Modelling the privacy landscape of the Internet of Vehicles

Ruben Cacciato
Dipartimento di Matematica e Informatica
Università di Catania
Catania, Italy
ruben.cacciato@studium.unict.it

Mario Raciti
IMT School for Advanced Studies Lucca
Lucca, Italy
Dipartimento di Matematica e Informatica
Università di Catania
Catania, Italy
mario.raciti@imtlucca.it

Sergio Esposito
Dipartimento di Matematica e Informatica
Università di Catania
Catania, Italy
sergio.esposito@unict.it

Giampaolo Bella
Dipartimento di Scienze Politiche e Sociali
Università di Catania
Catania, Italy
giamp@dmi.unict.it

ABSTRACT

Within the dynamic realm of Intelligent Transportation Systems (ITS), the Internet of Vehicles (IoV) marks a significant paradigm shift. IoV is an interconnected network of vehicles, infrastructures, and the Internet, driven by wireless communication technologies. This paper dissects the privacy landscapes of ITS and IoV, exploring gaps and redundancies in standards and academic literature. We do so by leveraging European Telecommunications Standards Institute (ETSI) ITS G5 standards and IoV analyses from literature, and building two relational models to depict said privacy landscapes. A macroscopic analysis reveals structural and thematic differences: ITS, governed by established standards, has a robust structure, while IoV, in its nascent stage, lacks formalisation. A detailed analysis highlights challenges in data collection, sharing, and privacy policies. As ITS transitions to IoV, increasing data volume demands enhanced privacy safeguards. Addressing these challenges requires collaborative efforts to develop comprehensive privacy policies, prioritise user awareness, and integrate privacy-by-design principles. This paper offers insights into navigating the evolving landscape of transportation technologies, laying the groundwork for privacy-preserving ITS and IoV ecosystems.

CCS CONCEPTS

• **Security and privacy**;

KEYWORDS

ITS, IoV, Privacy Landscape, Relational Model, Contrastive Analysis

ACM Reference Format:
Ruben Cacciato, Mario Raciti, Sergio Esposito, and Giampaolo Bella. 2024. Modelling the privacy landscape of the Internet of Vehicles. In *The 19th International Conference on Availability, Reliability and Security (ARES 2024), July 30–August 02, 2024, Vienna, Austria.* ACM, New York, NY, USA, 7 pages. https://doi.org/10.1145/3664476.3669977

ARES 2024, July 30–August 02, 2024, Vienna, Austria

ACM ISBN 979-8-4007-1718-5/24/07
https://doi.org/10.1145/3664476.3669977

1 INTRODUCTION

In the field of Intelligent Transportation Systems (ITS), the integration of cutting-edge communication technologies has been pivotal in enhancing traffic management, safety, and the environmental sustainability of transportation networks. ITS leverages a broad array of technologies to facilitate the dynamic exchange of information between vehicles, infrastructure, and pedestrian devices, aiming to improve the transportation ecosystem's efficiency and responsiveness [7]. The European Telecommunications Standards Institute (ETSI) has been instrumental in developing standards that underpin various applications and technologies constituting ITS.

A notable example is ETSI ITS G5 [6], which focuses primarily on vehicular communication systems designed to ensure interoperability and reliable performance across European roads. These standards encompass protocols, application guidelines, and communication frameworks that dictate the efficacy of ITS deployments.

Despite the comprehensive framework provided by ETSI, rapid advancements in vehicular technology and the rise of the Internet of Vehicles (IoV) [23] present new challenges and opportunities. IoV extends beyond traditional vehicular communication, incorporating more extensive data exchange and connectivity that promise enhanced vehicular services and automation. However, this evolution also introduces complexities in privacy, security, and data management, areas where existing standards may not fully align with current technological capabilities and societal expectations [22].

As an example of privacy issues for IoV, the wireless transmission of data between vehicles and infrastructure is vulnerable to interception, compromising personal and operational confidentiality. Furthermore, continuous tracking of vehicles by malicious actors can expose sensitive personal information, such as location habits and routines. Data aggregation across ITS and IoV networks can inadvertently create detailed individual profiles, potentially leading to unintended privacy breaches [11]. Moreover, the complexity of these networks introduces vulnerabilities that could be exploited, threatening data integrity and the overall security of transportation systems [10]. Additionally, attempts to use a temporary identifier

instead of the station canonical's one, as stated by ETSI [8] to prevent linking attacks, often fall short as the detailed nature of the data being transmitted between vehicles and between vehicles and infrastructure allows for possible re-identification [1], a risk intensified by the increasing volume of data in IoV.

This paper aims to dissect these complexities by analysing gaps and redundancies in current standards and academic literature with respect to both traditional ITS and the nascent IoV paradigm to model their privacy landscapes.

1.1 Context

The Internet of Vehicles (IoV) represents a significant evolution in the domain of Intelligent Transportation Systems (ITS), encompassing a large-scale distributed system for wireless communication and information exchange between vehicles, roads, humans, and the Internet. This system needs standardised communication protocols and data interaction guidelines to facilitate intelligent traffic management and Vehicle-to-Everything (V2X) communication [23].

