Karlsruhe Reports in Informatics 2023,3
Edited by Karlsruhe Institute of Technology,
Faculty of Informatics
ISSN 2190-4782

Mobility Data Anonymization – A Literature Review and an Industry-Driven Survey

Maximilian Walter, Wasilij Beskorovajnov, Fridtjof Lieberwirth, Jan Sürmeli, Pascal Zwick, Robert Heinrich

2023

KIT – The Research University in the Helmholtz Association

Mobility Data Anonymization – A Literature Review and an Industry-Driven Survey

Maximilian Walter[KIT], maximilian.walter@kit.edu
Wasilij Beskorovajnov[FZI], beskorovajnov@fzi.de
Fridtjof Lieberwirth[DFE], lieberwirth@dresearch-fe.de
Jan Sürmeli[FZI], suermeli@fzi.de
Pascal Zwick[FZI], zwick@fzi.de
Robert Heinrich[KIT], robert.heinrich@kit.edu

August 2023

KIT Karlsruhe Institute of Technology (KIT), Karlsruhe, Germany
FZI FZI Forschungszentrum Informatik, Karlsruhe, Germany
DFE DReserach Fahrzeugelektronik GmbH, Berlin, Germany

Findings from the Project "Competence Cluster Anonymization for Connected Mobility Systems" (ANYMOS)

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

Finanziert von der Europäischen Union
NextGenerationEU

Abstract

The transformation of mobility is on the cusp of a significant shift, driven by data-centric technologies in both individual and public transport. However, this data often contains sensitive private data, which can be used, for instance, for tracking a person. Hence, anonymization of this mobility data is important. In this report, we present a structured literature review about anonymization methods in the mobility domain. Based on our findings, we present different anonymization methods and discuss their application scenarios and characteristics for public transport and individual one. Additionally, an industry-driven survey on anonymization methods within public transport, particularly centered around video technologies, is presented. This industry-driven survey, conducted within a video surveillance solutions company, highlights current trends and underscores the necessity for continued research. This report was created within the ANYMOS project.

1 Introduction

The future of mobility is poised to undergo a profound transformation fueled by the pervasive influence of data-driven technologies in both individual and public transport. This paradigm shift is propelled by two major driving forces: the steady progression towards automated mobility systems and the strategic endeavor to scale up public transport networks. The advent of autonomous vehicles, spanning from passenger cars to shuttle buses and delivery robots, mandates a perpetual awareness of other road users' behaviors to ensure safe and efficient operations. Achieving the desired expansion of public transport necessitates leveraging existing infrastructure more efficiently, wherein meticulous data analysis enables accurate capacity forecasts and personalized user recommendations to optimize utilization.

To catalyze innovation and foster healthy competition, a variety of stakeholders must have access to mobility data. Simultaneously the privacy of individuals needs to be safeguarded, in line with the stringent requirements outlined in the EU Data Protection Regulation. In this report, mobility data is synonymous to data in the transportation section including public transportation, e.g., buses or trams, and private transportation, e.g., cars or bikes. Effective data anonymization or pseudonymization methods play a pivotal role in striking this balance. As the lines blur between individual and public transport, intelligent and adaptable mobility solutions emerge as the frontrunners, propelling traditional distinctions into the background.

This technical report is a result of the ANYMOS [1] research project and represents the findings of work package 5.1. The scope of this work package, and this report, encompasses:

1. A comprehensive literature review, following the guidelines of Kitchenham *et al.* [2]. The review aims to offer valuable insights and address

challenges in the pursuit of a data-powered future of mobility.

2. An industry-driven survey by DFE focusing on anonymization methods in public transport, particularly for camera-based data. The survey will list the current industrial approaches and identifies key challenges from an industry perspective.

The paper reports on both parts, and is structured as follows. We describe the configuration of our literature review in section 3, and report the results of our review in section 4. We discuss our findings and interpret them in section 5, and examine limitations in section 6. The survey performed by DFE is presented and discussed in section 7. We conclude our report in section 8.

2 Work Package Goals and Description

In the later section, we introduce our configuration for the literature review. The configuration is built upon our work package goals and requirements as written in our project proposal. In this section, we summarize the research goals of our working package 5.2 in the ANYMOS project.

This research project revolves around anonymization and aims to establish the foundation for a toolkit of methods for the ANYMOS project. The primary objective is to systematically investigate the current state of the art in the mobility domain.

To achieve this, the project entails a systematic literature review. The formulation of specific search queries for anonymization methods will be a key step. Concurrently, criteria suitable for effectively comparing the identified methods will be defined. Subsequently, these methods will be compared based on the established criteria, highlighting their respective advantages, disadvantages, and application domains.

One of the significant contributions of this work package is the development of competence in the application of anonymization methods in the mobility domain. The research findings will be summarized in a technical report, offering insights into the current state of the art. Through this analysis, the work package seeks to provide a foundation for other work packages, address limitations, and enable further advancements in this domain. The protocols used in the literature review, including the configurations and results, will be documented. In addition, the work package will assess and reflect upon the literature review results.

A general overview of our research project can be found in Kneis *et al.* [1].

3 Configuration

We performed a structured literature review based on the guidelines from Kitchenham *et al.* [2] to answer our research questions. Based on the guidelines and our project description, the first step is to develop a search configuration. As recommended by Kitchenham *et al.* [2], we first derived a configuration and then performed a prestudy, where we tested our configuration. Based on the prestudy results, we refined the initial configuration. In the following, we will only report on the final configuration. However, the detailed changes in the configuration and results of the prestudy can be found in our data set [3]. In addition, the data set also contains the detailed final configuration.

3.1 Research Questions

The first step in the configuration is to explicitly define the research questions to be answered by the literature review. We derived the research question based on our initial task description of our research project ANYMOS[1]. In the following, we first list the research question and then describe the reason for the question in more detail. Our research questions are:

RQ1 What are data anonymization methods used in the mobility domain?

