Data Privacy Threat Modelling for Autonomous Systems: A Survey from the GDPR's Perspective

Naila Azam*, Lito Michala*, Shuja Ansari†, Nguyen Binh Truong*
*School of Computing Science, University of Glasgow, Glasgow G12 8QQ UK
†James Watt School of Engineering, University of Glasgow, Glasgow G12 8QQ UK
Email:{n.naila.1}@research.gla.ac.uk
{AnnaLito.Michala, shuja.ansari, nguyen.truong}@glasgow.ac.uk

Abstract—Artificial Intelligence-based applications have been increasingly deployed in every field of life including smart homes, smart cities, healthcare services, and autonomous systems where personal data is collected across heterogeneous sources and processed using ”black-box” algorithms in opaque centralised servers. As a consequence, preserving the data privacy and security of these applications is of utmost importance. In this respect, a modelling technique for identifying potential data privacy threats and specifying countermeasures to mitigate the related vulnerabilities in such AI-based systems plays a significant role in preserving and securing personal data. Various threat modelling techniques have been proposed such as STRIDE, LINDDUN, and PASTA but none of them is sufficient to model the data privacy threats in autonomous systems. Furthermore, they are not designed to model compliance with data protection legislation like the EU/UK General Data Protection Regulation (GDPR), which is fundamental to protecting data owners' privacy as well as to preventing personal data from potential privacy-related attacks. In this article, we survey the existing threat modelling techniques for data privacy threats in autonomous systems and then analyse such techniques from the viewpoint of GDPR compliance. Following the analysis, We employ STRIDE and LINDDUN in autonomous cars, a specific use-case of autonomous systems, to scrutinise the challenges and gaps of the existing techniques when modelling data privacy threats. Prospective research directions for refining data privacy threats & GDPR-compliance modelling techniques for autonomous systems are also presented.

Index Terms—Autonomous Systems, Data Privacy, General Data Protection Regulation, GDPR, Threat Modelling Technique

1 Introduction

In recent years, data-driven applications are increasingly being deployed in all aspects of life including smart homes, smart cities, healthcare, medical services, and autonomous systems (AS) [1]. In such applications, Artificial Intelligence (AI) incorporating various algorithms is profoundly employed, where personal data is collected and aggregated from heterogeneous sources before being processed using ”black-box” algorithms in opaque centralised servers [2]–[5]. As a consequence, preserving the data privacy and security of these applications is of paramount importance [6]. In this respect, a modelling technique for detecting potential threats and specifying countermeasures to mitigate the vulnerability plays a significant role in securing personal data from a variety of data breaches and privacy attacks.

Numerous threat modelling techniques have been proposed in the literature such as STRIDE, LINDDUN, and PASTA but none of them is sufficient to model the privacy threats of AS. This is due to several reasons such as: (i) most of the existing threat modelling techniques sorely focus on software-based security, not data privacy threats, (ii) several techniques such as LINDDUN are dedicated to modelling data privacy threats but their approaches are based on assumptions [7] (i.e., implementation assumptions [8] and security assumptions [9]); as a consequence, such techniques are limited to only pre-defined threats [7]–[9]; and (iii) these techniques are not adoptable to new privacy breaches and new types of privacy attacks in complex systems consisting of numerous components including humans, smartphones, sensors, and other types of Internet of Things (IoT) devices such as traffic cameras and road-side units (RSU). Modelling the privacy threats for such systems requires a holistic picture of threat landscapes in which diversified components are interplayed, rather than only considering some specified and pre-defined system models. Furthermore, since May 2018, the new data protection legislation in EU member states and the UK (i.e., the General Data Protection Regulations (GDPR)[1]) has come into force. Modelling the GDPR-compliance is more effective in ensuring users' privacy and protecting personal data, far beyond modelling data privacy threats, which only focus on different types of privacy-related attacks [10], [11]. This has called a critical need for applications and/or services processing personal data to have modelling tools for analysing data privacy threats and analysing compliance with sophisticated GDPR requirements [11]–[13].

In this paper, we conduct a survey on data privacy threat modelling techniques with the focal point of whether such techniques are applicable for modelling data privacy threats in autonomous systems, particularly under the perspective of complying with the GDPR. The main contributions of this

[1] https://gdpr-info.eu/

survey paper are as follows:

1) The review of the existing modelling techniques for privacy threats in autonomous systems under the GDPR compliance perspective.
2) An insightful analysis of modelling privacy threats and complying with the GDPR in autonomous systems, provides a better understanding of how complying with the GDPR directly results in preventing privacy threats by taking an autonomous car system as the evident instance.
3) The identification of challenges, gaps, and future research directions in developing an effective data privacy modelling technique leveraging the GDPR principles and requirements as the baseline, enabling the compliance verification and enforcement in autonomous systems.

The rest of the paper is organised as follows: In Section 2, we provide the background on various threat modelling techniques as well as an overview of autonomous systems. In Section 3, the state-of-the-art threat modelling techniques are described with analysis of how these techniques can determine the data privacy requirements and identify threats in AS. The next section (Section 4) provides detailed information about the GDPR principles and requirements, their roles in preserving data privacy in AS, and specifies the rationale for not being compliant with the GDPR. Section 5 presents an insightful discussion on how threat modelling techniques (i.e., STRIDE and LINDDUN) are applied in the Autonomous Car System (ACS) use-case, along with the challenges and gaps for identifying data privacy threats under the perspective of GDPR compliance. In this section, unsolved challenges hindering the existing modelling techniques from effectively modelling data privacy and the GDPR-compliance are also analysed. The last section (Section 6) summarises the paper and provides potential research directions to develop data privacy threat modelling techniques for AS based on the GDPR.

2 Background

This section provides background on the concept of threat modelling and notable modelling techniques that can be employed in AS. An overview of AS with characteristics, challenges, and difficulties in modelling data privacy threats is also provided. Table 1 depicts the acronyms with descriptions frequently used throughout this paper.

2.1 Overview of Threat Modelling

Threat modelling is a procedure that is used to (i) determine the security requirements of a system, (ii) identify threats and vulnerabilities, (iii) evaluate the criticality of the detected threats and vulnerabilities, and (iv) prioritize the mitigation methods. Threat modelling is based on several traditional security methods such as attack trees and STRIDE, which were developed in the 1990s. [14]. The modelling of threats requires comprehending the system's complexity and recognizing all possible dangers to the system [15]. It is essential to identify the threats that can occur in a system before claiming that it is secured [15]. Furthermore, the security of the system is defined using a systematic engineering approach [16]. This approach includes the identification of security risks, security requirements, and recovery strategies. It would require less time and effort to address the security issues if security engineering [17] is incorporated in the system design process [18] from the initial architecture specification.

The identification of threats helps in the formulation of realistic and relevant security requirements. This is important because if the security criteria [19] are inaccurate, the system's concept of security is incorrect, and the system cannot be secured. A proper threat assessment [20] reduces the capacity of attackers to misuse the system. The most succinct and basic descriptions of the threat modelling approach have been provided which include four key phases, namely decomposing the system, eliciting the threats, determining the countermeasure and mitigation, and prioritizing the threats. Therefore, a threat modelling technique is typically developed based on a four-step framework in accordance with the four phases, as illustrated in Figure 1 [21].

In step 1, a model of the system is created. Data flow diagrams and attack trees, for example, are good ways to illustrate system modelling. In step 2, the threat model/approach is used to find threats. Threat modelling approaches such as STRIDE [21], Attack trees [22], PASTA [23] etc., can be used to find threats in a system. In step 3, these approaches are used to outline mitigation strategies for the threats. Finally, in step 4, the model is validated for completeness and effectiveness (i.e., the system is secured from potential threats).

2.2 Notable Threat Modelling Techniques

A variety of threat modelling techniques have been proposed and are already used in real-world scenarios, coming with both pros and cons.

2.2.1 STRIDE

STRIDE is a model-based threat modelling technique developed by Microsoft [24]. It has been effectively applied to cyber-physical systems (i.e., grid systems, robotics systems etc.) [25]. This is a two-way method. In the first phase, a data flow diagram is created to check the flow of data. In the second phase, the STRIDE technique is utilized to identify and model the threats as defined by its name (i.e., Spoofing, Tempering, Repudiation, Information Disclosure, and Elevation of Privileges) [26]. The threats identified by STRIDE are listed in Table 2, along with their corresponding definitions.

Before the physical installation of systems (i.e., IoT devices, autonomous systems etc.), STRIDE [27] is utilized in the design phase to identify cyber-attacks(i.e, phishing attacks). After that, threat mitigation strategies are employed to stop the identified threats [28]–[30]. In addition, The main

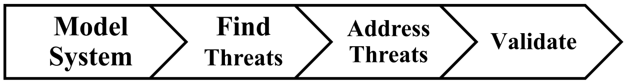


Fig. 1: The four-step framework for threat modelling techniques

TABLE 1: Acronyms with Descriptions

Acronyms	Description	Acronyms	Description
AC	Autonomous Car	IOI	Items of Interest
AS	Autonomous System	LINDDUN	Linkability, Identifiability, Non-Repudiation, Detectability, Disclosure of Information, Unawareness, and Non-Compliance
ACS	Autonomous Car System	PbD	Privacy by Design
DC	Data Controller	RSU	Road Side Unit
DP	Data Process	STRIDE	Spoofing Tempering Repudiation Information Disclosure and Elevation of Privileges
DS	Data Subject	TA	Trusted Authority
DoI	Disclosure of Information	V2V	Vehicle to Vehicle
GDPR	Data Protection Regulation	V2I	Vehicle to Infrastructure

TABLE 2: Threat Categories of STRIDE

Threat	Security Requirement	Description
Spoofing	Authentication	Pretending to be something or someone other than yourself.
Tampering	Integrity	Try to add/modify something in resources(disk, network, memory etc.).
Repudiation	Non-Repudiation	Claiming you were not responsible or did not do something.
Information Disclosure	Confidentiality	The information is provided to the one who is not authorized.
Denial of Service	Availability	Restrict the resources that are required to deliver.
Elevation of privilege	Authorization	Permitting someone to perform a task for which they are not authorised.

TABLE 3: Threat Categories of LINDDUN

Threats	Properties
Linkability	Unlinkability
Identifiability	Anonymity & pseudonymity
Non-repudiation	Plausible deniability
Detectability	Undectecbility & unobservability
Disclosure of information	Confidentiality
Content unawareness	Content awareness
Policy and content non-compliance	Policy and content compliance

issue of modelling with the STRIDE is that as the system's complexity grows, so does the number of threats. Another drawback of STRIDE is that it cannot guarantee to model the system's data privacy threats [31].

2.2.2 LINDDUN

LINDDUN stands for Linkability, Identifiability, Non-Repudiation, Detectability, Disclosure of information, Unawareness, and Non-Compliance. Linkability allows the attacker to connect two or more Items of Interest (IoIs) to establish a link to a specific system. The term "identifiability" means that the attacker will be able to locate the object of interest. Non-repudiation is another threat in which an adversary attempts to attack a target, but difficult-to-counter evidence. Detectability refers to whether an enemy can identify a target of interest. Furthermore, information disclosure is a security risk that exposes information that should not be exposed [32].

Moreover, Unawareness is a threat that occurs when a user does not know the effects of sharing information. The non-compliance threat shows that the system is not compliant with the regulations and legislation. Table 3 illustrates the threat categories of LINDDUN. Furthermore, LINDDUN uses the iterative process to discover dangers in a system and then build threat trees [33]–[35]. The strong point of LINDDUN is that it has rich privacy documentation. On the other hand, it is a lengthy procedure.

Another deficiency of LINDDUN is that it is based on some pre-defined assumptions and lacks flexibility in complex scenarios where different components interplay with each other. The assumptions are defined in the LINDDUN tutorial [33] as "direct or indirect choices to trust the system components (i.e., data store or data flow) to behave as expected". The LINDDUN threat template (which is included in the supporting materials) allows assumptions to be entered in the 'Remarks' section. However, the study [7] found that most of the assumptions are based on the DFD notation's limitation of expressiveness. Some assumptions directly refer to concepts such as trust and attacker capabilities that are not typically modelled in a system architecture, which raises the question of whether these aspects should be modelled directly as a part of the system [7].

2.2.3 PASTA

Process for Attack Simulation and Threat Analysis (PASTA) is a risk-centric technique that consists of seven stages [36]. It has several functions which are performed at various phases. Stage 1, defines the objectives; stage 2, defines the technical purpose; stage 3, implements the application decomposition; stage 4, conducts threat analysis; stage 5, conducts vulnerability and weaknesses analysis; stage 6, conducts attack modelling; and stage 7 conducts risk and impact analysis [23], [37]. This technique can be used to meet both business and technical goals [38]. PASTA has rich documentation to assist with its laborious and extensive process [39]. However, this technique is insufficient to deal with data privacy threats.

2.2.4 Persona non-Grata

The Persona Non-Grata (PnG) modelling approach focuses on attackers, their motivations, and their ability to attack a system. It allows the threat modellers to identify the threats from the counter side. The technical experts try to identify vulnerabilities that are caused by the potential adversary [40]. This technique [41] identifies misuse cases with a target, possible attack scenarios, and adversarial personas [42].

Furthermore, This technique is simple to implement, yet it is underutilized in research. It has a low rate of false positives and a good level of consistency, although it may not be able to detect all threat types [41]. This technique can be used with an agile approach that includes personas.

2.2.5 Security Cards

This is an informal technique based on brainstorming for identifying novel and difficult attacks. The analysts utilize play cards to answer questions about potential attacks in various scenarios. For instance, why is the system under attack? Who is responsible for this? What kind of assets can be harmed and how can they be harmed? [41].

To identify threats, the Security Cards modelling technique uses a deck of 42 cards such as human impact (9 cards), adversary's motivations (13 cards), adversary resources (11 cards), and adversary's methods (9 cards). This approach can be used to discover almost any form of threat, but it produces a lot of false positives and can not be employed in non-standard scenarios [41]. In industry, the Security Card technique is hardly used [41].

2.2.6 *hTMM*

The Hybrid Threat modelling Method (hTMM) is made up of SQUARE (Security Quality Requirements Engineering Method), Security Cards, and PnG activities [42], which was developed by Software Engineering Institute in 2018. The main characteristic of the technique is to provide a consistent result with no false positives(i.e., an object, that has been classified as harmful despite the fact that it isn't a threat), and no overlooked threats [42]. The main steps of hTMM are to highlight the system to be threat-modelled, apply for the security cards, remove unlikely PnG (i.e., there are no realistic attack vectors), use the tool support for finalizing the results, and finally continue to process for risk assessment. The flaw in htMM is that it does not provide mitigation for the threats that have been identified, and it requires a lot of effort to model complex systems.

2.2.7 *Attack Trees*

This is one of the oldest techniques, and it has been widely used in conjunction with other threat modelling techniques like STRIDE, CVSS, and PASTA [43], [44]. The attacker's aim is put at the root of the tree, while the strategies to achieve the goal are put at the leaf nodes. By travelling through the leaves, AND and OR nodes are used for various aims. Attack trees are used to make security decisions and determine whether the system is vulnerable to attack. The use of the attack tree modelling technique was proposed [44] to develop the threat model of buildings and home automation systems to model the security flaws in their development and implementation. This strategy is simple to understand and only beneficial when security considerations are properly comprehended [44].

2.2.8 *Quantitative Threat modelling Method (QTMM)*

This technique [45] consists of STRIDE, CVSS and Attack Trees. With this technique [46], a few pressing issues could be solved for cyber-physical systems. Another aim of QTMM technique is to generate attack ports for individual components. These attack ports then forward the risk to the connected components. The system risk assessment is done by score card (i.e., (1) Insignificant, (2) Minor, (3) Moderate, (4) Major, and (5) Catastrophic). If the component root nodes have a high-risk score, the attacked port has a high-risk score as well and is thus more likely to be executed. This is a time-consuming technique and requires high effort to achieve consistent results.

2.2.9 *Trike*

In Trike, the threat modelling is performed from the viewpoint of defensive and risk management [47]. This technique starts by defining a system. Then the expert analyses the requirement model by enumerating and understanding the system's actors, assets, intended actions, and rules. As a result, an actor-asset-action matrix can be built. The trike modelling technique lacks documentation and is a time-consuming process.

2.2.10 *CVSS*

The Common Vulnerability Scoring System (CVSS) modelling approach identifies vulnerability attributes and assigns a numerical score to their severity. This establishes a consistent grading system for a variety of cyber-physical systems [48], [49]. CVSS has three metric categories (Base, Temporal, and Environmental), each with a set of measurements.

The algorithms for computing the scores of metrics are confusing, even though these metrics are thoroughly detailed in the documentation. However, this approach is still commonly employed. Other threat modelling techniques are utilized in conjunction with this technique.

2.2.11 *VAST*

The Visual, Agile, and Simple Threat (VAST) modelling approach is an automated threat modelling approach. Because of its scalability and applicability, this strategy is employed in large organizations to offer actionable and dependable findings for a variety of stakeholders [50], [51].

Two models are developed in this technique: an application threat model that uses data flow diagrams and an operational threat model that is based on attacker mindset DFDs. As a result, VAST can be integrated into the development and DevOps life-cycle of an organization [50]. This technique is used to model security and privacy in intelligent autonomous vehicles [52]. However, this technique is time-consuming and requires extensive effort in modelling a system.

2.2.12 *OCTAVE*

For cyber-security planning and assessment, the Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) modelling technique [53], [54] are utilized. It is primarily concerned with identifying organizational risks and does not address technical threats. This strategy was created primarily for large organizations. Small businesses can also benefit from OCTAVE-S. This technique is comprehensive and adaptable. However, It's a time-consuming procedure with vague documentation.

Table 4 illustrates the strengths and weaknesses of threat modelling techniques [38]. These techniques are evaluated based on various parameters such as maturity, focus, time/effort, mitigation etc. The 'maturity' is determined by how effectively each technique is specified, how frequently it has been utilized in case studies, and how frequently it has been coupled with other techniques. The 'focus' shows the point of view or the perspective based on which the technique was designed. The 'Time/Effort' indicator indicates how time-consuming and labor-intensive

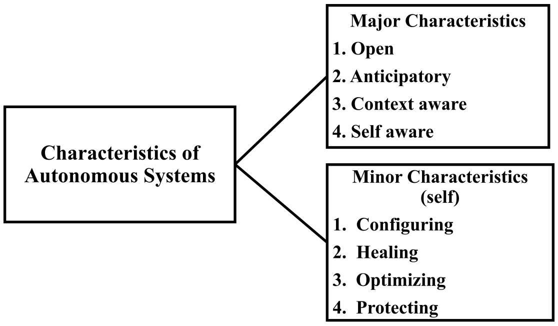


Fig. 2: Characteristics of Autonomous Systems [57]

the procedure is. The term 'mitigation' refers to whether the procedure includes any mitigation strategies. The term 'consistent results' refers to whether or not a technique provides consistent results when repeated. The 'Easy to use/learn' term represents how easily these techniques are adopted. The term 'automation' shows the ability of the technique to be examined in an automated way. Finally, the term 'tool' shows its integration with Software Development Life Cycle (SDLC).