The integration of 5G and edge cognitive computing (ECC) [4] has significantly advanced intra-vehicle communications, enhancing the speed, intelligence, and stability of interactions between wearable and vehicular devices. This improvement plays a critical role in ensuring the safety and comfort of individuals within vehicles and enhances the overall safety of the traffic system.

Inter-vehicle networks, which include all communicative vehicles sharing resources, add another dimension of complexity. On a larger scale, the Cognitive Internet of Vehicles (CIoV) [4] analyses data from a comprehensive network that includes intra-vehicle, adjacent vehicle, and environmental road data to bolster road traffic safety. The complexity of these systems necessitates stringent network reliability to prevent issues like personal data breaches and traffic system failures, highlighting the importance of joint physical and network space cognition. Furthermore, the IoV paradigm faces considerable challenges in privacy and security, underlined by the need for robust measures against potential cyber threats. Promoting a human-centred approach [4] helps to ensure service safety and the protection of personal information across these vehicular networks, thus addressing essential security aspects such as confidentiality, integrity, availability, and privacy [20].

Moreover, the absence of universally accepted standards presents considerable challenges in Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communications, impeding the scalability and integration of IoV systems across different regions and technologies [19]. The staged roll-out of IoV systems, beginning with low-risk implementations and advancing towards broader, systemic deployments, highlights the critical need for robust regulatory frameworks and widespread population adaptation. The integration of IoV with other infrastructures is imperative to create a holistic Internet of Things (IoT) ecosystem, enhancing collaboration and interconnection across various sectors.

In Europe, the ETSI ITS G5 standards serve as a cornerstone for ITS, aiming to ensure reliable V2V and V2I communications [6]. Formulated by the European Telecommunications Standards Institute (ETSI), these standards utilise technology based on IEEE 802.11p — a modification of the Wi-Fi standard tailored for automotive applications. This forms the basis for the Dedicated Short-Range Communications (DSRC) system, which operates within the 5.9 GHz band and is engineered for low-latency, high-reliability communications critical to automotive safety applications. The ETSI ITS G5 standards encompass protocols for various applications, including Cooperative Awareness Messages (CAM) and Decentralised Environmental Notification Messages (DENM). CAMs facilitate the regular exchange of basic vehicle information to enhance situational awareness, while DENMs alert drivers and automated systems to hazardous situations or emergency conditions in real-time. Comparatively, the US counterpart to ETSI ITS G5 is Wireless Access in Vehicular Environments (WAVE) [13], which also operates under the IEEE 802.11p standard and is institutionalised by the US Federal Communications Commission within the DSRC framework.

1.2 Motivation

Given the above context, it is crucial to model the current privacy landscapes of both ITS and IoV. With the term "privacy landscape", we refer to the intricate scenario of privacy concerns, regulations, and practices within a specific domain or technological ecosystem. It encompasses the dynamic interplay between technological advancements, regulatory frameworks, and societal expectations regarding the protection of personal data and privacy rights. This understanding is essential for evaluating the applicability and sufficiency of standards in addressing the privacy and security requirements of both ITS and the forthcoming IoV contexts.

There is a pronounced need to evaluate how the privacy landscape influences the development and implementation of standards within ITS and IoV. This involves conducting a systematic review of the protocol stack, key message types such as CAM and DENM, and the various application classes defined within these standards. For these reasons, it becomes imperative to provide a comprehensive overview of where the standards successfully support ITS and IoV functionalities and where they may fall short or exhibit inefficiencies, particularly from a privacy perspective.

This analysis is not only critical for assessing current capabilities, but also for anticipating the adjustments required to ensure that privacy considerations are adequately addressed as we transition from ITS to IoV.

1.3 Research Questions and Contributions

Building on the motivation given above, this paper addresses the following research questions:

> RQ1 *How can we model the privacy landscape of the Intelligent Transportation Systems?*
>
> RQ2 *How can we model the privacy landscape of the Internet of Vehicles?*
>
> RQ3 *What are the differences between the privacy landscape of the Intelligent Transportation Systems and the Internet of Vehicles?*

While answering such questions, we observe that there is a lack of standards in the IoV domain, due to the novelty of this new paradigm. In fact, existing standards are limited to the IoV predecessor, i.e., the ITS framework. Hence, this paper first investigates the privacy landscape of ITS, in particular at the European level, analysing the ETSI ITS G5 standards. Furthermore, with the IoV

paradigm emerging to replace ITS, this paper extends the initial exploration on ITS by analysing recent academic literature, so as to comprehensively obtain an overview of the privacy landscape for the IoV.