RQ2 What are typical application scenarios for data anonymization methods in the mobility domain?

RQ3 What type of data is anonymized?

RQ4 What are the advantages of certain data anonymization methods in the mobility domain?

RQ5 What are the disadvantages of certain data anonymization methods in the mobility domain?

The first research question **RQ1** investigates anonymization methods in the mobility domain. We concentrate on anonymization methods because our work packages should provide an overview of the used anonymization approaches. The application domain is the mobility domain. As previously stated, mobility refers to public transport and private cars. The mobility focus is also based on our task description because it explicitly names approaches in the mobility domain.

The second research question **RQ2** investigates the scenarios in which data anonymization methods are used. This is important because the different anonymization approaches can differ between different scenarios. This means, we cannot investigate an anonymization method without considering

[1] ANYMOS project page: `https://www.anymos.de/`

the application scenario for it. Additionally, the same aspect is found in our work package description.

The third research question **RQ3** investigates which data is anonymized. This question is important because different mobility data might require different anonymization methods. For example, location data through GPS position may be anonymized differently than the name of a person. Consequently, we need to identify for which data the anonymization methods can be used.

The fourth research question **RQ4** and the fifth research question **RQ5** investigate the advantages and disadvantages of a certain anonymization method. They are important because they enable us to compare the different anonymization methods in a certain scenario. The previous questions only give us insights regarding the potential application areas but do not discuss how good a method is in these areas. These two research questions are there to enable this discussion. In addition, these questions are also directly derived from our initial task description.

3.2 Search Terms, Inclusion & Exclusion Criteria

We decided to perform a database search to identify the relevant literature for our review. The database search is beneficial, in our case, because we did not have prior knowledge on anonymization methods in the mobility domain. For the database search, we need to identify keywords and then build search terms. These search terms are then used to query a database with the help of a search engine. We derived the search terms based on our task definition in our project proposal and the previously presented research questions. We first identified the important keywords. In our project, we want to investigate the *anonymization* in *mobility systems*. We look at mobility systems that consist of two aspects, a car related part with *automotive* and a *public transport* part. Based on these aspects, we then identified synonyms through related work or prior knowledge of the authors. After finding the keywords and the synonyms, we derived the search terms. In our case, we split the search terms into two terms. The first search term investigates more general anonymization methods in mobility systems. The second search term focuses on tracking entities within a mobility system. Our two search terms are:

1. $(Anonymization|Privacy)\&(\text{"}mobility\ system\text{"}|$ $automotive|in-vehicle|\text{"}public\ transport\text{"}|\text{"}transportation\ system\text{"})$
2. $(privacy|anonym|Pseudo)\&(\text{"}driver\ identification\text{"}|trajectory|$ $\text{"}passenger\ tracking\text{"})\&(mobility|\text{"}transportation\ system\text{"}|$ $automotive|in-vehicle)$

The ampersand (&) stands for a conjunction ("and") and the pipe | for a disjunction ("or") of keywords. In case of a keyword consisting of multiple

words, such as *public transport*, we use quotation marks to indicate the complete keyword.

While our search terms would yield a set of publications, this set might still include irrelevant publications. Therefore, we defined the following inclusion and exclusion criteria, as recommended by Kitchenham *et al.* [2].

- Inclusion Criteria
  - any data anonymization method within the mobility domain,
  - methods as foundations for the method kit.
- Exclusion Criteria
  - non-English publications,
  - non peer-reviewed publications,
  - sole description of attacks on anonymization/privacy,
  - non-privacy or non-anonymization approaches (e.g. Integrity ...),
  - no full text of the publication available,
  - surveys,
  - challenge papers,
  - vision papers.

Based on our research questions, we derived the criteria as suggested by Kitchenham *et al.* [2]. In addition, we used our task description. Our inclusion criteria selects publications with anonymization or approaches for the method kit. We excluded non-English publications because English results increase the reproducibility, and we might not be able to understand other languages. We also only wanted to include peer-reviewed publications to increase the scientific quality and only to identify approaches with a certain maturity. We also excluded publications that only discuss attacks because they do not provide methods for our kit. In addition, another work package in ANYMOS investigates attacks. We also excluded publications that do not investigate anonymization or privacy because other security properties are, in our case, not relevant. We also excluded publications where we could not access the full text. In addition, we excluded survey, challenge, and vision papers because they do not provide methods, which was the goal for our survey.

3.3 Search Engines

In the next step, we selected search engines. Our selection criteria for the search engines were (1) support for our search terms and (2) indexation of commonly used publication venues in computer science. Based on these criteria, we chose the following four search engines:

1. *Google Scholar*[2]
2. *IEEE Xplore*[3]
3. *ACM Digital Library*[4]
4. *Semantic Scholar*[5].

In addition to the mentioned engines, we also considered the search engines of Springer and Elsevier, respectively. However, they did not comply to our first criterion: We could not enter our search terms since they do not support sophisticated search queries. However, *Google Scholar* includes the results from Springer and Elsevier.

For each selected search engine, we slightly adapted the search terms syntactically, so that the term corresponded to the required syntax of the search engine. Originally, we planned to apply the search terms to both abstract and title where supported by the search engine. However, due to a high number of results (e.g., 637 publications only for IEEE) and a high number of false positives we found in the results, we decided to apply the search term only to the titles. Afterward, we extracted the found papers, removed duplicates and applied our inclusion and exclusion criteria. We used the title and abstract to decide the conformance to exclusion and inclusion criteria. Where title and abstract were insufficient, we used the conclusion of the respective paper. We performed our search at the start of July 2023, and as such only papers published at this point time could be considered.

3.4 Data Extraction Form

Table 1 illustrates the data we extracted for every *valid* publication. A publication is valid if it was identified in the previous steps taking into account our inclusion and exclusion criteria. The left column contains our considered data fields, the right column describes possible values. While some data fields are enumerations of predefined values, some fields allow free text and are marked accordingly with *free text*.