2.3 Autonomous Systems and Characteristics

A machine or a system is considered to be autonomous when it is capable of thinking, contemplating, speculating, and making judgments without human involvement [56]. Figure 2 [57], illustrates the characteristics of an autonomous system (AS). These characteristics are divided into minor and major characteristics. The minor characteristics include self-configuring, self-healing, self-optimizing, and self-protecting (termed as CHOP); and the major characteristics include open, anticipatory, context-aware, and self-aware.

The relationship between ISO 9126 quality parameters and AS features [58], [59] is depicted in Table 5. Functionality, Reliability, Usability, Efficiency, and Maintainability are examples of quality factors. The term 'Functionality' refers to software that can meet the needs of its users. It also has the security features of appropriateness, accuracy, and interoperability [60], [61]. The term 'Reliability' refers to a system's ability to adapt to changes in the environment, correct problems, and improve its own performance. Moreover, 'Usability' refers to how easily a user can communicate with a system. Understandability, learnability, attractiveness, and operability are all sub-factors of Usability. The 'Efficiency' is measured in the context of time and resources; i.e., the extent to which the system can make use of its resources. Furthermore, the capacity to facilitate ease of maintenance is referred to as 'Maintainability'. The sub-factors of maintainability are analysability, testability, changeability, and scalability. The ability of software to adapt to and transfer to any environment is referred to as 'Portability'. Portability [61] has sub-characteristics such as adaptability, instability, replicability, and coexistence.

The characteristics of AS highly affect the privacy preservation in autonomous systems [62]. For example, the characteristics of AS such as being open and transparent are important factors for its users since it fosters confidence in the system by giving them an easy way to comprehend what the system is doing and why. Moreover, transparency is crucial for AS safety certification because it makes the system's procedures available for independent verification against safety requirements. If accidents occur, an AS (i.e., Autonomous Car) must be open to investigators and be able to pinpoint the internal procedure that caused the accident. Thus, failing to be transparent would lead to an untrustworthy AS, requiring the threat modelling technique to ensure how the AS would respond to the external adverse environment and identify the emergence of threats.

Figure 3 shows the architecture of the Autonomous System (AS). The AS has five main components [63]: autonomic manager, knowledge source, touch-point, manual manager, and enterprise service bus. These components work together to manage the system itself. The autonomic manager uses the control loop which is made up of four functions known as MAPE (Monitor, Analyze, Plan and Execute). It controls both hardware and software components. Autonomic Manager consists of two elements i.e., managed element and the autonomic element. The managed element represents the entire system that has sensors and effectors. Sensors collect the information of current states and store it in a knowledge base and effectors help the autonomic manager to trigger actions over the managed elements.

The flow of data in Figure 3, illustrates how the managed element collects the information through sensors and transfer it to the control unit to decide on and dictate appropriate actions to the effectors. All components work together to perform tasks by transforming knowledge. The knowledge component contains knowledge of any type of data that is used by the autonomic manager for performing management functions. The knowledge can be in the form of information on policies, requests or changes in plans. Moreover, the touch-point identifies the current state of the managed element and performs some management operations. The manual managers allow IT professionals to perform management operations. Whereas the enterprise service bus enables the connection between all the building blocks of a system through which they can communicate with each other.

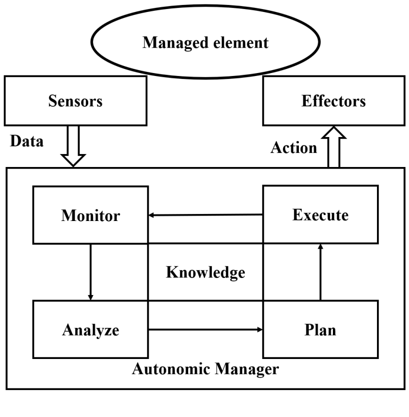


Fig. 3: Architecture of Autonomous System

TABLE 4: Strengths and Weaknesses of some notable Threat modelling Techniques [38]

Threat modelling Techniques	Maturity	Focus	Time/Effort	Mitigation	Consistent results	Portability	Easy to use/learn	Automation	Tool
STRIDE [26]	High	Defender	High	Yes	No	Yes	Medium	Yes	Yes
LINDDUN [33]	High	Assets /Data	High	Yes	No	Yes	No	No	No
PASTA [36]	High	Risk	High	Yes	No	Yes	No	No	No
CVSS [55]	High	Scoring	High	No	Yes	No	No	Yes	No
Attack Trees [44]	High	Attacker	High	No	Yes	Yes	Yes	No	No
PnG [41]	Medium	Attacker	Medium	No	Yes	Yes	Yes	No	No
Security Cards [41]	Medium	Attacker	Medium	No	No	Yes	Yes	No	No
hTMM [42]	Low	Attacker /Defender	High	No	Yes	Yes	Medium	No	No
Quantitative TMM [45]	Low	Attacker /Defender	High	No	Yes	Yes	No	No	No
Trike [47]	Low	Risk	High	Yes	No	Yes	Medium	No	No
VAST [50]	High	Attacker	High	Yes	Yes	Yes	Medium	Yes	Yes
OCTAVE [53], [54]	Medium	Risk /Organization	High	Yes	Yes	Yes	No	No	No

TABLE 5: Mapping Characteristics of Autonomous Systems with Quality Factors [58], [59]

Quality Factors	**Autonomous System Characteristics**	
	Minor (self)	**Major**
Functionality	Configuring Protecting Optimizing Protecting	Self Aware Context Aware
Reliability	Healing Protecting	——
Usability	Configuring	——
Efficiency	Optimizing	Anticipatory
Maintainability	Configuring Healing Optimizing	Anticipatory
Portability	Configuring	Open

2.4 Preserving Data Privacy in Autonomous Systems

The wide use of Autonomous Systems (AS) has resulted in various ethical and privacy issues and concerns [64]. Users' privacy must be protected not just to comply with the Universal Declaration of Human Rights [2], but also to prevent cybercrime such as phishing attacks [65], identity theft [66], cyber frauds [67], online discrimination [68], cyberbullying [69], cyberstalking [70], and other forms of cyber-crimes [71]. Privacy is an important factor to be considered when it comes to safeguarding the ethics and values of AI systems [72]. The effects and challenges of privacy in AI-based equipment are described in the studies [73]–[75].

Autonomous technologies such as drones [76], self-driving cars [77], robots [78], and personal assistants [79] acquire a significant amount of data from their users. This data is gathered through surveillance and interrogatory ways [80]. In surveillance mode, autonomous systems gather information automatically, E.g., an autonomous car collects the data of distance travelled, time-stamped location, routes taken, and departure and arrival points [81]. In the interrogation mode, the user is asked to supply information. Personal assistants, for example, might inquire about the next song to be played, or a self-driving car might inquire about the destination location. The data obtained by these devices may have privacy problems (i.e., drones may be used to spy on individuals on purpose [82]). Thus, challenges to privacy vary depending on the extent of autonomy, for example, a completely autonomous system [83] is independent in collecting data and can modify the technique or type of data collection at any time.

Information processing of collected data by the AS can lead to a variety of activities. Aggregation is one of these activities [80]. This allows the system to learn more about the individual than the individual knows about themselves, a phenomenon known as inverse privacy [84]. For example, the autonomous automobile can create a detailed profile of the passenger's travel patterns and behaviors, proving someone was at a specific location, and predicting the user's future trips [81]. Exclusion [80] is another activity, where the user is unable to change or remove his previously stored data, allowing the AS to make incorrect decisions about them based on their previously stored data. Identification of the individual based on linkability is another activity [80]. Drones that collect information on individuals, for example, have cameras that are not static like CCTVs, and can readily identify the individual based on his ongoing data collection. The owner of a car can be identified by the face and gait as developed by Jaguar [85]. This could also allow the Autonomous Car (AC) to distinguish between passengers in other automobiles, as well as pedestrians who happen to be walking by. As a result, what people do and where they travel could be monitored.

Another challenge with the AS's information processing of obtained data is the use of individual data for segregation and discriminating reasons [86], which is often regarded as violating people's privacy [87]. For example, a healthcare robot [88], [89] could decide on its own whether or not to provide a specific treatment to someone who leads an unhealthy lifestyle or to prioritize those who are in better health. Additionally, further research is being carried out to see if the AS is capable of lying and manipulating us to persuade us [90]. As, AS gather more information about us, it is privy to using persuasive methods on us [91].

Another significant challenge in ensuring data privacy in AS is information dissemination [91]. The AS may share the information it collects with other parties for marketing or advertising purposes. The location of the vehicle and its owner can be tracked and shared by the infrastructure with

[2] https://www.un.org/en/about-us/universal-declaration-of-human-rights

third parties. Furthermore, some organizations promote drone-based advertising [92]. Individuals would be easily exposed to coordinated autonomous systems without the need for any precise time or location constraints. As a result, this may pose a greater threat to an individual's privacy than any previous attacks in this technologically advanced age.

In the next section, we will discuss how data privacy threats in AS can be modelled using the existing threat modelling techniques.

3 Data privacy threat modelling for autonomous systems

This section examines how existing threat modelling techniques are used for conducting data privacy threats, particularly for autonomous systems. We also scrutinize barriers and challenges when implementing these techniques for modelling data privacy and GDPR compliance as well as discuss the reasons why such techniques are not fully suitable for data privacy analysis in autonomous systems.

3.1 Overview of Data Privacy Threat Modelling Techniques for Autonomous Systems

Existing threat modelling techniques such as STRIDE, PASTA, and Attack trees are well suited for modelling security threats for AS [93]; however, these may not be effective enough to model the data privacy of an AS [94]. In the survey [95], the authors cover cyber-security and modelling approaches for finding and mitigating risks and vulnerabilities in the AS. The researcher further focuses on modelling systems, threats, vulnerabilities, and attacks of AS but does not highlight the approaches to model the data privacy threats in autonomous systems.

Moreover, the survey [96] highlighted models and methods based on machine learning (ML) and deep learning (DL) that can detect and counter both known and unidentified threats (i.e., SQL injection, OS fingerprinting, malicious code execution, etc.) in big data. The study also suggested a Secure Data Analytics (SDA) architecture based on DL and ML to characterize input data as acceptable or malicious. Similarly, in the review paper [97], the authors examine certain threat models and risk assessment techniques related to IoT. They also discuss the various IoT risk assessment techniques. To predict and evaluate cyber risks and safeguard industrial assets from future cyberattacks, the study [98] suggests a structured threat modelling technique for Industrial Cyber-Physical Systems (ICPS). The process includes categorizing ICPS assets according to their level of importance before examining the cyber security flaws, threats, risks, effects, and solutions. However, these studies do not discuss the data privacy threats and the countermeasures specifically for AS.

Syed Ghazanfar Abbas [99] used the STRIDE threat modelling technique to identify phishing threats in the automotive system [100] and the smart home [101]. Phishing causes data breaches which are done by theft of the user's credentials by sending emails [102]–[104]. Moreover, in [105], the authors used various threat modelling techniques such as VAST, PASTA, STRIDE etc. for the Intelligent Autonomous Vehicles (IAV) to discuss and mitigate the privacy and security-related vulnerabilities. It also discusses the taxonomy of security, vulnerability, and privacy. The researchers in [106], use the CIA (Confidentiality, Integrity, Availability) model to analyze each component of a system to identify security and privacy-related attacks. However, these techniques are not fully effective in detecting phishing attacks and preventing AS from data breaches.

In [107], the authors used LINDDUN threat modelling technique and presented the evaluation criteria for a smart home hub using common criteria. The descriptive study [108] of LINDDUN assumptions is presented for the empirical study of IoT-based home automation systems. The result showed that these assumptions are suitable for mitigating some potential threats, but some assumptions are under analysis where some are not in the scope of LINDDUN. Moreover, in the study [109], the authors explained that LINDDUN is not sufficient to mitigate the privacy threats [110], which is not directly related to regulatory compliance (i.e. General Data Protection Regulation (GDPR)). He proposed the basis for developing a new framework for ensuring the privacy of IoT-based applications (i.e. smart homes). This framework would be based on PbD and GDPR. Thus, LINDDUN failed to fully detect the data privacy threats and ensure data protection in AS systems.

Moreover, many researchers have proposed various privacy models for preserving the privacy of the AS systems but they are not effective enough to ensure the data privacy of these. For example, Feng [111], proposed the Sybil attack model for VANET where attackers exploit the identities of others to send false messages and create accidents in VANET. The researcher describes different situations where the attacker sends false notifications and messages to create traffic issues. The authors in [112], discuss the Bell-LaPadula privacy model for preserving the confidentiality of information in securing Unmanned Autonomous Systems (UAS) from cyber threats. Furthermore, in [112], the authors describe how the privacy-related legislation of various countries is not enough to meet the privacy requirements of the AS such as unmanned aircraft systems. They suggest combining the legislated requirements and impact assessments to properly deal with the privacy of the systems. Therefore, privacy-related legislation should be incorporated into the proposed privacy models for AS system.

In [113], the researcher discusses the privacy and security threats in IoT devices (i.e. smart locks). An attacker can steal the credentials of the authorized person to permit to open the smart lock. The researchers suggested geo-fencing and touch-to-unlock techniques for unwanted unlocking of smart locks. To deal with the trust and privacy of the network of IoT devices the authors developed a fog computing paradigm [114] instead of using threat modelling techniques.

3.2 Challenges and difficulties in conducting threat modelling for AS

In [115], STRIDE, LINDDUN, QTMM and CORAS modelling techniques are used for security research for autonomous applications (i.e IoT devices). The researchers discuss three gaps in threat modelling frameworks that are used for IoT security research. First, threat modelling techniques are more focused on the software-based threat, thus ignoring the hardware-based threats. Second, threat modelling methods are limited to the defined threats as explained by their authors. Finally, these techniques are not adaptable to new attack concepts for IoT devices. Thus, there is a requirement for a holistic picture of the threat landscape.

It has been noticed that UAV [116] is a popular field of research regarding system modelling. Initially, the modelling of the autonomous vehicle started to deal with the DARPA challenge [106]. The UAV has a complex architecture and most of the information regarding measures in place is confidential, so it is difficult to identify which threat is more dangerous to a UAV that needs to be modelled at utmost priority [106]. Moreover, there has been wide research for modelling the security and privacy of vehicle-to-vehicle (V2V) [117], Vehicle-to-infrastructure (V2I) [118] and Vehicle-to-everything (V2X) [119]. But threat modelling techniques (such as STRIDE, LINDDUN) are not sufficient for securing V2V, V2I and V2X because they require the autonomy approach [120] to deal with privacy and security vulnerabilities. The detailed taxonomy of security and privacy vulnerabilities of AV is proposed with active, passive and preventive mechanisms [105]. However, there would be computational or real-time limitations for those proposed mechanisms. In short, the researchers found that existing regulatory approaches are not enough to model privacy concerns of Unmanned Aircraft System (UAS) due to their high complexity [121].

The traditional threat modelling techniques have failed to cope with the high-volume and the high velocity of big data applications [122]. A system processing big data normally imposes significant data leaks which include intentional leaks and inadvertent leaks, leading to both internal and external threats [123]. These threats can be network intrusion, phishing, espionage, leakage of sensitive information etc. However, threat modelling techniques identify only some specified threats (i.e., spoofing, EoP, identifiability etc.) that may not be suitable for modelling such potential threats. For example, Intelligent Transportation Systems (ITS) [124] produces high volume data that have high impact on the architecture and application of the system. However, numerous data privacy and security risks are not dealt with by the STRIDE modelling technique [125]. Thus, it is suggested that researchers should develop novel privacy-preserving techniques as big data applications rapidly grows resulting in new security issues arising that cannot be addressed with traditional modelling techniques [122].

There are various challenges while modelling AS systems. For example, a semantic modelling paradigm is proposed to check the safety and reliability of AS during run-time in a dynamic environment [126]. The proposed approach is limited to the robotic system which would be expanded to more complex systems and determine its adaptability to various environmental constraints. In [112], the authors suggested dealing with high-risk threats by breaking them into sub-attacks and then ranking these threats using cyber threat modelling and cyber risk analysis techniques. But this approach would be time-consuming and require proper management. Furthermore, the study [113] shows how the attacker exploits the flaws in the design and implementation of smart locks. Several defences and mitigation were proposed, but It is believed that the security of the smart lock and other similar IoT devices would be enhanced if the proposed defences are adopted.

Another example of the challenges for the existing data privacy threat modelling techniques is to model complex and distributed systems in which a large number of participants are exchanged sensitive data for a collaborative task such as a Federated Learning-based system. Federated learning (FL) is a prospective collaborative learning technique that provides better privacy preservation when processing (i.e., training) personal data [127]. However, there still exist data privacy threats in Federated Learning-based systems due to the exchanged information (i.e., ML model parameters) between partners in the FL network [128]. The survey [129] highlighted the two main attacks in FL such as poisoning attacks and inference attacks. The poisoning attacks are aimed to induce the federating learning application to output the target label intended by the attacker and to minimize the accuracy of the application [130]. The inference attacks [131] occur while exchanging gradient in FL training that result in wide privacy leakages. To preserve data privacy the techniques are divided into three categories such as differential privacy [132], secure computation [133], and trusted execution environment [134]. But these techniques are employed at the expense of accuracy [135]. The data privacy constraints change from device to device and even within pieces of data, which is a dire challenge for privacy preservation.

In Federated Learning-based systems, threat modelling techniques (e.g., LINDDUN [33]) can be used for detecting data privacy threats. The linkability threat that may occur in the FL system can be modelled by the LINDDUN. For example, when used by the FL server to link certain pieces of information to specific distinguishable individuals and message metadata—such as the sender's IP address or the timestamp—it can reveal sensitive information about particular individuals. It is possible to prevent communicating parties from knowing the message metadata by using anonymous communication channels, which also guarantees unlinkability [3] in sender-message. Therefore, data privacy threat techniques are also required to be conducted effectively in FL-based systems [136].

3.3 Limitation of the existing data privacy threat modelling techniques

In earlier sections, we provided a thorough review of a variety of threat modelling methods such as STRIDE, PASTA, and LINDDUN, which are used to model security and privacy in AS [95], [137], [138]. However, these techniques only emphasize some specified security but not data privacy threats. Only LINDDUN highlights the privacy-related concerns of the system [108], [110]. However, LINDDUN does not fully identify all potential data privacy-related threats in a complex AS. The challenges of using threat modelling techniques for dealing with privacy-related concerns of AS are discussed in the following paragraphs.

[3] https://www.linddun.org/linkability

In [107], LINDDUN is used as a reference for personal information protection in the smart home hub. However, it is not sufficient to deal with all types of privacy threats in a system as mentioned in the privacy threat taxonomy [107], [108]. Similarly, authors in [108] have illustrated the descriptive study of assumptions based on LINDDUN for home automation systems. However, some specified assumptions are outside of the privacy scope of LINDDUN; it also lacks expressiveness which might cause random assumptions.

Rima Deghaili [139] proposed a STRIDE-based trust-privacy trade-off in a distributed computing environment. However, distributed computing systems, which are made up of autonomous systems, may pose wide privacy and security concerns than that highlighted by STRIDE. In [140], the authors addressed the issue of security by modelling autonomous vehicles with STRIDE. But modelling with STRIDE is limited to the design phase. Autonomous systems are dynamic by nature and STRIDE does not guarantee to preserve the privacy of the systems during the run time [93].