The main contributions of this paper are summarised as follows:

- A relational model that illustrates the privacy landscape of ITS, grounded in the ETSI ITS G5 standards.
- A relational model that illustrates the privacy landscape of IoV, informed by available academic research and potential standardisation gaps.
- A contrastive analysis between the privacy landscapes of ITS and IoV, highlighting the continuity and divergence in privacy as the technology transitions from ITS to IoV.

The remainder of this paper follows a linear structure. Section 2 reviews related work. Section 3 describes the modelling method adopted for designing the relational models presented in Section 4. Section 5 advances a contrastive analysis between the relational models, and Section 6 offers concluding remarks on our work.

2 RELATED WORK

The convergence of Intelligent Transportation Systems (ITS) and the Internet of Vehicles (IoV) has precipitated numerous privacy and security concerns addressed in various research studies. This Section reviews notable works in the field.

Ometov et al. [16] provided a comprehensive overview of positioning information privacy within ITS, highlighting the impact of European Union regulations and suggesting directions for future privacy strategies. Their discussion encapsulates the regulatory landscape and its implications for privacy in ITS.

Sadiku et al. [18] explored the ITS standards in relation to IoV. They discuss the privacy issues that emerge when tracking vehicles and individuals, emphasising the need for robust privacy-preserving mechanisms in ITS developments.

Butt et al. [3] reviewed privacy management challenges within the social aspects of IoV. They proposed the use of blockchain technology as a novel solution to enhance privacy and security in vehicular networks, providing a detailed analysis of blockchain's potential to address inherent privacy issues.

Hahn et al. [12] classified and analysed prevalent security and privacy issues in ITS. Their study employs a model-driven approach to better understand and mitigate the challenges faced in securing ITS architectures.

Sun et al. [21] focused on the integration of security and privacy requirements in IoV systems. They provided insights into the necessary frameworks that need to be established to support the safe deployment of ITS services.

Boualouache et al. [2] examined pseudonym changing strategies in Vehicular Ad-Hoc Networks (VANETs), identifying them as essential for protecting location privacy. Their review categorises these strategies and discusses their effectiveness against pseudonyms linking attacks, highlighting the ongoing need for robust solutions to prevent adversaries from tracking vehicles.

Petit et al. [17] systematically categorised and compared pseudonym schemes based on cryptographic approaches. They also offered insights into the state of standardisation in the field, along with identifying open research challenges that need to be addressed.

Zavvos et al. [24] explored privacy and trust challenges inherent in the IoV, emphasising the need for a holistic approach to address privacy concerns at the service level. As we shall see below, our paper builds on this work for the design of the relational model for the privacy landscape of IoV.

Each of these studies contributes to the state of the art by proposing frameworks, identifying challenges, and suggesting potential solutions to enhance privacy and security in ITS and IoV ecosystems. However, to the best of our knowledge, this paper presents the first work that uses relational models to analyse the privacy landscape of the Intelligent Transportation Systems and the Internet of Vehicles, and the first to perform a contrastive analysis between them.

3 OUR MODELLING METHOD

Our literature analysis covers the available European standards and recent scientific contributions that are relevant to both the ITS and IoV domains. In our modelling method, we adopt the Crow's foot notation [15], which is a standard diagramming technique used for representing relational database structures. The distinguishing feature of this notation lies in the graphical symbols denoting the "more" (one or more) side of relationships. Resembling a crow's foot, these symbols are the hallmark of this notation, hence its name.

A brief recall of the key components and their meanings in Crow's foot notation is given below:

- *Entities*: Represented by rectangles, entities are the objects or concepts about which data is stored, such as "Customer" or "Order". The entity's name is positioned at the top of the rectangle.
- *Attributes*: Below the entity's name, attributes are the properties or details of an entity, such as "Customer Name" or "Order Date".
- *Relationships*: Depicted by lines connecting entities, relationships illustrate how entities interact with one another. The nature of the relationship is indicated by symbols at each end of the line.
- *Cardinality*: Specifies how many instances of one entity can or must be associated with each instance of another entity. Cardinality is indicated by symbols such as:
  - A single line (|) for "one".
  - A three-pronged "crow's foot" for "many".
  - An optional circle or zero (O) to represent "zero or more".
  - A vertical bar (|) combined with a crow's foot to indicate "one or more".
- *Participation*: Denotes whether the relationship is optional or mandatory. Mandatory participation is shown by a line without a circle, whereas optional participation is indicated by adding a circle.

Briefly, our modelling method examines the relevant entities and their relationships in state-of-the-art documents, focusing on potential privacy gaps.

4 MODELLING THE LANDSCAPE

This Section presents the relational models for the privacy landscape of the Intelligent Transportation Systems and the Internet of Vehicles, hereafter referred to as the (relational) models for ITS

and IoV. The description of our relational models is conveniently structured into two subsections below.

4.1 A Relational Model for ITS

The relational model for Intelligent Transportation Systems comprises a total of ten entities, each representing a distinct aspect of the ITS ecosystem. The model builds upon the ETSI ITS G5 standards [6] and is depicted in Figure 1.