The first four data fields are metadata regarding the reviewer of the paper or the paper itself. In our tooling [4], the fields *Authors*, *Title* and *Identifier* are automatically extracted based on the BibTeX file containing the found literature. Afterward, we collect the name of the approach. This is important, especially if approaches are repeatedly mentioned in different publications. The field *domain* relates to our **RQ2**, and as such provides three possible answers: *Public Transport*, *In-Vehicle* or a free text field represented by *Other*. The next field *Data Types* is used to answer our

[2] `https://scholar.google.de/`
[3] `https://ieeexplore.ieee.org/Xplore/home.jsp`
[4] `https://dl.acm.org/`
[5] `https://www.semanticscholar.org/`

research question **RQ3**. The values are defined based on our values found in the prestudy. However, we also allow free text answers in case the predefined classes do not match the approach indicated by *Other*. Afterward, we have the fields for *advantages* and *disadvantages*, based on our research questions **RQ4** and **RQ5**, respectively. We extracted these based on advantages and disadvantages of the approach as named in the paper by the authors. The next field is used to describe the *validity* of the results, aiming at describing how well the approach is evaluated and how reliable the results are. In other words, what evaluation goals, such as accuracy or performance, were targeted. This also includes whether a case study or only a structured discussion or other methods are used. The *Data set* field describes whether the paper provides a data set or uses a publicly available data set. *Yes* describes that a data set including the cases, the developed approaches, and evaluation data is available. In the case of *Partial*, only some but not all of these parts are available. *No* describes that no part of the data set is available. The next field describes the *theoretical concept* behind the approach. This is important because it lets us group different approaches. The last field is the *Publication Type*. It indicates in which venue the paper is published. The options are *Journal*, *Conference*, *Workshop*, and *Other*. This category is intended to show the maturity of the approach.

3.5 Data Extraction Process

For the data extraction, we used the SLR Toolkit [4] and combined it with a Git-Repository as data storage. We created for each paper an issue in our Git-Repository. The reviewers assigned themselves the issues and then extracted the data from the publications. Due to the high number of publications and the reviewer numbers, each paper was only classified by one reviewer. However, as Kitchenham *et al.* [2] described for the case of only single reviewers, we performed afterward quality methods to assure consistent data extraction. In our case, we randomly selected results from other reviewers and checked whether the results were correct.

4 Results

We first performed a prestudy for the keywords and the data extraction. We used the prestudy to adjust our search terms and the data extraction form. After the prestudy, we added, for example, the fields regarding the *Publication Type* to emphasize the maturity of an approach.

After the prestudy, we started the regular survey. Table 2 lists the number of publications found for each search term, and its breakdown into excluded and included publications based on our criteria in section 3. Overall, we found 235 publications for both terms. We excluded 125 publications based on our exclusion criteria and included 110. In detail, for the

Table 1: Data Extraction Form

Object	**Values**
Reviewer's Name	*free text*
Authors	*free text*
Title	*free text*
Identifier	*free text*
Name of Approach	*free text*
Domain	"Public Transport", "In-Vehicle" or "Other: *free text*"
Data Types	"Text-Based", "Numerical", "Image", "Video" or "Other: *free text*"
Advantages	*free text*
Disadvantages	*free text*
Validity	*free text*
Data set	"Yes", "Partial" or "No"
Theoretical Concept	*free text*
Publication Type	"Journal", "Conference", "Workshop" or "Other: *free text*"

Search Term	Found	Excluded	Included
1	217	114	103
2	18	11	7
$\sum$	235	125	110

Table 2: Overview of selected and rejected papers

first query, we got 217 publications. There, we excluded 114 publications. The most common exclusion criteria are duplicates, surveys, or non-peer-reviewed publications. However, some of the non-peer-reviewed publications are arXiv[6] preprints and, therefore, a duplicate for the later published version. This results in 103 included publications for the first search term.

For the second search term, we found 18 publications and excluded 11. This leaves us with seven included papers. Here the main exclusion criteria were papers only describing attacks, duplicates, or non-peer-reviewed articles. A complete list with all found and excluded and included publications can be found in our data set [3].

In the following, we describe our findings. We start by answering **RQ1**. We answer this research question by giving an overview of the theoretical concepts field (c.f. section 3) from our data extractions. These methods used are always dependent on a specific application or data type. However, by enumerating the approaches first, we provide a first impression of the variety of methods to choose from. Many approaches use some form of differential privacy [5] such as Qiu *et al.* [6] or Zhao *et al.* [7]. Overall 15 publications use a notion of differential privacy to anonymize data. Other approaches use k-anonymity [8] such as Stegelmann *et al.* [9] or Damjanovic-Behrendt [10]. Overall nine approaches use k-anonymity. The two concepts are often used for anonymization of trajectory data sets.

Another popular approach, especially in combination with exchanging data, is blockchain-based approaches such as Yang *et al.* [11] or Li *et al.* [12]. These methods are often used in the communication with road side units or exchanging status information with a backend. Other approaches make use of selective disclosure, meaning the selection of the transferred data by the user, for instance, through a firewall as in Klement *et al.* [13] or access control as in Plappert *et al.* [14]. They are often combined with access to bus systems, such as OBD. Also, random pseudonyms are created to hide the identity as in Wan *et al.* [15] or random noise is used to conceal a location [16]. For machine learning approaches, some methods use generated data to learn, such as Abdelwahed *et al.* [17]. Others use federated learning such as Ruan *et al.* [18] or combine it with homomorphic encryption such as Wang *et al.* [19] or Han *et al.* [20]. Some approaches use multi-party

[6] `https://arxiv.org/`

computing (MPC) to operate within an anonymous system, such as Wang *et al.* [19] and Ying *et al.* [21]. A complete list of concepts used is described in our data set [3].