In [109], the authors developed a framework by considering Privacy by Design (PbD) and a compliance-driven approach (i.e. GDPR). But the validation of the proposed work should be extended by additional frameworks and taxonomies [109]. In [121], the researcher found that existing regulatory approaches are not enough to model the privacy concerns of Unmanned aircraft systems (UASs) due to their high complexity. The authors in [121], suggested that legislated and impact assessments can deal with privacy and civil liberties.

In the literature, we found only STRIDE [141] and LINDDUN [108], [110] methodologies for privacy modelling of AS. However, these modelling techniques are not sufficient to preserve the privacy of complex and highly scalable autonomous systems such as Autonomous Car (AC), Unmanned Aerial Vehicle (UAV) and robots. To adopt the privacy policies and to have a system compliant with the regulatory model, there should be a framework with a privacy-preserving threat modelling technique based on the regulatory compliance model (i.e., GDPR).

4 The GDPR and its Roles in modelling data privacy threats for autonomous systems

The goal of the GDPR is to preserve the privacy of personal data by enforcing all participants in the data collection and data processing to comply with its principles under strict conditions. This section introduces the GDPR with its seven principles as well as provides the relationship between GDPR-compliance and data privacy preservation. We also discuss the roles of the GDPR in specifying data privacy threats and determining mitigation solutions for autonomous systems.

4.1 What is the GDPR?

General Data Protection Regulation (GDPR) is a regulation on data protection and privacy [142]. This is enacted in May 2018 in the countries of the European Union [143]. This is an up-gradation of privacy principles proposed in 1995 [144]. GDPR is developed to preserve the privacy of personal data by complying with its principle under strict conditions [145]. Each organization in the EU is obliged to comply with GDPR. If the organization avoids complying with the GDPR then it would be liable to pay a heavy amount of fine [146]. The GDPR is detailed in more than 95 articles that cover all of the technical and administrative principles that govern how corporate and government organizations process personal data [147].

European legislators aimed to harmonize privacy law and enforcement with GDPR [148]. They intended to enhance individual privacy protection while preserving the benefits of data processing [149]. Each EU member state is supposed to have a supervisory authority that is responsible for monitoring GDPR compliance [150].

The organization should comply with Global Privacy Principles [4] such as being clear and transparent; being accountable and keeping personal data secure; taking responsibility and valuing privacy; processing personal data ethically and respecting individual preferences. The international data protection privacy laws are followed and guided by five global privacy principles [151] that include Notice; Choice and Consent; Access and Participation; Integrity and Security; and Enforcement. The principle of 'Notice' means that the user should notice and know about the rules available to protect personal information. The 'Choice and Consent' principle is meant to give individual choices and consent about the use, collection and management of personal information and storage. The 'Access and Participation' principle states that information should only be utilized and accessed by those who are authorized and have the appropriate security protocols in place. The 'Integrity and Security concept' is intended to ensure that data is accessed in a secure and authorized manner. Finally, the term 'enforcement' refers to the process of enforcing compliance with any regulatory model. Therefore, the GDPR is based on international data protection rules, which are an extension of privacy principles.

GDPR is open for interpretation because compliance requirements are abstract. It is made up of seven main principles [121], [152] such as Lawfulness, Fairness, and Transparency; Data minimization; Purpose limitation; Storage limitation; Accuracy; Integrity and Confidentiality; and Accountability. Based on these principles, GDPR is aimed to meet the privacy requirement of personal data.

GDPR defines three main entities [153] such as Data Controller [154] (DC), Data Processor (DP) [155], and Data Subject (DS) [156] play important roles while preserving data privacy. The enterprise must be a data controller and a third-party provider can be a data processor who performs on behalf of the enterprise. There is also a difference between the data controller and the data owner. For example, an accountant can be considered a data controller due to independent judgment which is done to perform professional duties [157]. The various scenarios in which acting as a data controller by enterprise and the third party are discussed in [157].

GDPR gives DS more control over its data by allowing it to exercise various rights such as the right to be informed; right of access; right to rectification; right to erasure; right to restrict processing; right to object; right to data portability;

[4] https://globaldma.com

and right to automated decision-making. The DC and DP are responsible to provide access to various rights to DS and fulfil the request of DS. Moreover, there are six lawful bases of data processing, for example, consent, legitimate interest, contract, legal obligation, vital interest, and public interest. For processing the data, one of these six lawful bases of processing is taken for ensuring compliance. For example, the DC should take the consent of the DS before processing its personal data; Without taking the consent of the DS, its data can not be processed.

The system can only be considered compliant when the principles identified by GDPR are adopted and the defined duties of DP and DC are performed for preserving the privacy of the individual. Furthermore, to comply with the GDPR, organizations are required to implement appropriate controls and statistical disclosure-limitation strategies. And one of the challenges for the implementation is the considerable conceptual gap between legal statements and mathematical formulation around data privacy [158]. The authors explained the concept of "*Predicate Singling Out*" (PSO), which is a privacy attack type that endeavours to capture the notion of singling out occurring in the GDPR. If an attacker identifies a predicate p matching exactly one row in x with a probability substantially higher than a statistical baseline, it isolates a dataset x using the output of a data-release mechanism $M(x)$. This further demonstrates that PSO security implied differential privacy [159] which is a mathematical concept with legal outcomes. The PSO security of differential privacy and k-anonymity are investigated in [160]. Furthermore, the study in [158] depicted that differentiated privacy necessitates PSO security through a relationship to statistical generalisation.

4.2 GDPR Principles and the reciprocity to data privacy threats

GDPR is aimed to provide data protection and privacy to individuals [142]. In today's modern age, preserving the privacy of individuals is not trivial. This sub-section discusses the reciprocity between GDPR principles and data privacy and security by scrutinizing the underlying threats which may occur in case of non-compliance. The relationship between non-complying with the GDPR principles and potential privacy threats will be thoroughly discussed.

4.2.1 Lawfulness, Fairness and Transparency

The first principle of GDPR is Lawfulness/Fairness & Transparency. The lawful basis for processing personal data must be considered for the processing to be lawful. There are six lawful bases (i.e., consent, legitimate interest, contract, legal obligation, vital interest, and public interest). If none of the legal bases applies, there will be a violation of this principle, resulting in the unlawful processing of personal data.

Fairness is applied when the data is handled reasonably. This covers how data is collected. The data controller violates the principle of fairness if they have misled someone to collect their data.

According to the principle of transparency, Individuals must know which data is obtained, for what purpose, for whom, and for how long it will be kept. This information should be written as clearly as possible in an easily understandable way.

If the processing of data is unlawful, unfair, and non-transparent, the processing of personal data would lead to *data abuse*, and *data exploitation* . For example, it is noted that Amazon processes the data of its users unlawfully without informing the DS which is the transparency requirement (i.e, the right to be informed). It was, therefore, recently fined a large sum of money (i.e. $877 million) due to the way it collects and shares personal data via cookie consent on its website [5]. Furthermore, the violation of principles of lawfulness, fairness & transparency would lead to privacy leakage with various privacy attacks (i.e., property inference, reconstruction, membership inference, and model extraction etc.) [161].

4.2.2 Purpose Limitation

This principle state that the processing of the data should be limited to legitimate, explicit, and specific 'purposes' clearly defined in the legal basis (e.g., consent) before the data collection. The processing of data should not be used or transferred beyond the initial purposes for which it has been collected or stored. Generally, processing personal data for new purposes outside of the originally stated purposes is considered unlawful; unless Data Controller performs and passes a 'Compatibility' test for a new purpose to ensure that the data is still processed on the same 'lawful basis. There are also exceptions including further processing based on EU or member state law and further processing for public interest purposes. Purpose limitation is designed to ensure the confidentiality, reliability, and accuracy of personal data being collected and processed [162]. Preserving purpose limitation is of interest to Data Subject, ensuring the confidentiality of personal data, as well as safeguarding of the balance of powers between Data Subjects and Data Controllers [6].

Violation of this purpose limitation principle neglects personal privacy and might lead to various data privacy threats including *data misuse*, *data exploitation*, and *data breaches*. The fundamental purpose of this principle is to protect Data Subject's privacy from data misuse and data exploitation. For instance, Google has been found to unlawfully feed personal data to advertisers in violation of the purpose limitation principles and unclear data consent policies by the French data regulator [7]. This could go further than just a targeted advertisement, and the damage could be tremendous. Personal data could be processed for numerous illegitimate purposes including (e.g., by using inference attacks [163], [164]) to political campaigns [8].

4.2.3 Data Minimization

According to the principle of Data Minimization, only the required detail of personal data that is necessary for a specific purpose should be processed by the data controller. The data breaches would result in a violation of the data minimization principle. As H&M was fined (i.e., $41.4 million)

[5] https://www.tessian.com/blog/biggest-gdpr-fines-2020/

[6] https://migrationpolicycentre.eu/point-no-return-migration-and-crime/

[7] https://www.bbc.co.uk/news/technology-46944696

[8] https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/1791/179110.htm

for data breaches that occur due to violating the principle of data minimization [9].

If the data provided for processing is not minimized sufficiently, there would occur the privacy threats of Linkability and Identifiability [10]. Because the excessive availability of data [165] would let the attacker easily find and identify the two items of interest (IOI)s for the specific target. The violation of data minimization would also lead to data abuse [165] and inference privacy attacks (i.e., location privacy attacks, property inference etc.) [166].

4.2.4 Accuracy

According to the principle of Accuracy, the data provided for processing should be accurate and up to date. Organizations should ensure that the given data is correct and provide the option of erasure and rectification to DS for updating their personal data.

Failing to comply with the 'Accuracy' principle would lead to the processing of data with inaccurate and erroneous data. This would also mean not providing the right to erasure and rectification to the data subject. Therefore, the processing of data with inaccurate data would lead to data abuse and data exploitation [167], [168].

4.2.5 Storage Limitation

According to the principle of Storage Limitation, organizations should keep personal data until the purpose of processing is achieved. The personal data should be erased after the required processing. Thus, erasure from the storage is needed after the processing. The violation of the 'storage limitation' principle would lead to the linkability and identifiability [11] at the data store because data stored even after the purpose of processing is completed would let the attacker easily identify the two Items of Interests (IOI)s and link it to the targeted object (i.e, AC). The violation of storage limitation would lead to data breach incidents and undesired inference of data [169]. For instance, the data breaches [170] caused by privacy attacks include similarity attack, skewness attack, differential privacy attacks, homogeneity attack and background attack etc. [171], [172].

4.2.6 Integrity and Confidentiality

According to the principle of Integrity and Confidentiality, DC should ensure the secrecy and confidentiality of personal data. For integrity, the controller should maintain the 'accuracy and validity (consistency)' of the data. There should be the 'trustworthiness' of the data. For confidentiality, data should be protected from unauthorized access, theft, or disclosure of information.

The violation of the '*integrity and confidentiality*' principle would lead to the privacy threats of disclosure of information [12] and data theft because if the data is not secured any unauthorized user can get access to personal data which would lead to the disclosure of information. The violation of the principle of integrity and confidentiality would also lead to data privacy threats [173] of tempering and unauthorized alteration and destruction of data [174], [175].

4.2.7 Accountability principles

The Accountability principle asserts taking responsibility for whatever you do with the data of the DS. It also enforces showing how you comply with the other principles. Therefore, there should be appropriate measures and records to present the compliance with the GDPR.

The violation of the principle of accountability would lead to data breaches [176] and the privacy threat of non-repudiation [176], for which the subject would be held accountable if it is not able to repudiate a claim or action.

GDPR principles provide the compliance requirements that need to be adopted to reduce privacy threats [13]. The relation of data privacy threats with GDPR principles is illustrated in Table 6.

4.3 Role of the GDPR in data privacy threat modelling for autonomous system

Under the GDPR, organizations and institutions can provide data protection, ensure privacy risk management [177] and adopt proactive methods for advanced technology, particularly for Artificial Intelligence and Autonomous Systems (AS) [178]–[180]. Mark Coeckelbergh *et al.* have discussed the ethical and philosophical issues in Human-Autonomous Systems cooperation that have to be addressed by research, development and legal legislation [181]. Autonomous systems may perform any task which is ethically and legally prohibited under the data protection regulation [147]. Moreover, the regulatory frameworks of various countries [182] as Italy, Greece, and New Zealand are still at the initial stage of modelling AV's ethical, legal, and social challenges [183]. GDPR is rapidly integrating into AVs systems for data protection and management in the EU [182]. In [184], the authors suggested, based on the 'Data Minimization' principle of GDPR, AV should minimize the collection of personal data and remove the data after the purpose of processing has been completed. Inspired by GDPR, the authors in [185], suggested introducing the 'right to reparation' and accountability strategies for building trust and accountability in AS (i.e., AV) for unacceptable tasks.

The European Parliament's resolution on Civil Law Rules on Robotics [14] and the European policy debate on the GDPR showed how to deal with the challenges posed by robotics. In [186], the authors suggested implementing cybersecurity and safety regulation (i.e. Arts 25 and Art 32 in the GDPR) in Care Robots. This is because the personal data of the patients are processed by healthcare providers. In addition, among the principles of GDPR, the accountability mechanism has got an important focus which is termed as 'right to explanation'. The systems can make biased, discriminatory and unfair decisions that put people at risk [186]. For example, companion robot Papper [187], policing robot Knightscope [188] and Tesla Autonomous Cars [189], autonomously take decisions whether something is a car or a person on road, or something posing a threat to them. As a result, autonomous technology may take an undesirable decision that needs to be accountable, transparent, and explainable. The privacy and security challenges posed by AS

[9] https://www.bankinfosecurity.com/clothing-retailer-hm-told-to-wear-41-million-gdpr-fine-a-15111

[10] https://www.linddun.org/linddun-threat-catalog

[11] https://www.linddun.org/

[12] https://www.linddun.org/disclosure-of-information

[13] https://www.linddun.org/

[14] https://www.europarl.europa.eu/doceo/document/TA-8-2017-0051_EN.pdf?redirect

TABLE 6: Data privacy threats and related GDPR principles

Data Privacy threats	Description	Consequences	Related GDPR Principles
Linkability	Being capable to identify whether two items of interests (IOI)s are linked or not.	It can cause identifiability and inference about the particular subject.	Data Minimization
Identifiability	The subject can be identified easily within available set of subjects.	It causes severe privacy violations (when subject is assumed anonymous).	Data Minimization
Non-repudiation	Unable to deny a claim or an action.	If a subject is not able to repudiate claim/action, it can be held accountable.	Accountability
Detectability	The ability to distinguish if an item of interests (IOI)s exists or not.	Inference of a subject can be caused by the detection of an IOI.	-
Disclosure of information	This is referred to information disclosure of the subject.	This can lead the disclosure of personal information of subject.	Confidentiality
Unawareness	Not aware of impacts and consequences of sharing information.	This can lead to linkability and identifiability.	-
Consent non-compliance	The system/organization is compliant if it adheres to regulatory principle of transparency and take the user's consent.	This can make consent inconsistent.	Transparency

are reflected in GDPR's accountability mechanism. Therefore, GDPR's principles of 'Transparency' and 'Accountability' play important role in AI, Autonomous Systems and Robotics [190].

5 Data Privacy Threat Modelling for ACS

In this section, we are going to discuss how threat modelling techniques (i.e., STRIDE and LINDDUN) can be used to model the data privacy threats in a specific autonomous system namely Autonomous Car Systems (ACS). We examine the challenges and gaps when conducting these techniques for identifying data privacy threats by leveraging GDPR as the baseline.

5.1 Use-cases: Data Privacy threats in ACS

5.1.1 Overview of ACS

ACS is one of the milestone inventions in autonomous technology [191] including automotive capabilities based on LIDAR, Radar [192], [193] and machine learning algorithms. The successful implementation of ACS depends on both safety parameters (i.e., the effectiveness of the self-driving mechanisms, cyber-security and data privacy) and human trust [194]. ACS can only be practically deployed in the real world if it is trustworthy [195]–[197]. Along with technologies to ensure safety, there should be approaches to educate and enhance users' confidence and trust in ACS [194], [198].

Figure 4 [199], illustrates the main components of an ACS in which data acquisition is done by the radars, sensors, cameras, communication devices, and Light Detection and Ranging (LIDAR). Data collected by these devices are manipulated and processed by a central system of the Autonomous Car (AC), and then passed to a decision-support system which let the system perform a set of required tasks. To travel from point A to point B, AC perceives and gets awareness of the external surroundings, plans an appropriate route, navigates, and makes controlled movements.

Moreover, Figure 5 [199] is a simple illustration of the ACS in which AC communicates with other communicating nodes that include the Road Side Unit (RSU), Trusted Authority (TA)(i.e., registration and management authorities), and other connected AC for its fully implemented. Notably, AC communicates with RSU, other connected vehicles, and TA through VANET by LTE, WiFi, visible light communication etc. In ACS a vehicle (e.g., AC) interacts with another vehicle (V2V) [200], [201], and infrastructure (V2I) [202], [203] such as RSU and TA for sharing information (i.e., traffic information, safety warnings etc.).

Furthermore, one of the most serious issues in the automotive industry is the threat to security and privacy [199]. The researchers in [204] and [205] have examined numerous cyber-threats in autonomous vehicles. There are a variety of conventional security vulnerabilities in ACS such as the injection of malicious code into various sensors and telematics units [206], [207]; hacking into an in-car network

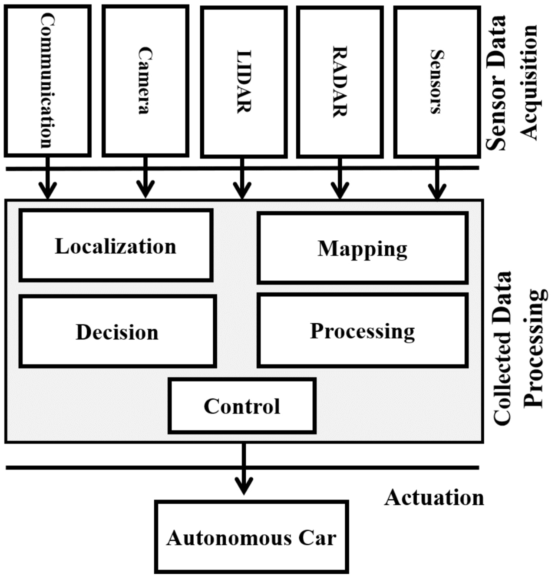


Fig. 4: AC Architecture

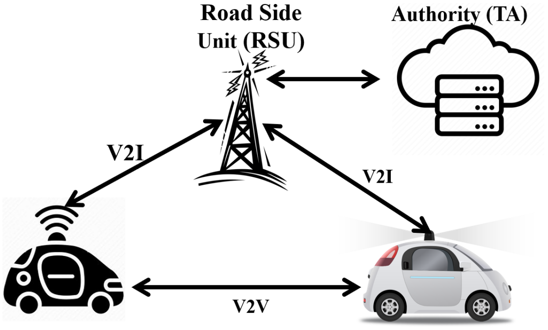


Fig. 5: Simple illustration of ACS

[208], [209]; external spoofing while communication [210]; packet fuzzing [211]; and jamming [212], [213]. Researchers have also demonstrated how an automobile may be readily hacked using a bus of Connected and Autonomous Networks (CAN) [214]. Furthermore, a car communicates with the other car through the CarSpeak mechanism for sharing sensory information [215] which should be protected for privacy concerns. In ACS, personal data is shared with infrastructure and other connected cars for multiple purposes (e.g., safety and value-added services), thus it is crucial to preserve the privacy and security of such data.

