion attack on vanet applications-a message plausibility problem. In *2007 IEEE Globecom Workshops*. IEEE, 1–8.
[32] Zhaojun Lu, Gang Qu, and Zhenglin Liu. 2018. A survey on recent advances in vehicular network security, trust, and privacy. *IEEE Transactions on Intelligent Transportation Systems* 20, 2 (2018), 760–776.
[33] Adnan Mahmood, Wei Emma Zhang, and Quan Z Sheng. 2019. Software-defined heterogeneous vehicular networking: The architectural design and open challenges. *Future Internet* 11, 3 (2019), 70.
[34] Eleni-Laskarina Makri, Zafeiroula Georgiopoulou, and Costas Lambrinoudakis. 2020. A proposed privacy impact assessment method using metrics based on organizational characteristics. In *Computer Security: ESORICS 2019 International Workshops, CyberICPS, SECPRE, SPOSE, and ADIoT, Luxembourg City, Luxembourg, September 26–27, 2019 Revised Selected Papers 5*. Springer, 122–139.
[35] Sahar Mazloom, Mohammad Rezaeirad, Aaron Hunter, and Damon McCoy. 2016. A Security Analysis of an In-Vehicle Infotainment and App Platform.. In *WOOT*.
[36] Yassine Mekdad, Ahmet Aris, Leonardo Babun, Abdeslam El Fergougui, Mauro Conti, Riccardo Lazzeretti, and A Selcuk Uluagac. 2023. A survey on security and privacy issues of UAVs. *Computer Networks* (2023), 109626.
[37] Ahmed Refaat Mousa, Pakinam NourElDeen, Marianne Azer, and Mahmoud Allam. 2016. Lightweight authentication protocol deployment over FlexRay. In *Proceedings of the 10th International Conference on Informatics and Systems*. 233–239.
[38] Jianbing Ni, Kuan Zhang, Yong Yu, Xiaodong Lin, and Xuemin Shen. 2018. Privacy-preserving smart parking navigation supporting efficient driving guidance retrieval. *IEEE Transactions on Vehicular Technology* 67, 7 (2018), 6504–6517.
[39] Antonia Nisioti, George Loukas, Aron Laszka, and Emmanouil Panaousis. 2021. Data-driven decision support for optimizing cyber forensic investigations. *IEEE Transactions on Information Forensics and Security* 16 (2021), 2397–2412.
[40] U.S. Department of Health & Human Services. 2002. Privacy Rule of the Health Insurance Portability and Accountability Act. https://www.hhs.gov/hipaa/for-professionals/privacy/index.html Accessed: March 25, 2023.
[41] National Institute of Standards and Technology. 2020. *NIST Privacy Framework: A Tool for Improving Privacy Through Enterprise Risk Management*. Technical Report Version 1.0, Includes updates as of January 16, 2020. U.S. Department of Commerce, Washington, D.C. https://doi.org/10.6028/NIST.CSWP.01162020
[42] Information Commissioner's Office. 2018. *Data Protection Impact Assessment*. Technical Report. https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessment-dpia-1-0.pdf Accessed: March 25, 2023.
[43] Habeeb Olufowobi, Clinton Young, Joseph Zambreno, and Gedare Bloom. 2019. SAIDuCANT: Specification-based automotive intrusion detection using controller area network (CAN) timing. *IEEE Transactions on Vehicular Technology* 69, 2 (2019), 1484–1494.
[44] Basker Palaniswamy, Seyit Camtepe, Ernest Foo, and Josef Pieprzyk. 2020. An efficient authentication scheme for intra-vehicular controller area network. *IEEE Transactions on Information Forensics and Security* 15 (2020), 3107–3122.
[45] Sakshyam Panda, Aristeidis Farao, Emmanouil Panaousis, and Christos Xenakis. 2021. Cyber-Insurance: Past, Present and Future. In *Encyclopedia of Cryptography, Security and Privacy*. Springer, 1–4.
[46] Sakshyam Panda, Emmanouil Panaousis, George Loukas, and Christos Laoudias. 2020. Optimizing investments in cyber hygiene for protecting healthcare users. *From Lambda Calculus to Cybersecurity Through Program Analysis: Essays Dedicated to Chris Hankin on the Occasion of His Retirement* (2020), 268–291.
[47] Sakshyam Panda, Stefan Rass, Sotiris Moschoyiannis, Kaitai Liang, George Loukas, and Emmanouil Panaousis. 2022. HoneyCar: a framework to configure honeypot vulnerabilities on the internet of vehicles. *IEEE Access* 10 (2022), 104671–104685.
[48] Sakshyam Panda, Daniel W Woods, Aron Laszka, Andrew Fielder, and Emmanouil Panaousis. 2019. Post-incident audits on cyber insurance discounts. *Computers & Security* 87 (2019), 101593.
[49] Ying Qiu, Yi Liu, Xuan Li, and Jiahui Chen. 2020. A novel location privacy-preserving approach based on blockchain. *Sensors* 20, 12 (2020), 3519.
[50] Laurens Sion, Dimitri Van Landuyt, Kim Wuyts, and Wouter Joosen. 2019. Privacy risk assessment for data subject-aware threat modeling. In *2019 IEEE Security and Privacy Workshops (SPW)*. IEEE, 64–71.
[51] Daniel J Solove. 2006. A taxonomy of privacy. *University of Pennsylvania law review* (2006), 477–564.
[52] Xiaoqiang Sun, F Richard Yu, and Peng Zhang. 2021. A survey on cyber-security of connected and autonomous vehicles (CAVs). *IEEE Transactions on Intelligent Transportation Systems* 23, 7 (2021), 6240–6259.
[53] Jun Tang, Yong Cui, Qi Li, Kui Ren, Jiangchuan Liu, and Rajkumar Buyya. 2016. Ensuring security and privacy preservation for cloud data services. *ACM Computing Surveys (CSUR)* 49, 1 (2016), 1–39.
[54] Maria Tsiodra, Sakshyam Panda, Michail Chronopoulos, and Emmanouil Panaousis. 2023. Cyber Risk Assessment and Optimisation: A Small Business Case Study. *IEEE Access* (2023).
[55] Hiroshi Ueda, Ryo Kurachi, Hiroaki Takada, Tomohiro Mizutani, Masayuki Inoue, and Satoshi Horihata. 2015. Security authentication system for in-vehicle network. *SEI technical review* 81 (2015), 5–9.
[56] Paul Voigt and Axel Von dem Bussche. 2017. The eu general data protection regulation (gdpr). *A Practical Guide, 1st Ed., Cham: Springer International Publishing* 10, 3152676 (2017), 10–5555.
[57] Yuan Wu, Li Ping Qian, Haowei Mao, Xiaowei Yang, Haibo Zhou, Xiaoqi Tan, and Danny HK Tsang. 2018. Secrecy-driven resource management for vehicular computation offloading networks. *IEEE Network* 32, 3 (2018), 84–91.
[58] Kim Wuyts and Wouter Joosen. 2015. LINDDUN privacy threat modeling: a tutorial. *CW Reports* (2015).
[59] Chulin Xie, Zhong Cao, Yunhui Long, Diange Yang, Ding Zhao, and Bo Li. 2022. Privacy of Autonomous Vehicles: Risks, Protection Methods, and Future Directions. *arXiv preprint arXiv:2209.04022* (2022).