The choice of standards at the European level clearly affects the resulting model, as we shall detail below, and is founded upon two key factors: firstly, the significant similarities between ETSI ITS G5 and its American counterpart IEEE WAVE, particularly in their fundamental aim of enhancing road safety and facilitating intelligent transportation systems; and secondly, the profound influence of GDPR within the European Union, emphasising the paramount importance of privacy and data protection.

The first entity that we consider is Intelligent Transportation System (ITS) Domain, which represents the overarching context of the model, encompassing all components related to transportation systems that utilise information and communications technology to improve safety, efficiency, and the environment.

ITS Domain has two relationships with the ETSI standards that are conveniently divided into two separate entities. One is ETSI ITS G5 Basic Set of Applications [5], which contains a catalogue of V2X applications and use cases, grouped respectively by Applications Class and Application. The other is ETSI ITS G5 Other Standards, which gathers the list of documents that specify the five layers of the ETSI ITS G5 Protocol Stack, as presented by Fernandes et al. [9]. Both the ETSI ITS G5 entities refer to ITS Domain.

Finally, since ETSI has standardised two fundamental types of messages, we specialise the entity Message with CAM and DENM entities, both supporting more than a Use Case. Notably, all entities have no attributes, with the only exception for CAM and DENM.

4.2 A Relational Model for IoV

The relational model for Internet of Vehicles includes a total of five entities, each representing a distinct aspect of the IoV ecosystem. The model relies on the list of IoV services, information categories and privacy concerns presented by Zavvos et al. [24] and is depicted in Figure 2.

The choice of Zavvos et al. as the only document for IoV clearly affects the resulting model, as we shall detail below, and derives from the comprehensiveness and depth of their analysis regarding privacy concerns in IoV services and the absence of consolidated IoV standards. Their work offers valuable insights into the potential risks and implications associated with the collection, processing, and sharing of vehicular data.

The first entity is Internet of Vehicles (IoV) Domain, which encapsulates the interconnectedness of vehicles, infrastructure, and devices through network technologies to enhance transportation efficiency and safety.

The Zavvos et al. entity refers to the IoV Domain entity and also has a relationship with the IoV Service entity, as the work by Zavvos et al. [24] contains a list of services whose privacy concerns are systematically categorised by the authors into four basic categories: personal information privacy, multi-party privacy, trust, and consent to share information [24]:

- **Personal information privacy** raises significant challenges as users are required to share personal data to access IoV services, while facing risks of exploitation due to extensive data collection and storage. Achieving a balance between the provision of high-quality services and the minimal use of user data becomes a complex and nuanced endeavor.
- **Multi-party privacy** arises as a pressing issue, since the interconnected nature of the IoV heightens fears of breaching third-party privacy. In fact, the seamless exchange of information across multiple entities can lead to inadvertent privacy violations, and the monitoring of activities across IoV networks could severely undermine trust in the system.
- **Trust** assumes various forms within the IoV ecosystem, encompassing user-provider trust, inter-user trust, and trust in the IoV infrastructure itself. Ensuring trust is vital for the widespread adoption of IoV technologies, as a lack of trust may impede users from sharing information or engaging with IoV services.
- **Obtaining consent for data sharing** presents a complex challenge, as users grapple with unclear privacy trade-offs and the need for real-time consent management, which potentially disrupts user experiences in the IoV environment.

The last entity of the model for IoV is called Information Category. In fact, information has been arranged by Zavvos et al. according to its typical uses and into categories that, when combined, may present hazards to the user if not properly managed.

For example, the ID category pertains to uniquely identifying elements, such as vehicle details, user credentials, or third-party entities. Said identification is crucial for the functionality and security of IoV services. The GPS category offers insights into geolocation, velocity, direction of the vehicle at any point in time, and it is crucial for tracking movement. The Route Information category encompasses the origin, destination, and path of travel for a vehicle. The Multimedia Feeds category encompasses visuals and audio obtained from onboard sensors or external devices, and can enhance situational awareness and safety. The Profiles category is built from diverse data like behavioural patterns, health records, and emotional states. The Interests and Relationships category sheds light on personal preferences and social connections, enriching the user experience. Finally, the Other category encompasses information from sensors like RADAR or LIDAR, expanding the scope of data collection beyond the mentioned categories.

These facets collectively provides a thorough understanding of individuals, vehicles, and their interactions within various contexts.