5.1.2 Data Privacy Threats in ACS

There are a large number of data privacy threats in ACS, as the system is collecting and processing heterogeneous personal and sensitive information from different sources such as RSUs, central base stations, and other ACs. In [216], the researcher presented the main challenges to safety and security in ACS by identifying various attacks. For example, Sensor Attack [217] occurs when an attacker attempts to disable the GPS by hacking the sensor installed on the car. An attack on VANET [218] is done when a hacker employs brute force to get access to a vehicle's confidential data (i.e., passwords or keys). The V2X attack [219] is held when the attacker attack any gadget (i.e., smartphone) through which a vehicle communicates to an external network by WiFi, Global System for Mobile or Bluetooth. The V2V attack [220] in which a distributed denial-of-service (DDoS) occurs by overpowering and manipulating the V2V communication. Moreover, GPS spoofing attacks occur when the attacker pretended to be the legitimate terminal in the GPS network and tries to access confidential data and pose significant damage to the network. This would let the attacker navigate the AC by spoofing the GPS and taking control of the car.

The AC is more computerized in generating a large amount of data. This system is more vulnerable to privacy concerns [221], since the autonomous industry pays less attention to monitoring and analyzing how data is collected and created by the AC. Third parties and hackers now have more opportunities to abuse the vehicle's data. A hacker can easily access the driver's personal information, the vehicle's location, the information of others in the car (such as passengers), or someone in the vicinity of the automobile.

As demonstrated in Figure 4, in AC, the obtained data from the sensors [217] can be used by organizations and third parties for location tracking. In self-driving cars, location data is primarily collected and used for route planning [222]. A data collection that correlates location and travel information (e.g., current area, goal, speed, course, date, and time) may reveal sensitive information about users. These concerns about personal safety exist on both a personal and societal level (Data Protection Report [15]).

Moreover, autonomous vehicles are ideal for acquiring information about different drivers' driving habits, goals, and other information without their consent. Additional issues could arise as a result of the vehicle's use of symbolism, such as ownership questions and potential intrusion of protection claims, depending on the situations in which the images are captured [222]. Similarly, an individual's information around AC (i.e, client's locations and on-street behaviour) may be useful to third parties such as the government and private sector entities, law enforcement, the news media, private specialists, and insurance companies.

TABLE 7: Security and privacy threats in ACS (ACS)

Security and Privacy attacks in ACS	Description
Fake information attack	An attacker sends false/fake information in ACS for his interests. For instance, an attacker could transmit the emergency vehicle approach warning of getting a clear road.
Integrity attack	The attacker tempers the messages in a network for threatening the integrity of the communication link.
Message replay attack	The legitimate messages that sent already by the authenticate sender are sent again for malicious intentions (i.e., to create a delays to disrupt the traffic).
Repudiation attack	It is held when any message/consent send by the malicious vehicle later deny the message or information send by it.
Privacy attacks	This would lead a attack on AC sensitive information(i.e., identity of vehicle, driver, passenger, vehicle owner; driving style; geographical location; mileage; or car's technical data) from invalid entities.

5.2 Threat Modelling Techniques for ACS

Threat modelling plays a crucial role in identifying and mitigating the threats in ACS. This section provides systematic approaches for modelling potential threats in ACS by leveraging STRIDE and LINDDUN techniques [52].

5.2.1 Modelling Data Privacy Threats in ACS using STRIDE

The STRIDE approach consists of nine steps to model threats in ACS. Step-1: define the use-case scenarios: We identify the potential security and privacy threats for our use-case scenario (i.e, ACS) [199]. Step-2: gather a list of external dependencies: we identify that an AC operates in a communication network in which AC communicates with other ACs, Road Side Units (RSUs), and a central operation server called Trusted Authority (TA) [199]. Step-3: define security assumptions: we have analyzed that in ACS, there would be not only security threats but also privacy vulnerabilities which need to be mitigated. The security and privacy attacks in ACS are shown in Table 7 [52].

Step-4: create external security notes. As ACs operate with other connected entities in a communication network, there are external security and privacy concerns related to RSUs, TA, and other connected vehicles such as spoofing of AC and RSU etc. as presented in Table 7. Step-5: create DFDs of the system based on logical and structural entities. We illustrate the DFD of the ACS in Fig. 6 which will be discussed throughout this paper. In DFD, there is AC, Road Side Units (RSU), Trusted Authority (TA), and the data flow between these entities. In this DFD, ACS consists of V2V and V2I data flow (i.e., communications), where an AC shares its data (i.e., location, speed, route, or any danger/threat etc) with other ACs and RSUs. The information is further transmitted from RSUs to the TA, which is responsible for the registration of the vehicle (i.e., generating certificates), the revocability of the vehicle, as well as the information

[15] https://www.dataprotectionreport.com/2017/07/the-privacy-implications-of-autonomous-vehicles/

TABLE 8: Mapping STRIDE Threats

Security threat	Security property	AC	RSU	TA	DF
Spoofing	Authentication	×	×	×	
Tempering	Integrity	×	×	×	×
Non-Repudiation	Repudiation	×	×		
Information Disclosure	Confidentiality	×	×	×	×
Denial of Services	Availability	×	×	×	×
Elevation of Privilege	Authorization	×			

storage. The AC, RSU and TA are represented as processes in DFD. The dotted red line indicates the trust boundaries around TA which are assumed to be trustworthy in this scenario.

Step-6: determine the types of threats. STRIDE's taxonomy of threats is used to highlight the security threats in a system namely Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service and Elevation of Privilege. These threats are found against the security requirements such as Authentication, Integrity, Non-repudiation, Confidentiality, Availability, and Authorization respectively. Step-7: identify the threats to the ACS. Each entity and process in a DFD is mapped to a set of threats. Table 8 shows the mapping of security threats on various elements of DFD (marked with ×).

In this paper, we have illustrated the threat tree pattern of only Spoofing with ACS, as shown in Figure 7. The oval (or circle) shape in the threat tree shows the root threat that may lead to other possible threats. The rectangle represents the concrete threat in the attack path. Step-9: determine and prioritize the risks. For each identified threat, the security risks are determined and prioritized for their resolution in ACS. Step-9: plan mitigation. In this final step, the risks of the identified threats are minimized by suggesting the appropriate mitigation approaches. Table 9, illustrates the risk priority and mitigation approaches of some possible security threats in ACS.

We discuss each threat specified by STRIDE separately which applies to the elements of the DFD of AC with mitigation approaches:

Spoofing: Spoofing with AC is attempted by tricking cameras, sensors, and receivers with wrong information (i.e., false notifications or fake signals) to change the recipient Car's behaviour or decision [228]. When an AC communicates in a network, an attacker/malicious vehicle may spoof the GNSS [229] and GPS's of the AC that attempts to impersonate it [228]. Moreover, a malicious vehicle may impersonate an RSU for distracting an AC. An attacker spoof the GPS and tempers the Basic Safety Massage (BSM) and lets the other AC accept the fake message that comes from the authenticate source [223].

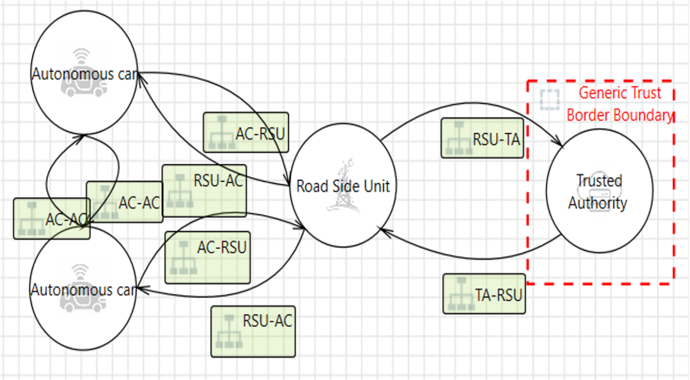


Fig. 6: DFD-ACS showing data flowing between AC, RSU, and a trusted centralised server TA.

Tempering: In ACS, the integrity of confidential information of AC (i.e. license plate) recorded by TA is important as it is responsible for providing maintenance with updating certificates, and keys and obtaining fresh Certificate Revocation List (CRL). The exchange of messages (i.e. location detail, speed, traffic congestion etc.) between AC, another vehicle, and RSU may be tempered/modified. Data signature can be used for information and integrity [224], [225].

Non-repudiation: The AC cannot deny the message it has already transmitted because the registered authority has logged it (i.e., TA). The denial of a node in communication would result in the loss of event traceability.

Information Disclosure: When an AC communicates with other entities in a network, information is exposed due to unsecured message transmission. For safe message transmission in a network, [226] suggests the Secure Message Transmission (SMT), NMD routing protocol with MAC, and asymmetric cryptography solutions.

Denial of Services (DOS): When an attacker generates jamming in a physical channel of a communication network, the data/message becomes unavailable or delayed. To mitigate DOS [227], availability and authentication must be met.

Elevation of Privileges (EoP): The RSU can grant services to an authorized AC who makes a request. If the RSU fails to validate the authorized vehicle, privileges may be elevated. In [230], the authors developed a strategy for preventing EoP in a communication network.

STRIDE is an appropriate approach for identifying some specified security threats (i.e. Spoofing, Tempering, Non-repudiation, Information Disclosure, Denial of Services, and Elevation of Privilege) in the ACS. However, STRIDE failed to deal with the data privacy threats in ACS as defined in Table 6.

5.2.2 Modelling Data Privacy Threats in ACS using LINDDUN

In this subsection, data privacy threats for ACS are modelled using LINDUNN technique, which consists of 6 processes as indicated in Figure 8 [33].

Step-1: The DFD of the ACS is constructed for modelling the system as illustrated in Figure 6. Step-2: we

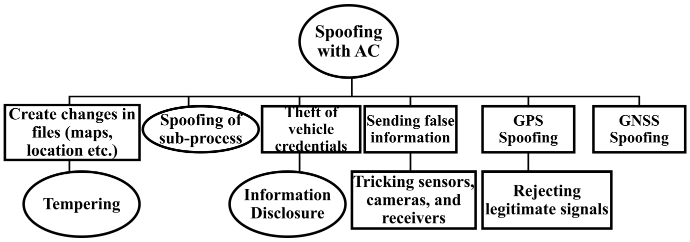

Spoofing with AC
Create changes in files (maps, location etc.)
Spoofing of sub-process
Theft of vehicle credentials
Sending false information
GPS Spoofing
GNSS Spoofing
Tempering
Information Disclosure
Tricking sensors, cameras, and receivers
Rejecting legitimate signals

Fig. 7: Spoofing with AC

TABLE 9: Prioritization of risks and mitigation approaches based on STRIDE

Title	Category	Description	Priority	Mitigation /Justification
Spoofing the AC, and RSU	Spoofing	AC and RSU may be spoofed by an attacker, and this may lead to Information Disclosure.	high	Standard authentication mechanism must be implemented to identify the valid processes. [223].
Spoofing TA	Spoofing	TA may be spoofed by a malicious vehicle or an attacker.	low	TA is assumed trustworthy, so there are less chance of Spoofing TA.
Tempering of AC, and RSU and DF	Tempering	Data flowing across Data Flow may be tampered by an attacker. This may lead to a denial-of-service, elevation of privilege, or information disclosure attacks against AC, RSU. For example, fake information attack, illegal pre-emption attack.	high	Integrity must be maintained; Data signature can be used for integrity [224], [225].
Tempering of TA	Tempering	TA may be tempered by a malicious vehicle or an attacker.	low	TA is assumed as trustworthy, there are less chance of tempering TA.
Data Repudiation of AC	Non-Repudiation	AC claims that it did not receive data from a source outside (i.e., RSU).	medium	Logging and auditing are required.
Information Disclosure of Data Flow	Information Disclosure	Data flowing across Data Flow may be sniffed by an attacker. Depending on what type of data an attacker can read, it may be used to attack other parts of the system or simply be a disclosure of information leading to compliance violations.	high	Encryption of data flow must be implemented; secure message transmission (SMT), NMD routing protocol with MAC and asymmetric cryptography solutions are suggested for secure message transmission in a network [226].
Potential Process Crash (AC, RSU)	DoS	AC and RSU crashes, halts, stops, or runs slowly; in all cases violating an availability metric.	high	Availability mechanism must be applied [227].
Potential Process Crash (TA)	DoS	TA may be attacked by external attacker.	low	Availability mechanism must be applied [227].
Data Flow potentially interrupted	DoS	An external agent interrupts data flowing in either direction. This further lead to denial of services for AC, TA, and RSU. For example, replay attack.	high	Availability mechanism must be applied [227].
AC may be Subject to Elevation of Privilege	Elevation of Privilege	Malicious vehicle/attacker may be able to impersonate AC to gain additional privilege from RSU.	high	Authorization should be applied.

TABLE 10: Mapping LINDDUN threats on DFD-ACS

DFD Elements	Threat Targets	L	I	N	D	D	U	N
Data Flow	AC data stream (AC-AC)	×	×	×	×	×	×	×
	AC data stream (AC-RSU)	×	×	×	×	×	×	×
	RSU data stream (RSU-TA)	×	×	×	×	×		×
Process	Road Side Unit (RSU)	×	×	×	×	×		×
	Trusted Authority (TA)							×
Entity	Autonomous Car (AC)	×	×	×	×	×	×	×

mapped the LINDDUN privacy threat types i.e, Linkability, Identifiability, Non-repudiation, Detectability, Disclosure of information, Unawareness, and Non-compliance with the elements of DFD-ACS.

Table 10 illustrates the mapping of LINDDUN threats on DFD of AC System. An attacker or a malicious vehicle, for example, can detect the two Items Of Interest (IOI)s (i.e, speed and location of AC) in a system at any time to trace or monitor the vehicle. Following the Linkability, an attacker can identify the targeted AC and continue to pursue his harmful goals. Detectability happens when an attacker/malicious vehicle determines whether the IOIs exist in ACS to obtain his interests. Furthermore, a misbehaving AC cannot deny that it has engaged in any specific activity in the case of non-repudiation (i.e. sending any malicious message). If the AC repudiates the violent behaviour, it will be held liable.

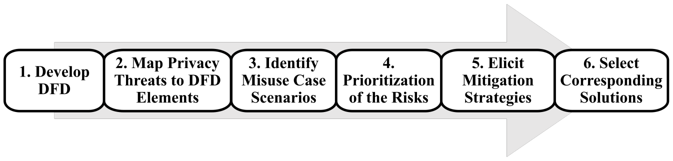

1. Develop DFD
2. Map Privacy Threats to DFD Elements
3. Identify Misuse Case Scenarios
4. Prioritization of the Risks
5. Elicit Mitigation Strategies
6. Select Corresponding Solutions

Fig. 8: 6-step procedure in LINDDUN to model privacy threats.

Moreover, The theft of confidential data of the AC (i.e., pseudo-identity) can lead to the threat of Disclosure of Information (DoI). the threat of 'Unawareness' in ACS, refers to the unawareness of the driver/owner and passenger, about how their data is being captured, shared, or manipulated. In addition, non-compliance highlights the lack of the proper integration of privacy policies in the ACS. An attacker may tamper with the privacy principles and make AC's consent inconsistent. For example, an attacker or third party may use the personal data of the car for his interests without the consent of the driver, owner, or passenger.

Step-3: The misuse of AC for Linkability is illustrated in Figure 9. Linkability of AC is the root threat that may lead to Identifiability, Detectability, and Disclosure of information. If the personal data (i.e. pseudo-identity and location) of AC is not protected, then the attacker can easily track and identify the current location of the car, resulting in the disclosure of information about the AC. Step-4: The risks identified in the ACS are prioritized with a number (1-12) in Table 11, which should be mitigated accordingly. The items indicated with 12* mean that non-compliance and consent threats have an effect on the ACS (DFD) as a whole. The threats marked with '×' are considered as not related to the ACS.

Step-5: the privacy requirements are elicited across the entities of the DFD of the ACS against the LINDDUN threats

TABLE 11: LINDDUN potential threats on DFD-ACS

DFD Elements	Threat Targets	L	I	N	D	D	U	N
Data Flow	AC data stream (AC-AC)	2	5	×	×	9		12*
	AC data stream (AC-RSU)	3	6	×	×	10		12*
	RSU data stream (RSU-TA)	×	×	×	×	×		12*
Process	Road Side Unit (RSU)	×	×	×	×	×		12*
	Trusted Authority (TA)							12*
Entity	Autonomous Car (AC)	1	4	7	×	8	11	12*

TABLE 12: LINDDUN privacy requirements & DFD entities

Threats	DFD Entities	Privacy Requirements
Linkability	AC, AC-AC, AC-RSU	Unlinkability
Identifiability	AC, AC-AC, AC-RSU	Pseudonymity/ anonymity
Non-repudiation	AC	Plausible deniability
Detectability	AC, RSU, DF	Undetactability
Disclosure of Information	AC, RSU, DF	Confidentiality
Unawareness	AC	Awareness of content
Non-compliace	AC, RSU, TA, DF, DS	Consent and regulatory compliance

in Table 12. Unlikability [231] is meant to break or remove the link between any two IOIs. For example, two different locations visited by the same vehicle, two different accidents are done by the same miss behaving car etc. Anonymity [231] is another privacy security requirement that is provided by removing the link between actions, information or identity. Moreover, plausible deniability [232] shows that no one can prove that an individual has done something. Undetectability is the opposite of detectability which assures that no one can detect the two IOIs. For eliminating the threat of DoI, confidentiality [233] is important to be maintained. Furthermore, the awareness of the content and providing consent and regulatory compliance to the system as a whole is important to preserve the privacy of the system [234].

Step-6: we suggest the desired solutions for the identified threats in ACS. Table 13, summarizes the suggested strategies and mitigation approaches for the identified threats in our use-case scenario.

LINDDUN is used for modelling some specified privacy threats of an ACS. It does not guarantee to deal with the other privacy threats, for example, non-compliance with data minimization, non-compliance with storage limitation, un-accountability etc. as discussed in the following section.

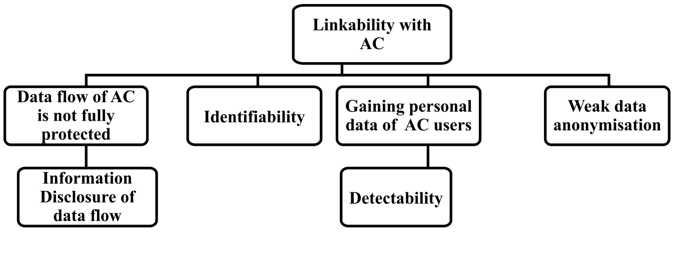

Linkability with AC
Data flow of AC is not fully protected
Identifiability
Gaining personal data of AC users
Weak data anonymisation
Information Disclosure of data flow
Detectability

Fig. 9: Linkability threat tree

5.3 Detailed Challenges in modelling data privacy threats in ACS

As GDPR Principles provide the finest foundation for assuring data protection and privacy in a system, we will utilize them as a baseline to analyze STRIDE and LINDDUN concerning their capabilities in modelling data privacy in ACS.