Next, we present the results for the application domains. This answers our research question **RQ2**. Figure 1 illustrates the different application domains. It is important to note that multiple selections are possible as an answer. The majority of publications are in the *In-Vehicle* domain, with 83 publications focusing on it. Other domains occur less frequently. The second-largest group are *Public Transport* and *Other* with each 18 publications. Only nine publications cover *Pedestrian*. Looking into more detail in the other application domains, we also see many car-specific applications, such as Singh *et al.* [22] or Fan *et al.* [23] with VANET. Other domains are transportation systems in general or smart grids together with charging protocols such as in Agilandeeswari *et al.* [24]. However, these are also more car-related topics. Hence, we can say that many publications are focused on car-related topics. One possible reason might be that also car manufacturers invest in research in this domain, for instance, publications such as Plappert *et al.* [14], Li *et al.* [25] or Asaj *et al.* [26] are co-authored by researchers from car manufacturers.

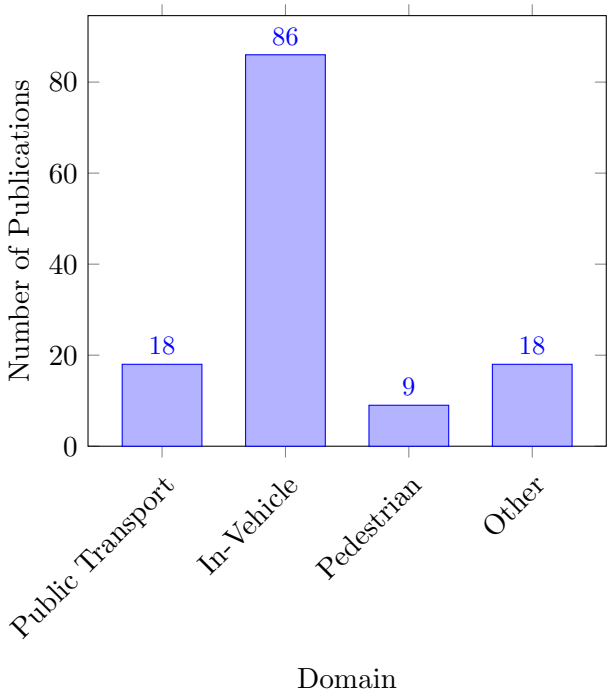

Figure 1: Application Domains

The next research question **RQ3** is answered by the data type field in our extraction form. Figure 2 illustrates the data types found. Again, multiple

selections are possible for each publication. Overall, many publications could not be mapped to our predefined data types. This is the case because the approaches are often very specific or consist of complex data types. Examples of very specific anonymization data types are, for instance, the heart rate in Ruan *et al.* [18] or the identifiers of a car as in Hong *et al.* [27]. In these very specific cases, we selected the more general data type *Numerical* and additionally added the more specific information in the *Other* text field. Examples of complex data are Ticket-Punch-Data [28] or electric car data for the smart grid [29]. If we look more closely into the *Other* field, we can identify many approaches that focus on the anonymization of car or driver identifiers, such as Salem *et al.* [30] or Ahmed *et al.* [31]. Overall these are 13 publications. Two other larger groups in the *Other* field are location data or trajectory data, such as in Fan *et al.* [23] or Ruan *et al.* [18]. Overall 24 approaches cover trajectory or location data.

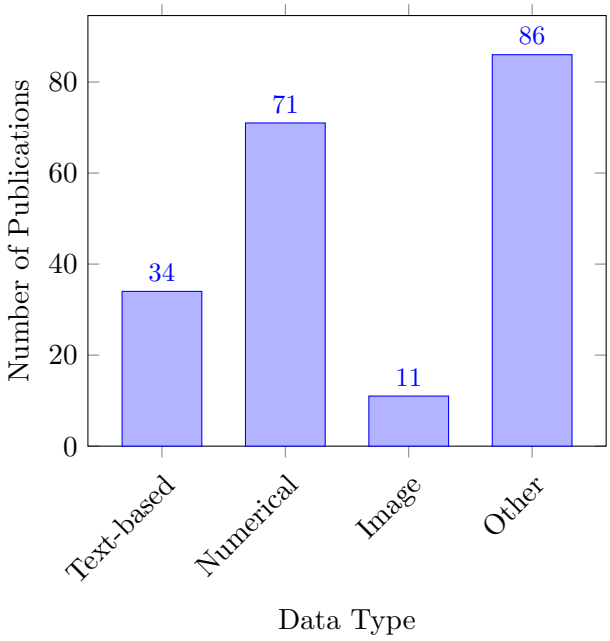

Figure 2: Anonymized Data Types

The following two research questions, **RQ4** and **RQ5**, discuss the advantages and disadvantages. In this regard, we only extracted the advantages and disadvantages mentioned in the publications by the respective authors. In the next section (c.f. section 5), we will interpret these results and give a comparison. Some of the advantages of the approaches include confidential pseudonyms for authentication, unlinkability, resistance against common attacks, elimination of vehicle IDs, secure key exchange, location and usage privacy [6], [11], [17], [24], [32], support of billing, minimizing changes to ex-

isting standards [33], hiding trajectory movements [34], [35], anonymization of location and passenger data [28], [36], [37], secure communication [38]–[40], protection against traffic flow analysis [41], controlled data sharing [10], [42], privacy-preserving authentication and communication [43], [44], task assignment based on privacy-preserving geo data [45], protection of vehicle location [46], [47], secure and private data exchange [48], cryptographic guarantees [7], [9], [25], [49]–[59].

Some of the disadvantages of the mentioned privacy methods in the mobility domain include communication overhead [11], no consideration of other attackers [6], high resource demands [17], [34], focus only on exchange of vehicle ID [24], [32], [24], no general anonymization of data [33].