5 CONTRASTIVE ANALYSIS

The relational models presented in Section 4 serve as the foundation for conducting a contrastive analysis between the privacy landscapes of ITS and IoV. For the sake of clarity, this Section is conveniently structured into two subsections. The first subsection provides a contrastive analysis of the two relational models at a macroscopic level, outlining their broad structural and thematic differences. The second subsection delves into a detailed contrastive

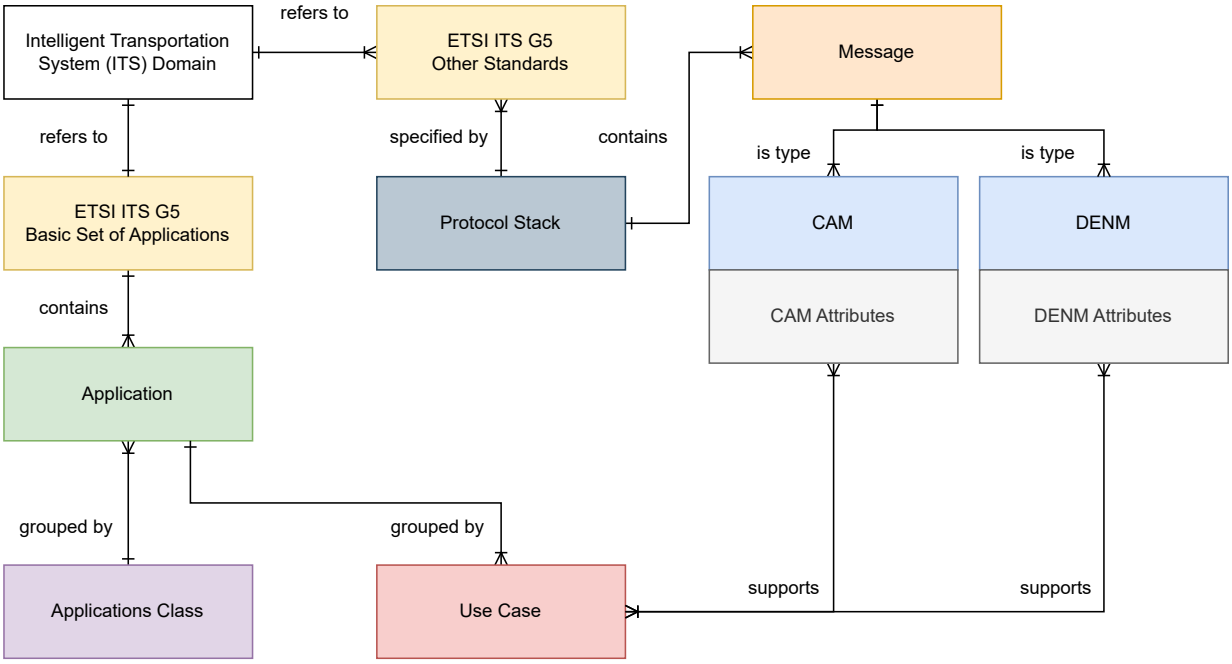

Figure 1: Relational Model for ITS.

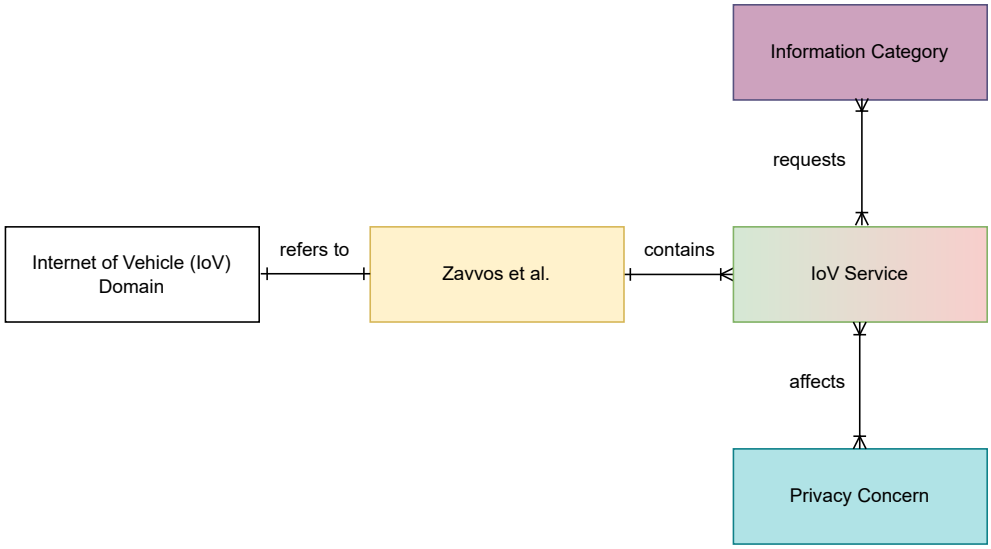

Figure 2: Relational Model for IoV.

analysis, examining the specific elements and implications of each model in depth, along with privacy considerations.

5.1 Macroscopic Analysis

We undertake an initial comparative analysis at a macroscopic level between the relational models. As stated in Section 4, both the relational models are affected by the selected documents, i.e. the ETSI standards and the work by Zavvos et al., which clearly imply some

restrictions in terms of completeness, a well-known open problem in the field of modelling. In particular, the model for ITS reflects the European landscape as it leverages the ETSI ITS G5 standards. By contrast, the model for IoV is based on the contribution by Zavvos et al. Both choices introduce inherent limitations to the models, as they may not fully encapsulate global ITS and IoV privacy issues. Additionally, the relational models depend on the availability and accuracy of current literature, which may not completely represent the rapidly evolving IoV landscape. Nevertheless, their structured approach facilitates a comprehensive understanding and analysis, enabling effective navigation through the complexities of ITS and IoV, and ultimately fostering innovation in these domains.