5.3.1 Comparison between threat modelling techniques for ACS

Table 14 presents the comparison of the threat model using STRIDE and LINDDUN in accordance with the GDPR principles, individual rights, and other requirements. We use the GDPR as the baseline for comparing STRIDE and LINDDUN, which consists of 7 principles and requirements (e.g. individual rights and international transfer). If one of the requirements of a principle is not covered by a modelling technique, then the main principle is not covered. LINDDUN is 37% providing compliance with GDPR as it is mapped with 6 principles. And STRIDE provides 12% GDPR compliance because it is mapped with only 2 principles.

GDPR Principles: The comparison of STRIDE/LINDDUN based on GDPR principles [242], and the identified gaps are discussed below:

1) **Lawfulness, Fairness and Transparency:** The privacy requirements of awareness and compliance mentioned in LINDDUN do discuss the consent. But it does not provide any reference about AC users' (i.e. owner/driver and passenger) ability to update/withdraw and view consent; and AC users' consent for sharing data with third parties. On the other hand, STRIDE does not define any threat to processing the data based on lawfulness. Moreover, LINDDUN and STRIDE do not provide any description for processing the AC's users' data on a lawful basis which includes: legitimate interests, contract, legal obligation, vital interest, and public interest. Similarly, LINDDUN and STRIDE do not provide any reference to the principle of fairness and transparency. Thus, these two modelling approaches do not deal with the compliance threats of un-lawfulness, unfairness, and non-transparency.
2) **Purpose Limitation:** In LINDDUN and STRIDE, we do not find any reference regarding purpose limitation, hence these techniques do not cover this principle. Therefore, STRIDE and LINDDUN do not address the non-compliance threat of 'violating the purpose limitation'.
3) **Data Minimization:** LINDDUN has a reference to data minimization, under the threat tree of Linkability and Identifiability. However, LINDDUN does not include any direct privacy targets/countermeasures or Privacy Enhancing Techniques (PET) to address data minimization, which is regarded as a gap/challenge. STRIDE, on the other hand, shows no evidence of adhering to this principle. As a result, there is a threat of 'non-compliance with data minimization, which must be addressed.

TABLE 13: Strategies and mitigation approaches for threats in ACS

No.	Threats in Autonomous Car System (ACS)	Privacy Requirements	Suggested strategies and mitigation approaches
1	Linkability of AC	Unlikability of vehicle information such as location, speed, driving behavior.	Applying the data anonymization methods, such as k-anonymity [235].
2	Linkability of data flow of the AC data stream (AC-AC)	Unlinkability of messages/ information of AC-AC data stream, channel confidentiality.	Applying the data anonymization methods, such as Quasi-identifier, QID [236].
3	Linkability of data flow of the AC data stream to RSU (AC-RSU)	Unlinkability of messages/ information of AC-RSU data stream, link confidentiality.	Applying the data anonymization methods, such as Quasi-identifier, QID [237].
4	Identifiablity at the AC	Anonymity of the vehicle users (i.e., drivers, passengers, owner etc.).	Using anonymisation technique; de-identification can be employed to remove personal information of the AC's users [238].
5	Identifiability at data flow of AC data stream (AC-AC)	Anonymity of ACS users such that the users will not be identified from AC-AC communication by content; link confidentiality.	Applying anonymity of AC-AC communication link [239].
6	Identifiability at data flow of AC data data stream to RSU (AC-RSU).	Anonymity of ACS users such that the users will not be identified from AC-RSU communication by content; link confidentiality.	Applying AC-RSU link confidentiality [240].
7	Non-Repudiation at AC	Plusiable repudiation	Maintaining privacy and having plausible repudiation AC. [241]
8	Disclosure of Information at AC	Confidentiality of the AC data should be ensured.	Apply the anonymity system at AC; applying confidentiality of cryptographic keying in AC [198].
9	Disclosure of Information of data stream (AC-AC)	Confidentiality of the communication between AC-AC should be maintained.	Applying anonymity and confidentiality of AC-AC communication link [239].
10	Disclosure of Information of data stream (AC-RSU)	Confidentiality of communication between AC-RSU should be maintained.	Applying the data anonymization and confidentiality methods, such as Quasi-identifier, QID [237].
11	Unawareness at AC	AC users should know about how their data is collected, shared and manipulated; require data minimization.	Providing information about exercising different user rights to maintain its personal data [182]; Use feedback tools to raise user's privacy awareness.
12	Policy and consent non-compliance of the ACS	ACS need to be compliant with legal guidelines for data protection.	Employee GDPR regulatory compliance framework for ACS; penalised the system if the processing of the user's personal is done without user's consent.

TABLE 14: Modelling threats using LINDDUN & STRIDE in accordance with the GDPR

GDPR Principles and Requirements	STRIDE	LINDDUN
I. GDPR Principles		
1. Lawfulness, fairness, and transparency	No	No
1.1 Consent	-	X
1.2 Legitimate Interests	-	-
1.3 Contract	-	-
1.4 Legal Obligation	-	-
1.5 Vital Interests	-	-
1.6 Public Interests	-	-
2. Purpose Limitation	No	No
3. Data Minimization	No	Yes
4. Accuracy	Yes	Yes
5. Storage Limitation	No	Yes
6. Integrity and Confidentiality	Yes	Yes
7. Accountability	No	No
II. Data Subject Rights		
a. Right to be Informed	No	Yes
b. Right of Access	No	Yes
c. Right to Rectification	No	No
d. Right to Restrict Processing	No	No
e. Right to Data Portability	No	No
f. Right to Object	No	No
g. Right to Automated Decision Making	No	No
h. Right to Erasure	No	No
III. International Transfer	No	No

4) **Accuracy:** In LINDDUN, we get references about Accuracy under the threat tree of Unawareness. It also provides a solution for enhancing accuracy by allowing users to delete, update, or review data. In STRIDE, we get a reference of Accuracy/update data under the threat of Tampering, which requires Integrity as a security requirement. Thus, both approaches cover the Accuracy principle.
5) **Integrity and Confidentiality:** LINDDUN and STRIDE define the threat of Disclosure of Information, which has the security requirements of Integrity and Confidentiality. Hence, the principles of Integrity and Confidentiality are covered by these two approaches.
6) **Storage Limitation:** Under the Linkability of a Data Store Threat Tree, LINDDUN displays the potential threats that can arise as a result of storing data for an extended period of time or storing an excessive amount of data. So, we get the reference of storage limitation/retention time in LINDDUN. Furthermore, there is no mention of Storage Limitations in STRIDE. As a result, while modelling using STRIDE, there is a risk of 'non-compliance with the storage limitation' in ACS.
7) **Accountability:** In the use-case of the ACS, the accountability would be held by a Trusted Authority

(TA), which would generate revocation/or cancellation of the certificate for the misbehaving AC. LINDDUN does not define any threat related to Accountability. However, it refers to Accountability indirectly, under the Content Unawareness threat tree. Similarly, STRIDE makes no security requirements for Accountability and does not address any threats associated with it. As a result, the threat of 'non-accountability' is not addressed by both modelling techniques.

Data Subject Rights: The GDPR requires ACS to implement a variety of Data Subject rights to be compliant with the legislation and to protect Data Subjects from numerous data breaches, data exploitation, and data abuse.

1) **Right to Informed:** LINDDUN refers to the compliance requirement of this principle under the threat tree of Unawareness and Non-compliance. But STRIDE does not provide any reference to cover this right. In LINDDUN, under the Unawareness threat tree, there is a leaf node 'unable to review personal information that refers to the right to access. But this right does not directly mention if there is physical access to data or just reviewing the data. There is also a reference of DS to not being able to modify or remove data under the Non-repudiation of the data store threat tree. Moreover, STRIDE does not cover the Right to access, as it does not define any threat related to this right.
2) **Right to Rectification:** Neither LINDDUN nor STRIDE include any references or security/privacy requirements for the Right to Rectification. As a result, both modelling approaches fail to respect the right to rectification.
3) **Right to Erasure:** LINDDUN does not directly define the threat to the right to erasure. It does, however, appear in the Non-repudiation of a Data Store threat tree, where the user is unable to erase their own data. Because this right is not explicitly described in LINDDUN, it is assumed that it is not covered. Similarly, STRIDE does not have any reference related to this right. Thus, both modelling approaches fail to respect the right to erasure.
4) **Right to Restrict Processing:** In both LINDDUN and STRIDE, there is no description/reference of any privacy threat or countermeasure related to the right to restrict processing. Thus, this right is not covered by STRIDE and LINDDUN.
5) **Right to Data Portability:** This right is not covered by STRIDE and LINDDUN, as there is no description or reference related to the right to data portability in these two modelling approaches.
6) **Right to Object:** In both LINDDUN and STRIDE, there is no reference to any privacy threat, related to the right to object. Thus, this right is not covered by STRIDE and LINDDUN.
7) **Right to Automated Decision and Profiling:** This right is not covered by STRIDE and LINDDUN, as there is no description or reference related to the right to an automated decision and profiling in these modelling approaches.

International Data Transfer: The compliance requirements of International data transfers in ACS are intended to ensure that the controller/processor complies with the GDPR. However, neither LINNDUN nor STRIDE address the threat of 'Non-compliance of international data transfer'.

5.4 Challenges in modelling the GDPR compliance

LINDDUN and STRIDE failed to model non-compliance threats of un-lawfulness, unfairness, and non-transparency, as they do not meet the compliance requirements of lawfulness, fairness, and transparency for processing the AC and its user's personal data. The non-compliance threat of un-lawfulness occurs when the processing of personal data invalidates any lawful basis. Consent non-compliance [16], for example, occurs when trusted authorities fail to obtain the consent of AC's users (i.e., the driver/owner and passenger) before processing and sharing sensitive data with third parties, as well as when users are unable to update, view, or withdraw consent while their data is being processed. Similarly, neither LINDDUN nor STRIDE mention any compliance requirements for another lawful basis of data processing, such as legitimate interest, contract, legal obligation, vital interest, or public interest. Any lawful basis for data processing can be used to process the data of the ACS. For example, if a malicious AC causes an accident, data processing can be based on 'vital interest'. However, neither LINDDUN nor STRIDE address the threat of "not respecting vital interest". As a result, there is a gap in both LINDDUN and STRIDE to cope with the compliance threats of un-lawfulness, unfairness, and non-transparency.

Moreover, STRIDE and LINDDUN modelling techniques lack the privacy/compliance requirements to ensure the principle of 'Purpose limitation'. For example, the data of ACS collected for vehicle management should not be used to share with third parties (i.e., the insurance company - Direct Line Group (DLG)). Likewise, these two modelling approaches do not provide any reference to the compliance requirement of 'data minimization. For example, service providers and data processors (such as RSU, TA, and Uber) should only keep as much data as is required to process it for a specific purpose. LINDDUN and STRIDE also do not meet the 'storage limitation' compliance requirements, which assert holding the data until the purpose of processing is completed. Thus, LINDDUN and STRIDE failed to deal with the non-compliance threats of 'violating of purpose limitation'; 'non-compliance with data minimization'; and 'non-compliance with storage limitation'

Another challenge and gap in LINDDUN and STRIDE modelling techniques are that they do not deal with the compliance threat of 'unaccountability'. In our use-case of the Autonomous Car (AC) system, the principle of 'Accountability' plays a crucial role. Because if AC misbehaves or does any accident, then AC's users (i.e. driver/owner) should be accountable and explainable for this act. For example, In the case of collision and emergency, the AC's owner/driver would be accountable and explain this act [182]. Extensive research is going on the accountability [182], [191], [243] of the autonomous vehicle but none of the exist-

[16] https://www.linddun.org/

ing threat modelling techniques (i.e., LINDDUN/STRIDE) have covered this principle of GDPR.

The compliance requirements for the 'international transfer' of personal data are not guaranteed by LINDDUN and STRIDE. For example, the consent of AC users should be obtained before personal data is transferred for cross-border road safety investigations or commercial purposes (i.e., EU-US privacy shield C/2016/4176) [244].

Furthermore, there is a gap in LINDDUN and STRIDE to meet the compliance requirements of individual rights (Art.12-23). In the ACS, the users of the car should be able to exercise their right to rectification, right to update, right to object, and right to restrict its data processing. For example, it is the right of AC's users to know how their data is gained, stored, shared, and processed (Art. 13, 14 GDPR). The users of the AC may want to access its data from the TA or other data processors where it can exercise its 'right to access' (Art. 15 GDPR). Similarly, these two modelling methods are not respecting the 'right to rectification'; 'right to restrict processing '; right to object', 'right to data portability'; and 'right to automated decision making'.

5.5 Unsolved challenges and solutions for threat modelling techniques

Research directions and suggested solutions for the identified challenges are presented in Table 15. For processing the personal data in ACS and its users, the compliance requirements of the Purpose Limitation (Article 5 (1) (b)), Data Minimization (Article 5(1)(c)) and Storage Limitation (Article 5(1)(e)) should be integrated into a threat modelling approach for ACS. A framework should be developed for the ACS to check whether its users' data collected for one purpose should not be used for any other purposes [244]. Notably, the consent verification framework should be used to ensure that the consent of DS should be taken as a lawful basis for using the same recorded data for any other purpose. The compliance requirements of legitimate interests may also be incorporated into the modelling approach for processing the data. For example, the confidential data (i.e., real identity) of the ACS can be used by TA to create a revocation list for a misbehaving car based on the legitimate interests of data processing.

Similarly, the mechanism for Data Minimization should be implemented to ensure that a system is not collecting irrelevant information and respecting the purpose of processing [246]. Moreover, the requirements of Storage Limitations would also be implemented in the modelling approach for dealing with storage-related threats (linkability, identifiability etc.) in the ACS. The secure and required data storage/management may be implemented by employing an EDR/AD solution which is a regulatory prerequisite for the deployment of ACS [247].

It is essential to incorporate the principle of Accountability in a modelling method for the ACS [243]. Because the actions and interactions of ACS in the real-time environment are non-deterministic due to their high complexity and scalability. The AC should be comprehensible and trustworthy for its successful implementation in the real world [249]. For example, if an AC does an accident or misbehaves then its owner/driver should be accountable for it and should provide an explanation for doing so. Moreover, the compliance requirements of International Transfer should be implemented in modelling the ACS, because data protection is necessary while cross-border experiments on road safety and connectivity by digital technologies (i.e., EU-US Privacy Shield C/2016/4176) [244]. Furthermore, for securing the confidential data of AC(i.e, owner/driver and passenger), Integrity and Confidentiality should be incorporated into the modelling approach by employing authorization mechanisms [248]. The pseudonymization and encryption techniques should be implemented while communicating with messages (i.e., hash-based message authentication) in a network [250].

The users of ACS should be able to exercise the rights that are defined in GDPR for enhancing transparency and ensuring the protection of data. For example, the right to access, right to rectification, right to erasure the data (i.e., static road data (article 4), dynamic road data (article 5) and traffic data (article 6) defined by Delegated Regulation (EU) 2015/962) should be implemented in ACS. The privacy rights framework would also be implemented in the automotive industry. There are also some recommendations for the right to explanation and right to reparation [243] that may be included in the list of DS rights of the GDPR for ACS.

6 Recaps and Outlook

Recently, the misuse and abuse of personal data is blooming dramatically, resulting in serious data privacy concerns. Such concerns are particularly critical in the scenarios of AS (e.g., ACS) in which the operation of the systems are dependent on the processing of the data and without human intervention and verification. The increasing of ACS such as Tesla with autopilot autonomous driving function [251], [252] triggers the attention to a variety of privacy-related aspects, not only for conventional privacy preservation but also algorithm bias, ethics, and legal responsibility when processing personal data. This leads to a critical demand for a novel data privacy modelling technique as well as a GDPR-compliance verification scheme.

6.1 Conclusion

We have surveyed the existing threat modelling techniques with consideration for the applicability of these techniques when modelling data privacy threats in autonomous systems. We have argued that complying with the GDPR plays a bigger role in preserving users' privacy and protecting personal data compared to modelling data privacy threats, which only consider typical privacy-related attacks. Following this catalyst, we have provided an analysis of whether such techniques can relate the data privacy threat modelling to the GDPR-compliance. We have taken a specific use-case of AS, namely ACS, as an instance to demonstrate the analysis of STRIDE and LINDDUN when modelling the data privacy in ACS. We have also discussed the challenges and gaps, as well as provided suggestions for a novel modelling technique that not only models the traditional data privacy threats but also effectively performs the GDPR-compliance verification.

TABLE 15: Suggested solutions for unsolved challenges for Compliance requirements of ACS

Unsolved challenges for modelling GDPR-compliance for ACS	Suggested solutions
Unable to figure out unlawful/unfair/non-transparent data collection and processing	1. RSU, TA, and other service providers should be transparent, fair, and non-discriminatory to offer services to the ACS. 2. The mechanism to check whether implementation of a consent manager existed in ACS [244]. 3. Consent verification framework for ACS may be implemented [245].
Unable to figure out how data is processed (for what purpose) in ACS (fail to check Purpose Limitation compliance)	The mechanism to check Purpose Limitation (Article 5(1)(b), Article 89(1)) compliance in ACS [244].
Unable to figure out whether collected data is adequate, relevant and limited to the specific purposes (fail to check Data Minimization compliance)	A framework to check that not collecting and storing too much AC's users information with respect to purpose of processing. [246].
Unable to figure out whether collected data is stored for longer period needed or deleted (fail to check Storage Limitation compliance)	1. The technique to assure that the data should only be retained until the purpose of processing is fulfilled. 2. Ensure the secure and required data storage and management by employing EDR/AD solution which is a regulatory prerequisite for deployment of ACS [247].
Inability of securing confidential data and providing integrity in ACS	1. Employing the integrity and confidentiality compliance requirements in a threat modelling technique. 2. Preservation of privacy/personal data of AC(i.e., vehicle identity, location, speed, driving behavior etc.) and its users (i.e., driver/owner and passenger). 3. Integrity and Confidentiality should be implemented by employing authorization techniques (i.e., pseudonymization) [248].
Unable to figure out cross-border data transfer in autonomous industry (fail to check International Data Transfer requirement)	1. Integrating the compliance requirements of International data Transfer in a modelling technique for ACS. 2. Adopting the intelligent transport system (ITS)Dir 2010/40/UE with delegated regulations in modelling approach. 3. A framework for implementing the protection of personal data in electronic communications (privacy and electronic communication directives 2002/58/EC) for ACS [244].
Unable to incorporate data subject rights in ACS industry (fail to check an ACS implement DS rights as required)	1. Incorporating the data subject (i.e., owner/driver and passenger) rights (Art. 12-23) for ACS for preserving the privacy of its personal data and ensuring road safety [182]. 2. A modelling approach with Rights to explanation and rights to reparation [243] may be included in the list of other DS rights of GDPR.