The next fields of our extraction form are later used in our comparison (c.f. section 5) to differentiate between different approaches. We start by presenting the results for the validity. This is established through a variety of evaluation techniques for the presented anonymization methods. For instance, the approach by Yang *et al.* [11] is validated primarily through performance evaluation. Qiu *et al.* [6] conduct theoretical analysis on privacy properties and complexity, complemented by experimental evaluations on data sets. Abdelwahed *et al.* [17] validate their approach via testing on custom videos. Agilandeeswari *et al.* [24] combine simulation for identifying leaker data, performance evaluation, and energy assessment. While some approaches provide structured discussions or theoretical proofs, others rely on formal analysis, such as Ruan *et al.* [18] and Singh *et al.* [22]. Overall, validity is a difficult field because of the wide variety of used methods. However, many approaches do not prove that they actually satisfy the intended security property. They either only present their solution, e.g., Abumansoor *et al.* [32], Duri *et al.* [50] or only discuss why their approach should provide these aspects, such as ShanGuo [60] or Rabadi *et al.* [61]. The most frequent evaluation method is a performance-based analysis (around 40 papers). Here, it is preferred to measure the runtime of a feature in the approach.

However, reproducing these results is often very hard because most approaches do not have a publicly available data set. Figure 3 illustrates this aspect. It shows the number of publications with a full data set, only a partial one or no data set at all. Only two publications [19], [62] had a full data set published. This includes all aspects, like the source code and data used. 22 publications have a partial data set published. This was often the case when the authors referenced a case study or data set used for the evaluation. For instance, Löbner *et al.* [63] used a data set [64] containing data about the trajectory and energy consumption. Other approaches like Liu *et al.* [34] use a generator [65] to create trajectory data. However, not only trajectory data is used, for instance Ruan *et al.* [18] uses the heart rate

from the HARMONY[7] and PPG-DaLiA[8] data set. These data sets also contain other additional data, such as motion data of the device measuring the heart rate. Nevertheless, the publications marked with *Partial* often did not publish the modification on the data sets, concrete selection of the data, meaning which data fields are considered, or the source code. Most publications have no published data set. Despite that, many approaches claim to use a data set in their validation.

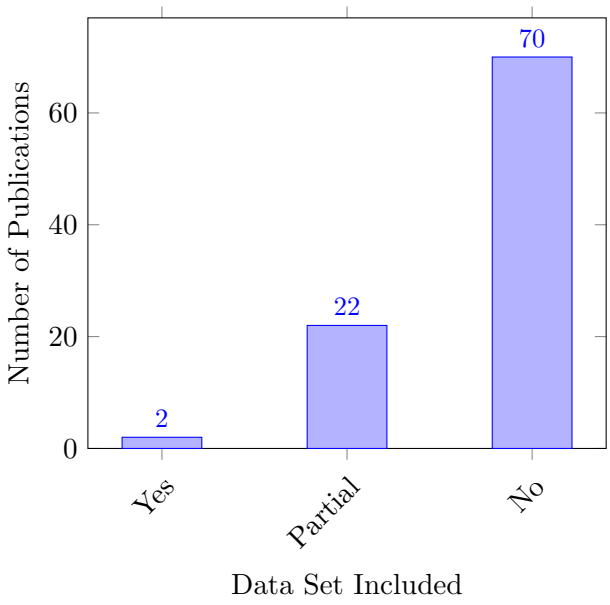

Figure 3: Data sets included

The last field that we present is the venue type of the publication. The venue type should show the maturity of the approach. Figure 4 illustrates the distribution of venue types. Most publications are published at conferences. These are 50 publications. The next big group are journal publications, with 45 ones. Only 11 publications are workshop publications. Two publications are neither of the previous ones. In our case, these were only poster submissions. Based on our findings, we can see that the research field is already established and contains mature approaches because many publications are found in journals or conferences.

5 Discussion of the Results

Based on our previously presented results, we discuss our different findings. An overall comparison of all the different methods is difficult to accomplish,

[7] `https://osf.io/zextd/`
[8] `https://archive.ics.uci.edu/dataset/495/ppg+dalia`

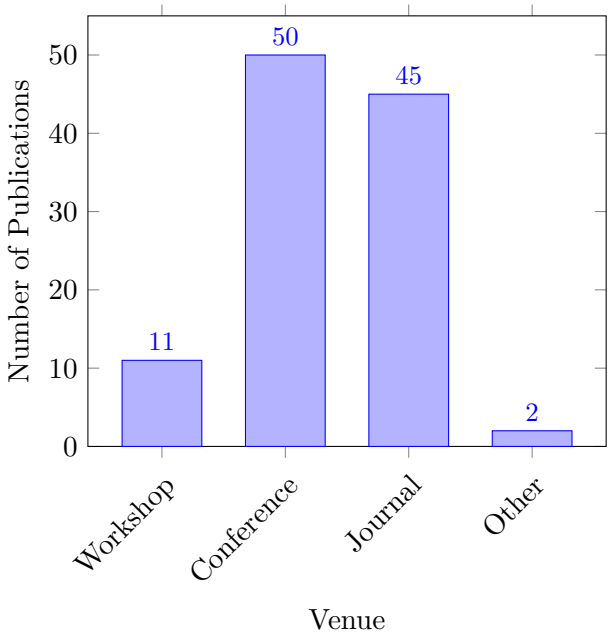

Figure 4: Publication Venues

because of the various application domains and approaches. Also, the lack of the published data or evaluation makes it harder. In addition, many approaches do not discuss their disadvantages or only in a very limited setting, such as Singh [66]. These aspects are especially relevant for future work, which should build up on identified approaches.

However, with these work packages in mind, we can identify relationships to other work packages (WP). For instance, Righini *et al.* [67] or Rupp *et al.* [68] describe a novel ticketing system for public transportation. In our WP 1.3.4, we look at a similar case. Hence, this approach might be a starting point for further discussions. Other relevant publications are, for instance, Abdelwahed *et al.* [17] for WP 1.3.5 as generating anonymous video training data or Sciancalepore *et al.* [69] for privacy-aware collision avoidance in autonomous vehicles, which is related to our WP 1.2 about autonomous cars.