Moreover, a disparity in dimensionality between the two models exists, attributable to the comprehensive structure provided by ETSI standards in contrast to the nascent IoV paradigm. The relational model for ITS exhibits a considerable breadth of entities and relationships, indicative of a robust and well-defined structure. Conversely, the relational model for IoV, existing solely as a paradigm, lacks the formalised structure and depth characteristic of established standards such as those promulgated by ETSI.

The originality of the model for IoV lies in its capacity to adapt within the evolving landscape of transportation technologies, leveraging the embryonic state of IoV to pioneer novel approaches and address emerging challenges with agility and foresight.

5.2 Detailed Analysis

By analysing the relational models for ITS and IoV at a microscopic level, both similarities and disparities emerge. A first similarity is the inclusion of the documents in both the models: in the model for ITS we have the ETSI standards, while in the model for IoV just the contribution by Zavvos et al.. In Figures 1 and 2, the entities representing these documents are highlighted in yellow.

It is noteworthy to highlight that the entities Application and Use Case, included in the model for ITS, are missing in the model for IoV. In fact, both these entities are integrated into the IoV Service entity. For example, the IoV service “Driver Assistance” is comparable with the application “Driving assistance”. By contrast, the IoV service “Safety Warnings” can be mapped to the use case “Wrong way driving warning”. The double nature of IoV Service is illustrated in Figure 2, where the entity has a double colour of green-red, with green representing the equivalence with Application and red with Use Case. Hence, the lack of rigour in the classification of the IoV services from Zavvos et al. finds a mitigation in our relational models. The remaining entities of the models for ITS and IoV are coloured differently, as we cannot identify any similarities.

Moreover, a notable absence in the relational model for IoV is the concept of Application Class, which holds significance in the ITS framework. In fact, the ETSI ITS G5 Basic Set of Applications groups Applications into distinct classes, i.e., Active road safety and Cooperative traffic efficiency, Co-operative local services, Global internet services, to facilitate organised categorisation. However, in the IoV context, the conventional notion of an Application undergoes a transformative shift. As described above, Application is redefined under IoV Service, encompassing a broader spectrum of functionalities and services tailored to the IoV ecosystem.

Unlike the ETSI ITS G5, where the delineation and standardisation of a Protocol Stack play a pivotal role, the IoV paradigm lacks a definitive network architecture. While numerous researchers propose various design schemes for IoV architectures [14], a unanimous consensus remains elusive. Consequently, the absence of an accepted Protocol Stack precludes its inclusion in the relational model for IoV.

Furthermore, in contrast to the relational model for ITS, where Message types, such as Cooperative Awareness Message (CAM) and Decentralised Environmental Notification Message (DENM), serve as integral components within the Protocol Stack hierarchy, their absence in the relational model for IoV is conspicuous. This omission is intrinsically linked to the absence of an established Protocol Stack in the IoV domain.

Finally, the entity Privacy Concern is present only in the model for IoV, reflecting Zavvos et al.’s inclusion of privacy concerns in their treatment of IoV. By contrast, the ETSI ITS standards lack of a thorough consideration of privacy, as evidenced by the missing Privacy Concern entity in the model for ITS.

When observing the specific applications and use cases included in the ETSI ITS G5 Basic Set of Applications alongside the IoV services provided in Zavvos et al., the transition from ITS to IoV translates to an increase in the number of applications, which in turn implies an extension of the use cases. Consequently, we identify a set of IoV services with no counterpart in the ITS domain. These IoV services are: Parking Finder, Intention-aware routing, Cooperative charging, Vocal warnings, Sensing tasks, Voice chat.

From the above considerations, several privacy issues that require attention can be identified:

- *Data collection and storage*: In the transition from ITS to IoV, there arises a pressing need for the collection of an expanding volume of data. This encompasses a spectrum ranging from vehicle location and speed to driver behaviour and environmental conditions. However, the proliferation of connected devices and sensors in IoV exacerbates concerns regarding the scope and sensitivity of data being gathered. This influx of data raises questions about the necessity and proportionality of data collection practices, as well as the adequacy of measures to anonymise or pseudonymise personally identifiable information. Furthermore, storing this data poses risks of security breaches leading to unauthorised access, and raises concerns about long-term retention.
- *Data sharing and access control*: The seamless connectivity inherent in IoV facilitates the sharing of data among various stakeholders, including government agencies, transportation operators, and third-party service providers. While data sharing holds promise for enhancing traffic management and fostering innovation, it also heightens concerns about data security and privacy. Issues such as inadequate access controls, insufficient encryption, and unclear data ownership rights can lead to unauthorised data access and misuse, potentially compromising individuals’ privacy.
- *Privacy policies and consent mechanisms*: Effective privacy protection requires clear and comprehensive privacy policies that outline how data will be collected, used, and shared within IoV ecosystem. Addressing the lack of transparency

and specificity in these policies is crucial [3]. Moreover, consent mechanisms for data collection and processing may be insufficient, leaving users unaware of the extent to which their data is being utilised and without meaningful options to exercise control over their personal information.