6.2 Future Research Directions

To preserve data privacy and prevent personal data from data misuse and data abuse effectively, a data privacy modelling technique should take the GDPR-compliance into consideration rather than focus only on modelling conventional privacy threats. To develop such a technique, the GDPR principles and requirements are leveraged as the baseline and incorporated into the technique knowledge-based. This is based on the analysis and results of extensive empirical studies on the GDPR. For instance, an extensive knowledge-base of the first GDPR principle (i.e., Lawfulness, Fairness, and Transparency) should be included in the knowledge-base as a part of a *non-compliance threat tree catalogue* with the associated threat description so that the analyst of data privacy and non-compliance threats are easily traced and examined. This enables the compliance verification and enforcement of the GDPR. For example, in ACS, the DS and DP should take consent from ACS end-users for processing their personal data [244]. Furthermore, communication networks, RSUs, TAs and other service providers should be operated in a transparent, fair, and non-discriminatory manner offering their services to any AC. Therefore, a novel modelling technique should develop a model for inspecting a legal basis for processing data, along with mechanisms for justifying transparency and fairness [244], [253].

Another important research direction to develop a novel modelling technique for data privacy and GDPR-compliance is to re-design the system model based on the traditional Data Flow Diagram used in most of the existing techniques like STRIDE and LINDDUN. In this respect, the re-designed Data Flow Diagram does not necessarily include all system components but the GDPR roles. In other words, DS, DC and DP can be a part of the data flow diagram besides some of the system components; and some components could also play the role of a DS, DC or DP. This will illustrate the movement and processing of personal data in the system effectively and enable the modelling technique to analyse any systems following the GDPR requirements.

References

[1] M. I. Jordan and T. M. Mitchell, "Machine learning: Trends, perspectives, and prospects," *Science*, vol. 349, no. 6245, pp. 255–260, 2015.

[2] N. B. Truong, K. Sun, G. M. Lee, and Y. Guo, "Gdpr-compliant personal data management: A blockchain-based solution," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 1746–1761, 2019.

[3] F. Doshi-Velez and B. Kim, "Towards a rigorous science of interpretable machine learning," *arXiv preprint arXiv:1702.08608*, 2017.

[4] M. Ananny and K. Crawford, "Seeing without knowing: Limitations of the transparency ideal and its application to algorithmic accountability," *new media & society*, vol. 20, no. 3, pp. 973–989, 2018.

[5] F. Harder, M. Bauer, and M. Park, "Interpretable and differentially private predictions." in *AAAI*, 2020, pp. 4083–4090.

[6] A. Adadi and M. Berrada, "Peeking inside the black-box: a survey on explainable artificial intelligence (xai)," *IEEE access*, vol. 6, pp. 52 138–52 160, 2018.

[7] D. Van Landuyt and W. Joosen, "A descriptive study of assumptions made in linddun privacy threat elicitation," in *Proceedings of the 35th Annual ACM Symposium on Applied Computing*, 2020, pp. 1280–1287.

[8] P. Torr, "Demystifying the threat modeling process," *IEEE Security & Privacy*, vol. 3, no. 5, pp. 66–70, 2005.

[9] H. Michael and L. Steve, "The security development lifecycle: Sdl: A process for developing demonstrably more secure software," 2006.

[10] K. A. Houser and W. G. Voss, "Gdpr: The end of google and facebook or a new paradigm in data privacy," *Rich. JL & Tech.*, vol. 25, p. 1, 2018.

[11] A. Tsohou, M. Magkos, H. Mouratidis, G. Chrysoloras, L. Piras, M. Pavlidis, J. Debussche, M. Rotoloni, and B. G.-N. Crespo, "Privacy, security, legal and technology acceptance requirements for a gdpr compliance platform," in *Computer Security*. Springer, 2019, pp. 204–223.

[12] S. Greengard, "Weighing the impact of gdpr," *Communications of the ACM*, vol. 61, no. 11, pp. 16–18, 2018.

[13] T. Z. Zarsky, "Incompatible: The gdpr in the age of big data," *Seton Hall L. Rev.*, vol. 47, p. 995, 2016.

[14] J. Fruhlinger, "Threat modeling explained: A process for anticipating cyber attacks," *Tersedia pada: https://www.csoonline.com/article/3537370/threat-modeling-explained-a-process-for-anticipating-cyber-attacks.html*, 2020.

[15] W. Xiong and R. Lagerström, "Threat modeling–a systematic literature review," *Computers & security*, vol. 84, pp. 53–69, 2019.

[16] G. Kotonya and I. Sommerville, *Requirements engineering: processes and techniques*. John Wiley & Sons, Inc., 1998.

[17] J. H. Allen, S. Barnum, R. J. Ellison, G. McGraw, and N. R. Mead, *Software security engineering*. Pearson India, 2008.

[18] H. Takeda, P. Veerkamp, and H. Yoshikawa, "Modeling design process," *AI magazine*, vol. 11, no. 4, pp. 37–37, 1990.

[19] A. P. A. Ling and M. Masao, "Selection of model in developing information security criteria on smart grid security system," in *2011 IEEE Ninth International Symposium on Parallel and Distributed Processing with Applications Workshops*. IEEE, 2011, pp. 91–98.

[20] U. Z. A. Hamid, Y. Saito, H. Zamzuri, M. A. A. Rahman, and P. Raksincharoensak, "A review on threat assessment, path planning and path tracking strategies for collision avoidance systems of autonomous vehicles," *International Journal of Vehicle Autonomous Systems*, vol. 14, no. 2, pp. 134–169, 2018.

[21] A. Shostack, *Threat modeling: Designing for security*. John Wiley & Sons, 2014.

[22] V. Saini, Q. Duan, and V. Paruchuri, "Threat modeling using attack trees," *Journal of Computing Sciences in Colleges*, vol. 23, no. 4, pp. 124–131, 2008.

[23] T. UcedaVelez, "Real world threat modeling using the pasta methodology," *OWASP App Sec EU*, 2012.

[24] R. Scandariato, K. Wuyts, and W. Joosen, "A descriptive study of microsoft's threat modeling technique," *Requirements Engineering*, vol. 20, no. 2, pp. 163–180, 2015.

[25] R. Khan, K. McLaughlin, D. Laverty, and S. Sezer, "Stride-based threat modeling for cyber-physical systems," in *2017 IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT-Europe)*. IEEE, 2017, pp. 1–6.

[26] S. Japs and H. Anacker, "Resolution of safety relevant security threats in the system architecture design phase on the example of automotive industry," *Proceedings of the design society*, vol. 1, pp. 2561–2570, 2021.

[27] S. G. Abbas, I. Vaccari, F. Hussain, S. Zahid, U. U. Fayyaz, G. A. Shah, T. Bakhshi, and E. Cambiaso, "Identifying and mitigating phishing attack threats in iot use cases using a threat modelling approach," *Sensors*, vol. 21, no. 14, p. 4816, 2021.

[28] J. Howell and B. Kess, "Baldwin," *Microsoft Threat Modeling Tool. Available online: https://docs. microsoft. com/en-us/azure/security/develop/threat-modeling-tool (accessed on 12 June 2021)*.

[29] S. Parkinson, P. Ward, K. Wilson, and J. Miller, "Cyber threats facing autonomous and connected vehicles: Future challenges," *IEEE transactions on intelligent transportation systems*, vol. 18, no. 11, pp. 2898–2915, 2017.

[30] A. Jacobsson, M. Boldt, and B. Carlsson, "A risk analysis of a smart home automation system," *Future Generation Computer Systems*, vol. 56, pp. 719–733, 2016.

[31] D. Van Landuyt and W. Joosen, "A descriptive study of assumptions in stride security threat modeling," *Software and Systems Modeling*, pp. 1–18, 2021.

[32] K. Wuyts, L. Sion, and W. Joosen, "Linddun go: A lightweight approach to privacy threat modeling," in *2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*. IEEE, 2020, pp. 302–309.

[33] K. Wuyts and W. Joosen, "Linddun privacy threat modeling: a tutorial," *CW Reports*, 2015.

[34] D. Van Landuyt and W. Joosen, "A descriptive study of assumptions made in linddun privacy threat elicitation," in *Proceedings of the 35th Annual ACM Symposium on Applied Computing*, 2020, pp. 1280–1287.

[35] K. Wuyts, R. Scandariato, and W. Joosen, "Empirical evaluation of a privacy-focused threat modeling methodology," *Journal of Systems and Software*, vol. 96, pp. 122–138, 2014.

[36] N. Mead, E. Hough, and T. Stehney II, "Security quality requirements engineering technical report," *Tech. Rep. CMU/SEI-2005-TR-009*, 2005.

[37] F. Shull, "Evaluation of threat modeling methodologies," *Software Engineering Institute, Carne-gie Mellon University*, 2016.

[38] N. Shevchenko, B. R. Frye, and C. Woody, "Threat modeling for cyber-physical system-of-systems: Methods evaluation," Carnegie Mellon University Software Engineering Institute Pittsburgh United . . . , Tech. Rep., 2018.

[39] T. UcedaVelez and M. M. Morana, *Risk Centric Threat Modeling: process for attack simulation and threat analysis*. John Wiley & Sons, 2015.

[40] J. Cleland-Huang, "How well do you know your personae non gratae?" *IEEE software*, vol. 31, no. 4, pp. 28–31, 2014.

[41] N. R. Mead, F. Shull, K. Vemuru, and O. Villadsen, "A hybrid threat modeling method," *Carnegie MellonUniversity-Software Engineering Institute-Technical Report-CMU/SEI-2018-TN-002*, 2018.

[42] N. R. Mead and T. Stehney, "Security quality requirements engineering (square) methodology," *ACM SIGSOFT Software Engineering Notes*, vol. 30, no. 4, pp. 1–7, 2005.

[43] L. Sion, K. Yskout, D. Van Landuyt, and W. Joosen, "Solution-aware data flow diagrams for security threat modeling," in *Proceedings of the 33rd Annual ACM Symposium on Applied Computing*, 2018, pp. 1425–1432.

[44] B. Schneier, "Attack trees," *Dr. Dobb's journal*, vol. 24, no. 12, pp. 21–29, 1999.

[45] J. Luna, N. Suri, and I. Krontiris, "Privacy-by-design based on quantitative threat modeling," in *2012 7th International Conference on Risks and Security of Internet and Systems (CRiSIS)*. IEEE, 2012, pp. 1–8.

[46] S. M. Muthukrishnan and S. Palaniappan, "Security metrics maturity model for operational security," in *2016 IEEE Symposium on Computer Applications & Industrial Electronics (ISCAIE)*. IEEE, 2016, pp. 101–106.

[47] P. Saitta, B. Larcom, and M. Eddington, "Trike v. 1 methodology document [draft]," *URL: http://dymaxion. org/trike/Trike v1 Methodology Documentdraft. pdf*, 2005.

[48] P. Mell, K. Scarfone, and S. Romanosky, "Common vulnerability scoring system," *IEEE Security & Privacy*, vol. 4, no. 6, pp. 85–89, 2006.

[49] P. Mell, K. Scarfone, S. Romanosky *et al.*, "A complete guide to the common vulnerability scoring system version 2.0," in *Published by FIRST-forum of incident response and security teams*, vol. 1, 2007, p. 23.

[50] A. Aitken, "Dual application model for agile software engineering," in *2014 47th Hawaii International Conference on System Sciences*. IEEE, 2014, pp. 4789–4798.

[51] N. R. Mead, F. Shull, K. Vemuru, and O. Villadsen, "A hybrid threat modeling method," *Carnegie MellonUniversity-Software Engineering Institute-Technical Report-CMU/SEI-2018-TN-002*, 2018.

[52] S. Kim and R. Shrestha, "Security and privacy in intelligent autonomous vehicles," in *Automotive Cyber Security*. Springer, 2020, pp. 35–66.

[53] C. Alberts, A. Dorofee, J. Stevens, and C. Woody, "Introduction to the octave approach," Carnegie-Mellon Univ Pittsburgh Pa Software Engineering Inst, Tech. Rep., 2003.

[54] C. J. Alberts and A. J. Dorofee, *Managing information security risks: the OCTAVE approach*. Addison-Wesley Professional, 2003.

[55] N. Shevchenko, T. A. Chick, P. O'Riordan, T. P. Scanlon, and C. Woody, "Threat modeling: a summary of available methods," Carnegie Mellon University Software Engineering Institute Pittsburgh United . . . , Tech. Rep., 2018.

[56] B. L. Stevens, F. L. Lewis, and E. N. Johnson, *Aircraft control and simulation: dynamics, controls design, and autonomous systems*. John Wiley & Sons, 2015.

[57] M. Salehie and L. Tahvildari, "Self-adaptive software: Landscape and research challenges," *ACM transactions on autonomous and adaptive systems (TAAS)*, vol. 4, no. 2, pp. 1–42, 2009.

[58] S. Mazeiar and T. Ladan, "Autonomic computing: emerging trends and open problems," *ACM SIGSOFT Software Engineering Notes*, vol. 30, no. 4, pp. 1–7, 2005.

[59] M. R. Nami and M. Sharifi, "Autonomic computing: a new approach," in *First Asia International Conference on Modelling & Simulation (AMS'07)*. IEEE, 2007, pp. 352–357.

[60] P. Narman, P. Johnson, and L. Nordstrom, "Enterprise architecture: A framework supporting system quality analysis," in *11th IEEE International Enterprise Distributed Object Computing Conference (EDOC 2007)*. IEEE, 2007, pp. 130–130.

[61] H.-W. Jung, S.-G. Kim, and C.-S. Chung, "Measuring software product quality: A survey of iso/iec 9126," *IEEE software*, vol. 21, no. 5, pp. 88–92, 2004.

[62] J. Bryson and A. Winfield, “Standardizing ethical design for artificial intelligence and autonomous systems,” *Computer*, vol. 50, no. 5, pp. 116–119, 2017.

[63] A. Computing *et al.*, “An architectural blueprint for autonomic computing,” *IBM White Paper*, vol. 31, no. 2006, pp. 1–6, 2006.

[64] J. Bryson and A. Winfield, “Standardizing ethical design for artificial intelligence and autonomous systems,” *Computer*, vol. 50, no. 5, pp. 116–119, 2017.

[65] B. B. Gupta, A. Tewari, A. K. Jain, and D. P. Agrawal, “Fighting against phishing attacks: state of the art and future challenges,” *Neural Computing and Applications*, vol. 28, no. 12, pp. 3629–3654, 2017.

[66] E. Şen and G. Tuna, “The anatomy of phishing attacks and the detection and prevention of fake domain names,” in *Handbook of Research on Cyber Approaches to Public Administration and Social Policy*. IGI Global, 2022, pp. 583–605.

[67] C. S. Biswal and S. K. Pani, “Cyber-crime prevention methodology,” *Intelligent Data Analytics for Terror Threat Prediction: Architectures, Methodologies, Techniques and Applications*, pp. 291–312, 2021.

[68] D. Hangartner, D. Kopp, and M. Siegenthaler, “Monitoring hiring discrimination through online recruitment platforms,” *Nature*, vol. 589, no. 7843, pp. 572–576, 2021.

[69] T. K. Chan, C. M. Cheung, and Z. W. Lee, “Cyberbullying on social networking sites: A literature review and future research directions,” *Information & Management*, vol. 58, no. 2, p. 103411, 2021.

[70] P. Kaur, A. Dhir, A. Tandon, E. A. Alzeiby, and A. A. Abohassan, “A systematic literature review on cyberstalking. an analysis of past achievements and future promises,” *Technological Forecasting and Social Change*, vol. 163, p. 120426, 2021.

[71] S. Rao, A. K. Verma, and T. Bhatia, “Online social networks misuse, cyber crimes, and counter mechanisms,” in *Analyzing Global Social Media Consumption*. IGI Global, 2021, pp. 183–203.

[72] K. Shahriari and M. Shahriari, “Ieee standard review—ethically aligned design: A vision for prioritizing human wellbeing with artificial intelligence and autonomous systems,” in *2017 IEEE Canada International Humanitarian Technology Conference (IHTC)*. IEEE, 2017, pp. 197–201.

[73] J. J. Borking, “Why adopting privacy enhancing technologies (pets) takes so much time,” in *Computers, privacy and data protection: an element of choice*. Springer, 2011, pp. 309–341.

[74] S. Chopra and L. White, “Privacy and artificial agents, or, is google reading my email?” in *IJCAI*, 2007, pp. 1245–1250.

[75] J. M. Such, A. Espinosa, and A. García-Fornes, “A survey of privacy in multi-agent systems,” *The Knowledge Engineering Review*, vol. 29, no. 3, pp. 314–344, 2014.

[76] B. Nassi, R. Bitton, R. Masuoka, A. Shabtai, and Y. Elovici, “Sok: Security and privacy in the age of commercial drones,” in *2021 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2021, pp. 1434–1451.

[77] C. Badue, R. Guidolini, R. V. Carneiro, P. Azevedo, V. B. Cardoso, A. Forechi, L. Jesus, R. Berriel, T. M. Paixao, F. Mutz *et al.*, “Self-driving cars: A survey,” *Expert Systems with Applications*, vol. 165, p. 113816, 2021.

[78] T. Sakai and T. Nagai, “Explainable autonomous robots: a survey and perspective,” *arXiv preprint arXiv:2105.02658*, 2021.

[79] S. S. S. Bhandari, P. P. Dsouza, D. C. J. Raina *et al.*, “Personal assistant robot,” *International Journal of Applied Sciences and Smart Technologies*, vol. 3, no. 2, pp. 145–152, 2021.

[80] D. J. Solove, “A taxonomy of privacy,” *U. Pa. l. Rev.*, vol. 154, p. 477, 2005.

[81] J. E. Siegel, D. C. Erb, and S. E. Sarma, “A survey of the connected vehicle landscape—architectures, enabling technologies, applications, and development areas,” *IEEE Transactions on Intelligent Transportation Systems*, vol. 19, no. 8, pp. 2391–2406, 2017.

[82] L. Meiländer, “Are autonomous drones perceived as trustworthy? the effects of fire department resemblance and transparent information on trust in a drone,” Master’s thesis, University of Twente, 2021.

[83] H. Chen, Y. Wen, M. Zhu, Y. Huang, C. Xiao, T. Wei, and A. Hahn, “From automation system to autonomous system: An architecture perspective,” *Journal of Marine Science and Engineering*, vol. 9, no. 6, p. 645, 2021.

[84] Y. Gurevich, E. Hudis, and J. M. Wing, “Inverse privacy,” *Communications of the ACM*, vol. 59, no. 7, pp. 38–42, 2016.

[85] “Jaguar files face and gait recognition system patent for vehicle entry,” accessed: 28 November 2016.

[86] S. Spiekermann and L. Cranor, “Engineering privacy’ieee transactions on software engineering 35, 1 (jan/feb 2009) 67,” 2009.

[87] C. O’neil, *Weapons of math destruction: How big data increases inequality and threatens democracy*. Broadway Books, 2016.

[88] R. Maity, R. Mishra, and P. K. Pattnaik, “A review of flying robot applications in healthcare,” *Smart Healthcare Analytics: State of the Art*, pp. 103–111, 2022.