In addition, there is a relation to our WP 5.2, which investigates machine learning and anonymity. Here, especially relevant are the following approaches. Abdelwahed *et al.* [17] is a privacy-aware passenger observing approach. Other interesting methods are using federated learning or combining it with homomorphic encryption [18]–[20], [70].

Another relation can be found with the WP 6, which investigates deanonymization approaches. Here, our publications can help to identify attacks because some approaches such as Da Silva *et al.* [71], Joy *et al.* [72] or Lu *et al.* [16] discuss in addition to their anonymization also attacks on

anonymized data.

Besides relating the identified publications to our other WPs in *ANYMOS*, we want to give an overview of different prerequisites for applying these approaches. Many approaches do not anonymize the data but rather encrypt them, such as Malina *et al.* [73], Salem *et al.* [39], or Mankar *et al.* [74]. This then requires a trusted entity to manage the data. Overall these approaches tend to use simpler encryption algorithms. Hence, they usually are more efficient and can be used on low-powered hardware. Other approaches like Liu *et al.* [34] use far more powerful hardware. In this case, it is an Intel Core i7. However, the approach also gives far more security guarantees about the reidentification than more straightforward approaches.

Regarding future research directions, we see a wide gap in the research between public transport and car-related research. Many approaches focus on car-related aspects or use their methods in car-related topics. In the future, it might be interesting to bring these two aspects closer together and close the gap between the different research areas. For instance, trajectory anonymization such as Liu *et al.* [34] can also be used to anonymize public transport data or person data. Also, our research project aims to unite both perspectives in our research.

Furthermore, it would be beneficial if the different approaches would provide data sets. This could help other researchers to compare different methods better. However, this is an ongoing problem, which also affects other areas like software engineering [75].

6 Limitations of the Review

In this section, we reflect on the limitations of our literature review. We start by discussing the limitations based on our decision about the configuration.

The first limitation is about the chosen search engines. As previously stated, we performed a database search. In this regard, the used databases are essential to identify the relevant publications. We can only find the publications if the database contains the relevant publication. In our case, we chose the most common and relevant databases in our field. In addition, we used Google Scholar, which indexes a wide variety of different publishers. Hence, we assume the limitation to be small.

Another point limiting our review are the used keywords. As discussed in the initial configuration (c.f. section 3), the keywords are essential for identifying relevant publications. We first created a list of keywords to avoid mistakes and discussed these in project workshops. Afterwards, we performed a prestudy to refine the keyword selection. Then, we again discussed the keywords in our project, and only then finally performed the actual literature review. This provides confidence to have identified the relevant keywords for our research questions. We note, however, that our

review focuses on anonymization approaches within the mobility domain. We did not investigate anonymization methods in general and how these could be applied in the mobility domain. Therefore, the review can only make statements about approaches already used in the mobility domain, and it is possible that additional approaches exist that could be applied in the mobility domain, but either have not been tried or the results published.

Next, having the extraction process performed by only one reviewer could limit the review quality. To reduce this threat, we performed a quality assurance step after the extraction. With this step, we unified the extracted data and verified the results. Our data set is [3] is publicly available, and as such, further checks could be performed by third parties.

Finally, while the survey lists different approaches, our results are not suitable for deciding for a single dominant anonymization strategy. As previously mentioned, the application area for anonymization in the mobility domain is vast, so up to now, and so far, no single approach appears to be able to solve all the problems. Our review provides a starting point for identifying necessary approaches, and could give rise to the development of new or the application of existing techniques.

7 An Industry-driven Survey on Status Quo and Demand

This section focuses on the anonymization techniques used specifically for video data in public transport. It is important to note that the discussion is limited to video data, excluding for example passenger counting data. The scope encompasses video data viewed outside of the vehicle, both in live and non-live scenarios.

The use cases discussed here are provided by DReserach Fahrzeugelektronik GmbH (DFE). DFE is a development-oriented company that offers CCTV solutions for public transport globally and has over 800 customers in "D-A-CH" region alone. Since its establishment in 1994, DResearch Media GmbH, along with its subsidiary company DFE (established in 2011), has accumulated extensive expertise in developing maintenance-free embedded systems for long-term service. With more than 40,000 active systems, DFE has solidified its position as market leader.

The insights and results presented in this section are derived from an informal in-house survey conducted among DFE project engineers. The survey aimed to gather information on the anonymization requirements, needs and usage of DFE customers in the public transport sector.

Since the focus increases on data privacy through regulations such as the General Data Protection Regulation (GDPR), the relevance of anonymization techniques, specifically used on video data will play a major role in future surveillance systems. The GDPR emphasizes the importance of pro-

tecting individuals' personal data, including video data, and requires organizations to implement measures to ensure data privacy.

The survey revealed various use cases for video data in public transport, including an estimation on whether anonymization is required according to GDPR:

1. Surveillance: Video data plays a crucial role in surveillance systems for enhancing security measures. Law enforcement agencies rely on clear video data to identify and investigate security incidents, such as theft, vandalism or unauthorized access. In these cases, anonymization is not applicable, as the clarity and quality of the footage are essential for effective analysis.

2. Quality Management: Video data is utilized for quality management purposes, such as investigating passenger complaints, monitoring service quality or assessing operational efficiency. Under data protection regulations like the General Data Protection Regulation (GDPR), there is a need to anonymize video data used in quality management processes to protect passenger privacy.

3. External Verification of People Counting Systems: Video data is employed to verify and validate people counting systems deployed in public transport. These systems help gather information on passenger flow, capacity utilization, and planning. To ensure privacy compliance, video data used for external verification purposes also requires anonymization.