- *Privacy-by-design*: Privacy-by-design principles advocate for the integration of privacy safeguards into the design and development of IoV systems from their inception. While such principles hold promise for mitigating privacy risks, their implementation remains uneven across different applications and contexts. Inadequate attention to privacy considerations during system design can result in vulnerabilities and loopholes that undermine individuals' privacy rights.
- *User awareness and control*: Central to ensuring privacy in IoV environment is the empowerment of users with awareness and control over their personal data. Yet, user awareness campaigns and educational initiatives regarding privacy risks and protective measures are often lacking. Moreover, the absence of user-friendly tools and interfaces for managing data preferences and consent settings further diminishes users' ability to exert control over their privacy.

6 CONCLUSIONS

This paper addressed the challenge of modelling the privacy landscape of the Internet of Vehicles. It did so by adopting a modelling approach that involved designing two relational models for the privacy landscapes of the Intelligent Transportation Systems and the Internet of Vehicles. This answered RQ1 and RQ2.

Furthermore, this paper advanced a contrastive analysis between the privacy landscapes of ITS and IoV. The analysis revealed structural and thematic differences between ITS and IoV, and highlighted gaps and redundancies that are present in the current European standards and literature. This answered RQ3.

The findings suggest an urgent need for policymakers and industry stakeholders to revisit and revise existing standards to align with the advanced privacy requirements of IoV. The standardisation of IoV will not only mitigate privacy risks but also foster awareness and trust among users, which are essential for the broader acceptance and success of IoV technologies.

ACKNOWLEDGMENTS

Sergio Esposito acknowledges financial support from: PNRR MUR project PE0000013-FAIR.
Giampaolo Bella and Mario Raciti acknowledge financial support from: PRIN 2022 MUR project E53D23008220006-FuSeCar.

REFERENCES

[1] Sebastian Bittl and Arturo A Gonzalez. 2015. Privacy endangerment from protocol data sets in vanets and countermeasures. In *Smart Cities, Green Technologies, and Intelligent Transport Systems: 4th International Conference, SMARTGREENS 2015, and 1st International Conference VEHITS 2015, Lisbon, Portugal, May 20-22, 2015, Revised Selected Papers 4*. Springer, 304–321.

[2] Abdelwahab Boualouache, Sidi-Mohammed Senouci, and Samira Moussaoui. 2018. A Survey on Pseudonym Changing Strategies for Vehicular Ad-Hoc Networks. *IEEE Communications Surveys & Tutorials* 20, 1 (2018), 770–790. https://doi.org/10.1109/COMST.2017.2771522

[3] Talal Ashraf Butt, Razi Iqbal, Khaled Salah, Moayad Aloqaily, and Yaser Jararweh. 2019. Privacy Management in Social Internet of Vehicles: Review, Challenges and Blockchain Based Solutions. *IEEE Access* 7 (2019), 79694–79713. https://doi.org/10.1109/ACCESS.2019.2922236

[4] Min Chen, Yuanwen Tian, Giancarlo Fortino, Jing Zhang, and Iztok Humar. 2018. Cognitive Internet of Vehicles. *Computer Communications* 120 (2018), 58–70. https://doi.org/10.1016/j.comcom.2018.02.006

[5] ETSI. 2009. ETSI TR 102 638 V1.1.1 (2009-06); Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Definitions. https://www.etsi.org/deliver/etsi_tr/102600_102699/102638/01.01.01_60/tr_102638v010101p.pdf.

[6] ETSI. 2010. ETSI ITS G5. https://www.etsi.org/committee/1402.

[7] ETSI. 2018. Intelligent Transport Systems. https://www.etsi.org/images/files/ETSITechnologyLeaflets/IntelligentTransportSystems.pdf.

[8] ETSI. 2022. ETSI TS 102 941 V2.2.1 (2022-11); Intelligent Transport Systems (ITS); Security; Trust and Privacy Management; Release 2. https://www.etsi.org/deliver/etsi_ts/102900_102999/102941/02.02.01_60/ts_102941v020201p.pdf.

[9] Bruno Fernandes, Joao Rufino, Muhammad Alam, and Joaquim Ferreira. 2018. Implementation and analysis of IEEE and ETSI security standards for vehicular communications. *Mobile Networks and Applications* 23 (2018), 469–478.