[89] T. Ribeiro, F. Gonçalves, I. S. Garcia, G. Lopes, and A. F. Ribeiro, “Charmie: A collaborative healthcare and home service and assistant robot for elderly care,” *Applied Sciences*, vol. 11, no. 16, p. 7248, 2021.

[90] M. Guerini, F. Pianesi, and O. Stock, “Is it morally acceptable for a system to lie to persuade me?” in *Workshops at the twenty-ninth AAAI conference on artificial intelligence*, 2015.

[91] A. Lima, F. Rocha, M. Völp, and P. Esteves-Veríssimo, “Towards safe and secure autonomous and cooperative vehicle ecosystems,” in *Proceedings of the 2nd ACM Workshop on Cyber-Physical Systems Security and Privacy*, 2016, pp. 59–70.

[92] “Dronecast.com,” accessed: 2022.

[93] A. L. Ramos, J. V. Ferreira, and J. Barceló, “Model-based systems engineering: An emerging approach for modern systems,” *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews)*, vol. 42, no. 1, pp. 101–111, 2011.

[94] A. Karahasanovic, P. Kleberger, and M. Almgren, “Adapting threat modeling methods for the automotive industry,” in *Proceedings of the 15th ESCAR Conference*, 2017, pp. 1–10.

[95] F. Jahan, W. Sun, Q. Niyaz, and M. Alam, “Security modeling of autonomous systems: a survey,” *ACM Computing Surveys (CSUR)*, vol. 52, no. 5, pp. 1–34, 2019.

[96] R. Gupta, S. Tanwar, S. Tyagi, and N. Kumar, “Machine learning models for secure data analytics: A taxonomy and threat model,” *Computer Communications*, vol. 153, pp. 406–440, 2020.

[97] M. Mahak and Y. Singh, “Threat modelling and risk assessment in internet of things: A review,” in *Proceedings of Second International Conference on Computing, Communications, and Cyber-Security*. Springer, 2021, pp. 293–305.

[98] M. Jbair, B. Ahmad, C. Maple, and R. Harrison, “Threat modelling for industrial cyber physical systems in the era of smart manufacturing,” *Computers in Industry*, vol. 137, p. 103611, 2022.

[99] S. G. Abbas, I. Vaccari, F. Hussain, S. Zahid, U. U. Fayyaz, G. A. Shah, T. Bakhshi, and E. Cambiaso, “Identifying and mitigating phishing attack threats in iot use cases using a threat modelling approach,” *Sensors*, vol. 21, no. 14, p. 4816, 2021.

[100] Y. Fu, C. Li, F. R. Yu, T. H. Luan, and Y. Zhang, “A survey of driving safety with sensing, vehicular communications, and artificial intelligence-based collision avoidance,” *IEEE Transactions on Intelligent Transportation Systems*, 2021.

[101] Y. B. Hamdan *et al.*, “Smart home environment future challenges and issues-a survey,” *Journal of Electronics*, vol. 3, no. 01, pp. 239–246, 2021.

[102] A. Basit, M. Zafar, X. Liu, A. R. Javed, Z. Jalil, and K. Kifayat, “A comprehensive survey of ai-enabled phishing attacks detection techniques,” *Telecommunication Systems*, vol. 76, no. 1, pp. 139–154, 2021.

[103] P. Burda, T. Chotza, L. Allodi, and N. Zannone, “Testing the effectiveness of tailored phishing techniques in industry and academia: a field experiment,” in *Proceedings of the 15th International Conference on Availability, Reliability and Security*, 2020, pp. 1–10.

[104] S. G. Abbas, I. Vaccari, F. Hussain, S. Zahid, U. U. Fayyaz, G. A. Shah, T. Bakhshi, and E. Cambiaso, “Identifying and mitigating phishing attack threats in iot use cases using a threat modelling approach,” *Sensors*, vol. 21, no. 14, p. 4816, 2021.

[105] S. Kim and R. Shrestha, “Security and privacy in intelligent autonomous vehicles,” in *Automotive Cyber Security*. Springer, 2020, pp. 35–66.

[106] A. Y. Javaid, W. Sun, V. K. Devabhaktuni, and M. Alam, “Cyber security threat analysis and modeling of an unmanned aerial vehicle system,” in *2012 IEEE Conference on Technologies for Homeland Security (HST)*. IEEE, 2012, pp. 585–590.

[107] J.-H. Park, S.-y. Kang, and S.-j. Kim, “Study of security requirement of smart home hub through threat modeling analysis and common criteria,” *Journal of the Korea Institute of Information Security & Cryptology*, vol. 28, no. 2, pp. 513–528, 2018.

[108] D. Van Landuyt and W. Joosen, "A descriptive study of assumptions made in linddun privacy threat elicitation," in *Proceedings of the 35th Annual ACM Symposium on Applied Computing*, 2020, pp. 1280–1287.

[109] R. Thorburn, A. Margheri, and F. Paci, "Towards an integrated privacy protection framework for iot: contextualising regulatory requirements with industry best practices," 2019.

[110] D. J. Solove, "A taxonomy of privacy," *U. Pa. l. Rev.*, vol. 154, p. 477, 2005.

[111] Y. Wang, Q. Wu, B. Qin, X. Chen, X. Huang, and J. Lou, "Ownership-hidden group-oriented proofs of storage from prehomomorphic signatures," *Peer-to-Peer Networking and Applications*, vol. 11, no. 2, pp. 235–251, 2018.

[112] B. B. Madan, M. Banik, and D. Bein, "Securing unmanned autonomous systems from cyber threats," *The Journal of Defense Modeling and Simulation*, vol. 16, no. 2, pp. 119–136, 2019.

[113] G. Ho, D. Leung, P. Mishra, A. Hosseini, D. Song, and D. Wagner, "Smart locks: Lessons for securing commodity internet of things devices," in *Proceedings of the 11th ACM on Asia conference on computer and communications security*, 2016, pp. 461–472.

[114] A. Alrawais, A. Alhothaily, C. Hu, and X. Cheng, "Fog computing for the internet of things: Security and privacy issues," *IEEE Internet Computing*, vol. 21, no. 2, pp. 34–42, 2017.

[115] P. Aufner, "The iot security gap: a look down into the valley between threat models and their implementation," *International Journal of Information Security*, vol. 19, no. 1, pp. 3–14, 2020.

[116] A. Shafique, A. Mehmood, and M. Elhadef, "Survey of security protocols and vulnerabilities in unmanned aerial vehicles," *IEEE Access*, vol. 9, pp. 46 927–46 948, 2021.

[117] S. Boddupalli, A. Hegde, and S. Ray, "Replace: Real-time security assurance in vehicular platoons against v2v attacks," in *2021 IEEE International Intelligent Transportation Systems Conference (ITSC)*. IEEE, 2021, pp. 1179–1185.

[118] A.-M. Jamil, S. Khan, J. K. Lee, and L. B. Othmane, "Towards automated threat modeling of cyber-physical systems," in *2021 International Conference on Software Engineering & Computer Systems and 4th International Conference on Computational Science and Information Management (ICSECS-ICOCSIM)*. IEEE, 2021, pp. 614–619.

[119] H. Mun, M. Seo, and D. H. Lee, "Secure privacy-preserving v2v communication in 5g-v2x supporting network slicing," *IEEE Transactions on Intelligent Transportation Systems*, 2021.

[120] S. Abraham, Z. Carmichael, S. Banerjee, R. VidalMata, A. Agrawal, M. N. Al Islam, W. Scheirer, and J. Cleland-Huang, "Adaptive autonomy in human-on-the-loop vision-based robotics systems," in *2021 IEEE/ACM 1st Workshop on AI Engineering-Software Engineering for AI (WAIN)*. IEEE, 2021, pp. 113–120.

[121] R. L. Finn and D. Wright, "Unmanned aircraft systems: Surveillance, ethics and privacy in civil applications," *Computer Law & Security Review*, vol. 28, no. 2, pp. 184–194, 2012.

[122] E. Damiani, "Toward big data risk analysis," in *2015 IEEE International Conference on Big Data (Big Data)*. IEEE, 2015, pp. 1905–1909.

[123] S. Yu and S. Guo, *Big data concepts, theories, and applications*. Springer, 2016.

[124] L. Qi, "Research on intelligent transportation system technologies and applications," in *2008 Workshop on Power Electronics and Intelligent Transportation System*. IEEE, 2008, pp. 529–531.

[125] A.-A. O. Affia, R. Matulevičius, and A. Nolte, "Security risk management in cooperative intelligent transportation systems: a systematic literature review," in *OTM Confederated International Conferences" On the Move to Meaningful Internet Systems"*. Springer, 2019, pp. 282–300.

[126] O. Zaki, M. Dunnigan, V. Robu, and D. Flynn, "Reliability and safety of autonomous systems based on semantic modelling for self-certification," *Robotics*, vol. 10, no. 1, p. 10, 2021.

[127] B. McMahan, E. Moore, D. Ramage, S. Hampson, and B. A. y Arcas, "Communication-efficient learning of deep networks from decentralized data," in *Artificial intelligence and statistics*. PMLR, 2017, pp. 1273–1282.

[128] Q. Li, Z. Wen, Z. Wu, S. Hu, N. Wang, Y. Li, X. Liu, and B. He, "A survey on federated learning systems: vision, hype and reality for data privacy and protection," *IEEE Transactions on Knowledge and Data Engineering*, 2021.

[129] L. Lyu, H. Yu, and Q. Yang, "Threats to federated learning: A survey," *arXiv preprint arXiv:2003.02133*, 2020.

[130] L. Huang, A. D. Joseph, B. Nelson, B. I. Rubinstein, and J. D. Tygar, "Adversarial machine learning," in *Proceedings of the 4th ACM workshop on Security and artificial intelligence*, 2011, pp. 43–58.

[131] P. Kairouz, H. B. McMahan, B. Avent, A. Bellet, M. Bennis, A. N. Bhagoji, K. Bonawitz, Z. Charles, G. Cormode, R. Cummings *et al.*, "Advances and open problems in federated learning," *Foundations and Trends® in Machine Learning*, vol. 14, no. 1–2, pp. 1–210, 2021.

[132] C. Dwork, "Differential privacy: A survey of results," in *International conference on theory and applications of models of computation*. Springer, 2008, pp. 1–19.

[133] S. Micali and P. Rogaway, "Secure computation," in *Annual International Cryptology Conference*. Springer, 1991, pp. 392–404.

[134] M. Sabt, M. Achemlal, and A. Bouabdallah, "Trusted execution environment: what it is, and what it is not," in *2015 IEEE Trustcom/BigDataSE/ISPA*, vol. 1. IEEE, 2015, pp. 57–64.

[135] V. Tolpegin, S. Truex, M. E. Gursoy, and L. Liu, "Data poisoning attacks against federated learning systems," in *European Symposium on Research in Computer Security*. Springer, 2020, pp. 480–501.

[136] B. Yu, W. Mao, Y. Lv, C. Zhang, and Y. Xie, "A survey on federated learning in data mining," *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, vol. 12, no. 1, p. e1443, 2022.

[137] M. A. Siddiqi, C. Iwendi, K. Jaroslava, and N. Anumbe, "Analysis on security-related concerns of unmanned aerial vehicle: attacks, limitations, and recommendations," *Mathematical Biosciences and Engineering*, vol. 19, no. 3, pp. 2641–2670, 2022.

[138] S. Katzenbeisser, I. Polian, F. Regazzoni, and M. Stöttinger, "Security in autonomous systems," in *2019 IEEE European Test Symposium (ETS)*. IEEE, 2019, pp. 1–8.

[139] R. Deghaili, A. Chehab, A. Kayssi, and W. Itani, "Stride: A secure framework for modeling trust-privacy tradeoffs in distributed computing environments," *International Journal of Dependable and Trustworthy Information Systems (IJDTIS)*, vol. 1, no. 1, pp. 60–81, 2010.

[140] A. Chattopadhyay, K.-Y. Lam, and Y. Tavva, "Autonomous vehicle: Security by design," *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 11, pp. 7015–7029, 2020.

[141] D. R. Thompson, J. Di, H. Sunkara, and C. Thompson, "Categorizing rfid privacy threats with stride," in *Proceedings ACM's Symposium on Usable Privacy and Security held at CMU*. Citeseer, 2006.

[142] S. Sharma, *Data privacy and GDPR handbook*. John Wiley & Sons, 2019.

[143] M. Budrytė, "General data protection regulation (gdpr) in european union: from proposal to implementation," B.S. thesis, 2021.

[144] D. Wright and C. Raab, "Privacy principles, risks and harms," *International Review of Law, Computers & Technology*, vol. 28, no. 3, pp. 277–298, 2014.

[145] H. Li, L. Yu, and W. He, "The impact of gdpr on global technology development," pp. 1–6, 2019.

[146] N. B. Truong, K. Sun, G. M. Lee, and Y. Guo, "Gdpr-compliant personal data management: A blockchain-based solution," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 1746–1761, 2019.

[147] P. Voigt and A. Von dem Bussche, "The eu general data protection regulation (gdpr)," *A Practical Guide, 1st Ed., Cham: Springer International Publishing*, vol. 10, no. 3152676, pp. 10–5555, 2017.

[148] G. Chassang, "The impact of the eu general data protection regulation on scientific research," *ecancermedicalscience*, vol. 11, 2017.

[149] C. Peukert, S. Bechtold, M. Batikas, and T. Kretschmer, "Regulatory spillovers and data governance: Evidence from the gdpr," *Marketing Science*, 2022.

[150] W. G. Voss, "European union data privacy law reform: General data protection regulation, privacy shield, and the right to delisting," *The Business Lawyer*, vol. 72, no. 1, pp. 221–234, 2016.

[151] N. F. Palmieri III, "Data protection in an increasingly globalized world," *Ind. LJ*, vol. 94, p. 297, 2019.

[152] D. A. Tamburri, "Design principles for the general data protection regulation (gdpr): A formal concept analysis and its evaluation," *Information Systems*, vol. 91, p. 101469, 2020.

[153] M. Davari and E. Bertino, "Access control model extensions to support data privacy protection based on gdpr," in *2019 IEEE International Conference on Big Data (Big Data)*. IEEE, 2019, pp. 4017–4024.

[154] U. Jayasinghe, G. M. Lee, and A. MacDermott, "Trust-based data controller for personal information management," in *2018 International Conference on Innovations in Information Technology (IIT)*. IEEE, 2018, pp. 123–128.

[155] M. Hintze, "Data controllers, data processors, and the growing use of connected products in the enterprise: Managing risks, understanding benefits, and complying with the gdpr," *Journal of Internet Law (Wolters Kluwer), August*, 2018.

[156] P. Wolters, "The control by and rights of the data subject under the gdpr," 2018.

[157] M. Hintze, "Data controllers, data processors, and the growing use of connected products in the enterprise: Managing risks, understanding benefits, and complying with the gdpr," *Journal of Internet Law (Wolters Kluwer), August*, 2018.

[158] A. Cohen and K. Nissim, "Towards formalizing the gdpr's notion of singling out," *Proceedings of the National Academy of Sciences*, vol. 117, no. 15, pp. 8344–8352, 2020.

[159] C. Dwork, "Differential privacy: A survey of results," in *International conference on theory and applications of models of computation*. Springer, 2008, pp. 1–19.

[160] L. Sweeney, "k-anonymity: A model for protecting privacy," *International journal of uncertainty, fuzziness and knowledge-based systems*, vol. 10, no. 05, pp. 557–570, 2002.

[161] M. Rigaki and S. Garcia, "A survey of privacy attacks in machine learning," *arXiv preprint arXiv:2007.07646*, 2020.

[162] E. R. Brouwer, "Legality and data protection law: The forgotten purpose of purpose limitation," 2011.

[163] J. Krumm, "Inference attacks on location tracks," in *International Conference on Pervasive Computing*. Springer, 2007, pp. 127–143.

[164] R. Shokri, M. Stronati, C. Song, and V. Shmatikov, "Membership inference attacks against machine learning models," in *2017 IEEE symposium on security and privacy (SP)*. IEEE, 2017, pp. 3–18.

[165] V. H. Robertson, "Excessive data collection: privacy considerations and abuse of dominance in the era of big data," *Common Market Law Review*, vol. 57, no. 1, 2020.

[166] M. Wernke, P. Skvortsov, F. Dürr, and K. Rothermel, "A classification of location privacy attacks and approaches," *Personal and ubiquitous computing*, vol. 18, no. 1, pp. 163–175, 2014.

[167] E. Biasin, "Why accuracy needs further exploration in data protection," in *Proceedings of the 1st International Conference on AI for People: Towards Sustainable AI*. EAI, 2021, pp. 1–7.

[168] A. Krašovec, G. Baldini, and V. Pejović, "Opposing data exploitation: Behaviour biometrics for privacy-preserving authentication in iot environments," in *The 16th International Conference on Availability, Reliability and Security*, 2021, pp. 1–7.

[169] C. Farkas, "Big data analytics: Privacy protection using semantic web technologies," in *NSF Workshop on Big Data Security and Privacy*, 2014.

[170] J. A. Shamsi and M. A. Khojaye, "Understanding privacy violations in big data systems," *It Professional*, vol. 20, no. 3, pp. 73–81, 2018.

[171] N. Li, T. Li, and S. Venkatasubramanian, "t-closeness: Privacy beyond k-anonymity and l-diversity," in *2007 IEEE 23rd international conference on data engineering*. IEEE, 2007, pp. 106–115.

[172] J. Soria-Comas and J. Domingo-Ferrert, "Differential privacy via t-closeness in data publishing," in *2013 Eleventh Annual Conference on Privacy, Security and Trust*. IEEE, 2013, pp. 27–35.

[173] M. Z. Gunduz and R. Das, "Analysis of cyber-attacks on smart grid applications," in *2018 International Conference on Artificial Intelligence and Data Processing (IDAP)*. IEEE, 2018, pp. 1–5.

[174] S. T. Siddiqui, S. Alam, R. Ahmad, and M. Shuaib, "Security threats, attacks, and possible countermeasures in internet of things," in *Advances in data and information sciences*. Springer, 2020, pp. 35–46.

[175] I. Ali, S. Sabir, and Z. Ullah, "Internet of things security, device authentication and access control: a review," *arXiv preprint arXiv:1901.07309*, 2019.

[176] M. Sharaf, "Non-repudiation and privacy-preserving sharing of electronic health records," *Cogent Engineering*, vol. 9, no. 1, p. 2034374, 2022.

[177] R. Gellert, "Understanding the notion of risk in the general data protection regulation," *Computer Law & Security Review*, vol. 34, no. 2, pp. 279–288, 2018.

[178] U. Pagallo, P. Casanovas, and R. Madelin, "The middle-out approach: assessing models of legal governance in data protection, artificial intelligence, and the web of data," *The Theory and Practice of Legislation*, vol. 7, no. 1, pp. 1–25, 2019.

[179] S. Wachter, "The gdpr and the internet of things: a three-step transparency model," *Law, Innovation and Technology*, vol. 10, no. 2, pp. 266–294, 2018.