4. Ensuring Functionality of the Video System: Remote live-streaming of video data is used to assess the functionality and performance of the video systems installed in public transport vehicles. Anonymization techniques are necessary in this case to safeguard passenger privacy while allowing for real-time monitoring and evaluation.

5. Creation and Extension of AI Training Data: Video data can be utilized to create and extent training datasets for artificial intelligence (AI) algorithms. Anonymization is crucial when using video data to develop AI models to ensure that personally identifiable information is removed or obscured, protecting the privacy of individuals captured in the footage.

Furthermore, the survey gave insights into the anonymization techniques currently used today, which are limited to pixelization of static areas. This technique is used for example, to pixelate video data showing the driver's seat in the vehicle, since German law prohibits the usage of surveillance at a workplace. However, to ensure ongoing GDPR compliance while maintaining usability, the implementation of more advanced anonymization techniques is necessary. For instance, incorporating dynamic object detection

and anonymization could prove to be beneficial. An area where this technique could be applied is real-time head detection and anonymization, which would effectively safeguard passenger privacy.

In conclusion, the current implementation of anonymization techniques for video data in public transport remains limited. However, with the increasing focus on data privacy and the enforcement of regulations such as the General Data Protection Regulation (GDPR), the relevance of anonymization techniques is expected to play a vital role in the future. Anonymization techniques will become crucial in complying with these regulations by removing personally identifiable information and preventing the risk of re-identification. By adopting effective anonymization methods, such as dynamic object detection and anonymization, public transport providers can strike a balance between privacy protection and data utility. This will enable them to continue benefiting from video data while safeguarding passenger privacy in accordance with GDPR rules.

8 Conclusion

This report presented our systematic literature review for the method building kit of the *ANYMOS* project. We presented our configuration with search terms and inclusion and exclusion criteria. We presented and discussed the results. In addition, we put the results in relation to other work packages in the research project. We also gave indicators on how to compare the different approaches and identified future research directions.

Besides the literature review, we also presented the result of an industry-driven survey by DFE regarding anonymization techniques used in public transport. This survey focuses on video technologies and was conducted within a company developing video surveillance technologies. It shows the current status quo and stresses the importance of further research in this area.

In the future, we plan to use our results in other working packages of the ANYMOS project.

Acknowledgements

This work was supported by the German Federal Ministry of Education and Research (BMBF) grant number 16KISA086 (ANYMOS) and the NextGenerationEU project by the European Union (EU).

References

[1] L. Kneis, M. Rill, S. Alpers, *et al.*, "Anonymität und Mobilität - Whitepaper zum Begriffs- und Domänenverständnis des Kompetenz-

cluster Anymos – Anonymisierung für vernetzte Mobilitätssysteme," Karlsruhe Institute of Technology, Tech. Rep., 2023. DOI: 10.5445/IR/1000161584.

[2] B. Kitchenham and S. Charters, "Guidelines for performing systematic literature reviews in software engineering," vol. 2, Jan. 2007.

[3] M. Walter, W. Beskorovajnov, F. Lieberwirth, *et al.* "Dataset for the literature review in anymos wp 5.1." (Aug. 20, 2023), [Online]. Available: https://doi.org/10.5281/zenodo.8210605.

[4] S. Götz, "Supporting systematic literature reviews in computer science: The systematic literature review toolkit," in *Proceedings of the 21st ACM/IEEE International Conference on Model Driven Engineering Languages and Systems: Companion Proceedings*, ser. MODELS '18, Copenhagen, Denmark: Association for Computing Machinery, 2018, pp. 22–26, ISBN: 9781450359658. DOI: 10.1145/3270112.3270117. [Online]. Available: https://doi.org/10.1145/3270112.3270117.

[5] C. Dwork, "Differential privacy," in *Automata, Languages and Programming*, M. Bugliesi, B. Preneel, V. Sassone, *et al.*, Eds., Berlin, Heidelberg: Springer Berlin Heidelberg, 2006, pp. 1–12, ISBN: 978-3-540-35908-1.

[6] G. Qiu and Y. Shen, "Mobility-aware differentially private trajectory for privacy-preserving continual crowdsourcing," *IEEE Access*, vol. 9, 2021, ISSN: 2169-3536. DOI: 10.1109/ACCESS.2021.3058211.

[7] Y. Zhao, X. Meng, and B. Kang, "A task allocation scheme for protecting location privacy in vehicle ad hoc networks," in *2020 IEEE 3rd International Conference on Automation, Electronics and Electrical Engineering (AUTEEE)*, IEEE, 2020, pp. 395–402.

[8] 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.

[9] M. Stegelmann and D. Kesdogan, "V2gpriv: Vehicle-to-grid privacy in the smart grid," in *Cyberspace Safety and Security: 4th International Symposium, CSS 2012, Melbourne, Australia, December 12-13, 2012. Proceedings 4*, Springer, 2012, pp. 93–107. [Online]. Available: https://link.springer.com/chapter/10.1007/978-3-642-35362-8_9.

[10] V. Damjanovic-Behrendt, "A digital twin-based privacy enhancement mechanism for the automotive industry," in *2018 International Conference on Intelligent Systems (IS)*, IEEE, 2018, pp. 272–279. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/8710526.

[11] Y. Yang, J. Wu, C. Long, *et al.*, "A blockchain-based cross-domain authentication for conditional privacy preserving in vehicular ad-hoc network," in *2021 The 3rd International Conference on Blockchain Technology*, ser. ICBCT '21, event-place: Shanghai, China, New York, NY, USA: Association for Computing Machinery, 2021, pp. 183–188, ISBN: 978-1-4503-8962-4. DOI: 10.1145/3460537.3460545. [Online]. Available: https://doi.org/10.1145/3460537.3460545.

[12] Y. Li, K. Ouyang, N. Li, *et al.*, "A blockchain-assisted intelligent transportation system promoting data services with privacy protection," *Sensors*, vol. 20, no. 9, p. 2483, 2020, Publisher: MDPI.