[10] Tanvi Garg, Navid Kagalwalla, Prathamesh Churi, Dr. Ambika Pawar, and Sanjay Deshmukh. 2020. A survey on security and privacy issues in IoV. *International Journal of Electrical and Computer Engineering (IJECE)* 10 (10 2020), 5409. https://doi.org/10.11591/ijece.v10i5.pp5409-5419

[11] Catalin Gosman, Ciprian Dobre, and Florin Pop. 2017. Privacy-preserving data aggregation in Intelligent Transportation Systems. In *2017 IFIP/IEEE Symposium on Integrated Network and Service Management (IM)*. 1059–1064. https://doi.org/10.23919/INM.2017.7987438

[12] Dalton Hahn, Arslan Munir, and Vahid Behzadan. 2021. Security and Privacy Issues in Intelligent Transportation Systems: Classification and Challenges. *IEEE Intelligent Transportation Systems Magazine* 13, 1 (2021), 181–196. https://doi.org/10.1109/MITS.2019.2898973

[13] IEEE. 2016. IEEE Standard for Wireless Access in Vehicular Environments–Security Services for Applications and Management Messages. *IEEE Std 1609.2-2016 (Revision of IEEE Std 1609.2-2013)* (2016), 1–240. https://doi.org/10.1109/IEEESTD.2016.7426684

[14] Baofeng Ji, Xueru Zhang, Shahid Mumtaz, Congzheng Han, Chunguo Li, Hong Wen, and Dan Wang. 2020. Survey on the Internet of Vehicles: Network Architectures and Applications. *IEEE Communications Standards Magazine* 4, 1 (2020), 34–41. https://doi.org/10.1109/MCOMSTD.001.1900053

[15] Robert J Muller. 1999. *Database design for smarties: using UML for data modeling*. Morgan Kaufmann.

[16] Aleksandr Ometov, Sergey Bezzateev, Vadim Davydov, Anna Shchesniak, Pavel Masek, Elena Simona Lohan, and Yevgeni Koucheryavy. 2019. Positioning Information Privacy in Intelligent Transportation Systems: An Overview and Future Perspective. *Sensors* 19, 7 (2019). https://doi.org/10.3390/s19071603

[17] Jonathan Petit, Florian Schaub, Michael Feiri, and Frank Kargl. 2015. Pseudonym Schemes in Vehicular Networks: A Survey. *IEEE Communications Surveys & Tutorials* 17, 1 (2015), 228–255. https://doi.org/10.1109/COMST.2014.2345420

[18] Matthew N. O. Sadiku, Nishu Gupta, Kirtikumar K. Patel, and Sarhan M. Musa. 2021. *An Overview of Intelligent Transportation Systems in the Context of Internet of Vehicles*. Springer International Publishing, Cham, 3–11. https://doi.org/10.1007/978-3-030-46335-9_1

[19] Lion Silva, Naercio Magaia, Breno Sousa, Anna Kobusińska, António Casimiro, Constandinos X Mavromoustakis, George Mastorakis, and Victor Hugo C De Albuquerque. 2021. Computing paradigms in emerging vehicular environments: A review. *IEEE/CAA Journal of Automatica Sinica* 8, 3 (2021), 491–511.

[20] Lion Silva, Naercio Magaia, Breno Sousa, Anna Kobusińska, António Casimiro, Constandinos X. Mavromoustakis, George Mastorakis, and Victor Hugo C. de Albuquerque. 2021. Computing Paradigms in Emerging Vehicular Environments: A Review. *IEEE/CAA Journal of Automatica Sinica* 8, 3 (2021), 491–511. https://doi.org/10.1109/JAS.2021.1003862

[21] Yunchuan Sun, Lei Wu, Shizhong Wu, Shoupeng Li, Tao Zhang, Li Zhang, Junfeng Xu, and Yongping Xiong. 2015. Security and Privacy in the Internet of Vehicles. In *2015 International Conference on Identification, Information, and Knowledge in the Internet of Things (IIKI)*. 116–121. https://doi.org/10.1109/IIKI.2015.33

[22] Hamideh Taslimasa, Sajjad Dadkhah, Euclides Carlos Pinto Neto, Pulei Xiong, Suprio Ray, and Ali A. Ghorbani. 2023. Security issues in Internet of Vehicles (IoV): A comprehensive survey. *Internet of Things* 22 (2023), 100809. https://doi.org/10.1016/j.iot.2023.100809

[23] W. Wu, Z. Yang, and K. Li. 2016. Chapter 16 - Internet of Vehicles and applications. In *Internet of Things*, Rajkumar Buyya and Amir Vahid Dastjerdi (Eds.). Morgan Kaufmann, 299–317. https://doi.org/10.1016/B978-0-12-805395-9.00016-2

[24] Efstathios Zavvos, Enrico H. Gerding, Vahid Yazdanpanah, Carsten Maple, Sebastian Stein, and m.c. schraefel. 2022. Privacy and Trust in the Internet of Vehicles. *IEEE Transactions on Intelligent Transportation Systems* 23, 8 (2022), 10126–10141. https://doi.org/10.1109/TITS.2021.3121125