[180] R. Rault and D. Trentesaux, "Artificial intelligence, autonomous systems and robotics: legal innovations," in *Service Orientation in Holonic and Multi-Agent Manufacturing*. Springer, 2018, pp. 1–9.

[181] M. Coeckelbergh and M. Funk, "Data, speed, and know-how: ethical and philosophical issues in human-autonomous systems cooperation in military contexts," in *International Workshop on Modelling and Simulation for Autonomous Systems*. Springer, 2016, pp. 17–24.

[182] F. Costantini, N. Thomopoulos, F. Steibel, A. Curl, G. Lugano, and T. Kováčiková, "Autonomous vehicles in a gdpr era: An international comparison," in *Advances in Transport Policy and Planning*. Elsevier, 2020, vol. 5, pp. 191–213.

[183] N. Thomopoulos, M. Givoni *et al.*, *ICT for transport: Opportunities and threats*. Edward Elgar Publishing, 2015.

[184] F. Vallet, "The gdpr and its application in connected vehicles-compliance and good practices," in *Electronic Components and Systems for Automotive Applications*. Springer, 2019, pp. 245–254.

[185] F. Galdon and A. Hall, "The right to reparations: a new digital right for repairing trust in the emerging era of highly autonomous systems," in *International Conference on Human Interaction and Emerging Technologies*. Springer, 2020, pp. 538–543.

[186] B. D. Mittelstadt, P. Allo, M. Taddeo, S. Wachter, and L. Floridi, "The ethics of algorithms: Mapping the debate," *Big Data & Society*, vol. 3, no. 2, p. 2053951716679679, 2016.

[187] W.-F. Tung, "Gec-hr: Gamification exercise companion for home robot with iot," in *International Conference on Human-Computer Interaction*. Springer, 2019, pp. 141–145.

[188] E. E. Joh, "Policing police robots," *UCLA L. Rev. Discourse*, vol. 64, p. 516, 2016.

[189] M. Dikmen and C. Burns, "Trust in autonomous vehicles: The case of tesla autopilot and summon," in *2017 IEEE International conference on systems, man, and cybernetics (SMC)*. IEEE, 2017, pp. 1093–1098.

[190] S. Wachter, B. Mittelstadt, and L. Floridi, "Transparent, explainable, and accountable ai for robotics," *Science robotics*, vol. 2, no. 6, p. eaan6080, 2017.

[191] D. Omeiza, H. Webb, M. Jirotka, and L. Kunze, "Explanations in autonomous driving: A survey," *IEEE Transactions on Intelligent Transportation Systems*, 2021.

[192] D. S. Hall, "High definition lidar system," Jun. 28 2011, uS Patent 7,969,558.

[193] D. K. Barton, *Radar system analysis and modeling*. Artech House, 2004.

[194] T. Ha, S. Kim, D. Seo, and S. Lee, "Effects of explanation types and perceived risk on trust in autonomous vehicles," *Transportation research part F: traffic psychology and behaviour*, vol. 73, pp. 271–280, 2020.

[195] F. Cuzzolin, A. Morelli, B. Cirstea, and B. J. Sahakian, "Knowing me, knowing you: theory of mind in ai," *Psychological medicine*, vol. 50, no. 7, pp. 1057–1061, 2020.

[196] M. McFarland, "Who's responsible when an autonomous car crashes?" *Accessed: Jul*, vol. 24, p. 2020, 2016.

[197] E. Yurtsever, J. Lambert, A. Carballo, and K. Takeda, "A survey of autonomous driving: Common practices and emerging technologies," *IEEE access*, vol. 8, pp. 58 443–58 469, 2020.

[198] J. Koo, J. Kwac, W. Ju, M. Steinert, L. Leifer, and C. Nass, "Why did my car just do that? explaining semi-autonomous driving actions to improve driver understanding, trust, and performance," *International Journal on Interactive Design and Manufacturing (IJIDeM)*, vol. 9, no. 4, pp. 269–275, 2015.

[199] R. Hussain and S. Zeadally, "Autonomous cars: Research results, issues, and future challenges," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 2, pp. 1275–1313, 2018.

[200] S. Darbha, S. Konduri, and P. R. Pagilla, "Benefits of v2v communication for autonomous and connected vehicles," *IEEE Transactions on Intelligent Transportation Systems*, vol. 20, no. 5, pp. 1954–1963, 2018.

[201] J. Harding, G. Powell, R. Yoon, J. Fikentscher, C. Doyle, D. Sade, M. Lukuc, J. Simons, J. Wang *et al.*, "Vehicle-to-vehicle communications: readiness of v2v technology for application." United States. National Highway Traffic Safety Administration, Tech. Rep., 2014.

[202] K. C. Dey, A. Rayamajhi, M. Chowdhury, P. Bhavsar, and J. Martin, "Vehicle-to-vehicle (v2v) and vehicle-to-infrastructure

(v2i) communication in a heterogeneous wireless network–performance evaluation," *Transportation Research Part C: Emerging Technologies*, vol. 68, pp. 168–184, 2016.

[203] H. Rakha and R. K. Kamalanathsharma, "Eco-driving at signalized intersections using v2i communication," in *2011 14th international IEEE conference on intelligent transportation systems (ITSC)*. IEEE, 2011, pp. 341–346.

[204] J. Petit and S. E. Shladover, "Potential cyberattacks on automated vehicles," *IEEE Transactions on Intelligent transportation systems*, vol. 16, no. 2, pp. 546–556, 2014.

[205] T. SAE, "Definitions for terms related to driving automation systems for on-road motor vehicles," *SAE Standard J*, vol. 3016, p. 2016, 2016.

[206] K. Koscher, A. Czeskis, F. Roesner, S. Patel, T. Kohno, S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham *et al.*, "Experimental security analysis of a modern automobile," in *2010 IEEE symposium on security and privacy*. IEEE, 2010, pp. 447–462.

[207] J. Liu, S. Zhang, W. Sun, and Y. Shi, "In-vehicle network attacks and countermeasures: Challenges and future directions," *IEEE Network*, vol. 31, no. 5, pp. 50–58, 2017.

[208] H. Kang, B. I. Kwak, Y. H. Lee, H. Lee, H. Lee, and H. K. Kim, "Car hacking and defense competition on in-vehicle network," in *Workshop on Automotive and Autonomous Vehicle Security (AutoSec)*, vol. 2021, 2021, p. 25.

[209] B. R. Payne, "Car hacking: Accessing and exploiting the can bus protocol," *Journal of Cybersecurity Education, Research and Practice*, vol. 2019, no. 1, p. 5, 2019.

[210] S. Gyawali, S. Xu, Y. Qian, and R. Q. Hu, "Challenges and solutions for cellular based v2x communications," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 1, pp. 222–255, 2020.

[211] K. Kim, J. S. Kim, S. Jeong, J.-H. Park, and H. K. Kim, "Cybersecurity for autonomous vehicles: Review of attacks and defense," *Computers & Security*, vol. 103, p. 102150, 2021.

[212] V. L. Thing and J. Wu, "Autonomous vehicle security: A taxonomy of attacks and defences," in *2016 ieee international conference on internet of things (ithings) and ieee green computing and communications (greencom) and ieee cyber, physical and social computing (cpscom) and ieee smart data (smartdata)*. IEEE, 2016, pp. 164–170.

[213] S. Gifei and A. Salceanu, "Integrated management system for quality, safety and security in developing autonomous vehicles," in *2017 10th International Symposium on Advanced Topics in Electrical Engineering (ATEE)*. IEEE, 2017, pp. 673–676.

[214] S. Woo, H. J. Jo, and D. H. Lee, "A practical wireless attack on the connected car and security protocol for in-vehicle can," *IEEE Transactions on intelligent transportation systems*, vol. 16, no. 2, pp. 993–1006, 2014.

[215] S. Liu, J. Tang, C. Wang, Q. Wang, and J.-L. Gaudiot, "A unified cloud platform for autonomous driving," *Computer*, vol. 50, no. 12, pp. 42–49, 2017.

[216] S. Almeaibed, S. Al-Rubaye, A. Tsourdos, and N. P. Avdelidis, "Digital twin analysis to promote safety and security in autonomous vehicles," *IEEE Communications Standards Magazine*, vol. 5, no. 1, pp. 40–46, 2021.

[217] C. Yan, W. Xu, and J. Liu, "Can you trust autonomous vehicles: Contactless attacks against sensors of self-driving vehicle," *Def Con*, vol. 24, no. 8, p. 109, 2016.

[218] S. R. Shetty and D. Manjaiah, "A comprehensive study of security attack on vanet," in *Data Management, Analytics and Innovation*. Springer, 2022, pp. 407–428.

[219] M. Muhammad and G. A. Safdar, "Survey on existing authentication issues for cellular-assisted v2x communication," *Vehicular Communications*, vol. 12, pp. 50–65, 2018.

[220] B. K. Bhargava, A. M. Johnson, G. I. Munyengabe, and P. Angin, "A systematic approach for attack analysis and mitigation in v2v networks." *J. Wirel. Mob. Networks Ubiquitous Comput. Dependable Appl.*, vol. 7, no. 1, pp. 79–96, 2016.

[221] R. Dave, E. Boone, and K. Roy, "Efficient data privacy and security in autonomous cars," *Journal of Computer Sciences and Applications*, vol. 7, no. 1, pp. 31–36, 2019.

[222] C. Bloom, J. Tan, J. Ramjohn, and L. Bauer, "Self-driving cars and data collection: Privacy perceptions of networked autonomous vehicles," in *Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017)*, 2017, pp. 357–375.

[223] J. Shen, J. Y. Won, Z. Chen, and Q. A. Chen, "Drift with devil: Security of {Multi-Sensor} fusion based localization in {High-Level} autonomous driving under {GPS} spoofing," in *29th USENIX Security Symposium (USENIX Security 20)*, 2020, pp. 931–948.

[224] N. K. Chaubey, "Security analysis of vehicular ad hoc networks (vanets): a comprehensive study," *International Journal of Security and Its Applications*, vol. 10, no. 5, pp. 261–274, 2016.

[225] A. Y. Dak, S. Yahya, and M. Kassim, "A literature survey on security challenges in vanets," *International Journal of Computer Theory and Engineering*, vol. 4, no. 6, p. 1007, 2012.

[226] R. S. Raw, M. Kumar, and N. Singh, "Security challenges, issues and their solutions for vanet," *International journal of network security & its applications*, vol. 5, no. 5, p. 95, 2013.

[227] N. Lyamin, D. Kleyko, Q. Delooz, and A. Vinel, "Real-time jamming dos detection in safety-critical v2v c-its using data mining," *IEEE Communications Letters*, vol. 23, no. 3, pp. 442–445, 2019.

[228] M. El-Said, X. Wang, S. Mansour, and A. Kalafut, "Building an impersonation attack and defense testbed for vehicle to vehicle systems," in *Proceedings of the 22st Annual Conference on Information Technology Education*, 2021, pp. 65–66.

[229] D. Kosmanos, A. Pappas, L. Maglaras, S. Moschoyiannis, F. J. Aparicio-Navarro, A. Argyriou, and H. Janicke, "A novel intrusion detection system against spoofing attacks in connected electric vehicles," *Array*, vol. 5, p. 100013, 2020.

[230] S.-J. Horng and S.-F. Tzeng, "Vanet-based secure value-added services," in *Proceedings of the 2014 International Conference on Social Computing*, 2014, pp. 1–4.

[231] A. Pfitzmann and M. Hansen, "A terminology for talking about privacy by data minimization: Anonymity, unlinkability, undetectability, unobservability, pseudonymity, and identity management," 2010.

[232] M. Roe, "Cryptography and evidence," University of Cambridge, Computer Laboratory, Tech. Rep., 2010.

[233] E. McCallister, *Guide to protecting the confidentiality of personally identifiable information*. Diane Publishing, 2010, vol. 800, no. 122.

[234] S. Lederer, J. I. Hong, A. K. Dey, and J. A. Landay, "Personal privacy through understanding and action: five pitfalls for designers," *Personal and ubiquitous computing*, vol. 8, no. 6, pp. 440–454, 2004.

[235] M. S. N. Khan, "Privacy in the age of autonomous systems," Ph.D. dissertation, KTH Royal Institute of Technology, 2020.

[236] T. Nandy, M. Y. I. B. Idris, R. M. Noor, S. Bhattacharyya, and N. B. A. Ghani, "Collaborative data anonymization for privacy-preserving vehicular ad-hoc network," in *2020 International Conference on Innovation and Intelligence for Informatics, Computing and Technologies (3ICT)*. IEEE, 2020, pp. 1–6.

[237] D. F. Llorca, M. Sotelo, S. Sánchez, M. Ocaña, J. Rodríguez-Ascariz, and M. García-Garrido, "Traffic data collection for floating car data enhancement in v2i networks," *EURASIP Journal on Advances in Signal Processing*, vol. 2010, pp. 1–13, 2010.

[238] L. Schnabel, S. Matzka, M. Stellmacher, M. Pätzold, and E. Matthes, "Impact of anonymization on vehicle detector performance," in *2019 Second International Conference on Artificial Intelligence for Industries (AI4I)*. IEEE, 2019, pp. 30–34.

[239] M. Arif, G. Wang, and T. Peng, "Track me if you can? query based dual location privacy in vanets for v2v and v2i," in *2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*. IEEE, 2018, pp. 1091–1096.

[240] M. Gupta, J. Benson, F. Patwa, and R. Sandhu, "Secure v2v and v2i communication in intelligent transportation using cloudlets," *IEEE Transactions on Services Computing*, 2020.

[241] F. Armknecht, A. Festag, D. Westhoff, and K. Zeng, "Cross-layer privacy enhancement and non-repudiation in vehicular communication," in *Communication in Distributed Systems-15. ITG/GI Symposium*. VDE, 2007, pp. 1–12.

[242] A. Ekdahl and L. Nyman, "A methodology to validate compliance to the gdpr," 2018.

[243] A. Boch, E. Hohma, and R. Trauth, "Towards an accountability framework for ai: Ethical and legal considerations."

[244] M. C. Gaeta, "Data protection and self-driving cars: The consent to the processing of personal data in compliance with gdpr," *Communications Law*, vol. 24, no. 1, pp. 15–23, 2019.

[245] C. Matte, N. Bielova, and C. Santos, "Do cookie banners respect my choice?: Measuring legal compliance of banners from iab europe's transparency and consent framework," in *2020 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2020, pp. 791–809.

[246] R. Zallone, “Connected cars under the gdpr,” in *2019 AEIT International Conference of Electrical and Electronic Technologies for Automotive (AEIT AUTOMOTIVE)*. IEEE, 2019, pp. 1–6.

[247] V. K. Veitas and S. Delaere, “In-vehicle data recording, storage and access management in autonomous vehicles,” *arXiv preprint arXiv:1806.03243*, 2018.

[248] E. Fialová, “Autonomous vehicles and european data protection law,” *MECCA Journal of Middle European Construction and Design of Cars*, vol. 17, no. 1, pp. 6–6, 2020.

[249] J. Zhu, A. Liapis, S. Risi, R. Bidarra, and G. M. Youngblood, “Explainable ai for designers: A human-centered perspective on mixed-initiative co-creation,” in *2018 IEEE Conference on Computational Intelligence and Games (CIG)*. IEEE, 2018, pp. 1–8.

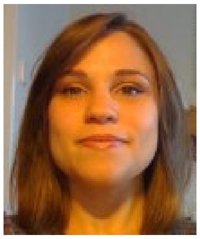
[250] S. Lahdya and T. Mazri, “Security study of routing attacks in vehicular ad-hoc networks (autonomous car),” *The International Archives of Photogrammetry, Remote Sensing and Spatial Information Sciences*, vol. 46, pp. 349–353, 2021.

[251] B. Brown and E. Laurier, “The trouble with autopilots: Assisted and autonomous driving on the social road,” in *Proceedings of the 2017 CHI conference on human factors in computing systems*, 2017, pp. 416–429.

[252] S.-C. Lin, Y. Zhang, C.-H. Hsu, M. Skach, M. E. Haque, L. Tang, and J. Mars, “The architectural implications of autonomous driving: Constraints and acceleration,” in *Proceedings of the Twenty-Third International Conference on Architectural Support for Programming Languages and Operating Systems*, 2018, pp. 751–766.

[253] D. Peras, “Guidelines for gdpr compliant consent and data management model in ict businesses,” in *Central European Conference on Information and Intelligent Systems*. Faculty of Organization and Informatics Varazdin, 2018, pp. 113–121.

Naila Azam is a PhD student at School of Computing Science, the University of Glasgow. Previously, she was a lecturer at the Department of Computing Science, Sardar Bahadur Khan Women’s University Balochistan, Pakistan in 2017-2021. She received her MS(CS), and BS(CE), degrees from Sardar Bahadur Khan Women’s University Balochistan, Pakistan, and Balochistan University of Information Technology, Engineering and Management Sciences, Pakistan in 2019 and 2013 respectively. She was an IT Assistant to Nutrition Program at PPHI Balochistan, a prestigious company that provides health care services in Pakistan, in 2016-2017. Her research interest lies in Data Privacy, Security, Trust, Threat Modelling, Personal Data Management, and Autonomous Systems.



Lito Michala is currently a lecturer within the school of computing science. She has previously worked as an RSE/SE Enterprise Fellow and as a Researcher on the AnyScale Applications EPSRC funded project under the supervision of Dr Jeremy Singer and Prof Phil Trinder. She acquired her MSc in 2008 on Biomedical Engineering at the University of Strathclyde and her Bachelor degree in 2007 in Computer Science from the University of Crete. Her research interests include Large scale, complex, cyber-physical systems engineering, machine learning and data fusion applications, edge computing, distributed systems, and heterogeneous architectures and autonomous systems.

Shuja Ansari (IEEE M’15-SM’20, IET M’15) received the M.Sc. degree (distinction) in Telecommunications Engineering in 2015, and the Ph.D. degree in Engineering in 2019 from Glasgow Caledonian University (GCU), UK. He is a Lecturer with the Glasgow College UESTC James Watt School of Engineering at the University of Glasgow (UofG) and Wave-1 Urban 5G use case implementation lead at Glasgow 5G Testbed (G5G) funded by the Scotland 5G Centre. Previously, he was a Research Associate involved in the planning, installation and commissioning of a campus wide 5G network as part of the Wave-1 Innovation Districts funded by the Scottish Government. His research interests include Wireless Communications, Internet of Things, Cooperative Intelligent Transport Systems, Autonomous Systems, Terrestrial/Airborne Mobile Networks, and Healthcare technologies.

Nguyen B. Truong is a lecturer at School of Computing Science, the University of Glasgow, UK. Previously, he was a Research Associate at Data Science Institute, Department of Computing, Imperial College London, UK in 2018-2022. He received his Ph.D, MSc, and BSc degrees from Liverpool John Moores University, UK, Pohang University of Science and Technology, Korea, and Hanoi University of Science and Technology, Vietnam in 2018, 2013, and 2008, respectively. He was a Software Engineer at DASAN Networks, a leading company on Networking Products and Services in South Korea in 2012-2015. His research interest is including, but not limited to, Data Privacy, Security, and Trust, Personal Data Management, Distributed Systems, and Blockchain.