[13] F. Klement, H. C. Pöhls, and S. Katzenbeisser, "Man-in-the-obd: A modular, protocol agnostic firewall for automotive dongles to enhance privacy and security," in *International Workshop on Attacks and Defenses for Internet-of-Things*, Springer, 2022, pp. 143–164. [Online]. Available: https://link.springer.com/chapter/10.1007/978-3-031-21311-3_7.

[14] C. Plappert, D. Zelle, C. Krauß, *et al.*, "A privacy-aware data access system for automotive applications," in *15th ESCAR Embedded Security in Cars Conference*, 2017, pp. 27–65. [Online]. Available: https://sedafa-projekt.de/media/EscarEU2017_Zelle.pdf.

[15] Z. Wan, W.-T. Zhu, and G. Wang, "PRAC: Efficient privacy protection for vehicle-to-grid communications in the smart grid," *Computers & security*, vol. 62, pp. 246–256, 2016, Publisher: Elsevier. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0167404816300761.

[16] Z. Lu, Z. H. Du Suguo, C. Cailian, *et al.*, "Location privacy in usage-based automotive insurance: Attack and countermeasures," *IEEE Trans. Inf. Forensics Secur.*, pp. 1–1, 2018. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/8387782.

[17] Y. Abdelwahed, O. Khaled, A. Elhamahmi, *et al.*, "Privacy-centric AI-based real-time storage-less edge computing approaches for passenger counting and action classification on public transport vehicles," in *2021 IEEE International Intelligent Transportation Systems Conference (ITSC)*, IEEE, 2021, pp. 3116–3121. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/9564830.

[18] H. Ruan, Q. Gong, Y. Chen, *et al.*, "Poster: A privacy-preserving heart rate prediction system for drivers in connected vehicles," in *Proceedings of the 21st Annual International Conference on Mobile Systems, Applications and Services*, ser. MobiSys '23, event-place: Helsinki, Finland, New York, NY, USA: Association for Computing Machinery, 2023, pp. 557–558. DOI: 10.1145/3581791.3597364. [Online]. Available: https://doi.org/10.1145/3581791.3597364.

[19] K. Wang, C.-M. Chen, M. Shojafar, *et al.*, "AFFIRM: Provably forward privacy for searchable encryption in cooperative intelligent transportation system," *IEEE Transactions on Intelligent Transportation Systems*, vol. 23, no. 11, pp. 22 607–22 618, 2022, Publisher: IEEE. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/9788514.

[20] X. Han, D. Tian, X. Duan, *et al.*, "A dual mode privacy-preserving scheme enabled secure and anonymous for edge computing assisted internet of vehicle networks," in *Proceedings of the 11th ACM Symposium on Design and Analysis of Intelligent Vehicular Networks and Applications*, ser. DIVANet '21, event-place: Alicante, Spain, New York, NY, USA: Association for Computing Machinery, 2021, pp. 65–70, ISBN: 978-1-4503-9081-1. DOI: 10.1145/3479243.3487310. [Online]. Available: https://doi.org/10.1145/3479243.3487310.

[21] Z. Ying, S. Cao, X. Liu, *et al.*, "PrivacySignal: Privacy-preserving traffic signal control for intelligent transportation system," *IEEE Transactions on Intelligent Transportation Systems*, vol. 23, no. 9, pp. 16 290–16 303, 2022, Publisher: IEEE. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/9713758.

[22] K. Singh, P. Saini, S. Rani, *et al.*, "Authentication and privacy preserving message transfer scheme for vehicular ad hoc networks (VANETs)," in *Proceedings of the 12th ACM International Conference on Computing Frontiers*, ser. CF '15, event-place: Ischia, Italy, New York, NY, USA: Association for Computing Machinery, 2015, ISBN: 978-1-4503-3358-0. DOI: 10.1145/2742854.2745718. [Online]. Available: https://doi.org/10.1145/2742854.2745718.

[23] C.-I. Fan, R.-H. Hsu, and C.-H. Tseng, "Pairing-based message authentication scheme with privacy protection in vehicular ad hoc networks," in *Proceedings of the International Conference on Mobile Technology, Applications, and Systems*, ser. Mobility '08, event-place: Yilan, Taiwan, New York, NY, USA: Association for Computing Machinery, 2008, ISBN: 978-1-60558-089-0. DOI: 10.1145/1506270.1506372. [Online]. Available: https://doi.org/10.1145/1506270.1506372.

[24] L. Agilandeeswari, S. Paliwal, A. Chandrakar, *et al.*, "A new lightweight conditional privacy preserving authentication and key–agreement protocol in social internet of things for vehicle to smart grid networks," *Multimedia Tools and Applications*, vol. 81, no. 19, pp. 27 683–27 710, 2022, Publisher: Springer. [Online]. Available: https://link.springer.com/article/10.1007/s11042-022-12946-5.

[25] H. Li, D. Ma, B. Medjahed, *et al.*, "Analyzing and preventing data privacy leakage in connected vehicle services," *SAE International Journal of Advances and Current Practices in Mobility*, vol. 1, no. 2019, pp. 1035–1045, 2019. [Online]. Available: https://saemobilus.sae.org/content/2019-01-0478.

[26] N. Asaj, B. Wiedersheim, A. Held, *et al.*, "Towards an identity-based data model for an automotive privacy process," in *2012 International Conference on Privacy, Security, Risk and Trust and 2012 International Confernece on Social Computing*, IEEE, 2012, pp. 789–796. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/6406325.

[27] Z. Hong, F. Tang, and W. Luo, "Privacy-preserving aggregate signcryption for vehicular ad hoc networks," in *Proceedings of the 2nd International Conference on Cryptography, Security and Privacy*, ser. ICCSP 2018, event-place: Guiyang, China, New York, NY, USA: Association for Computing Machinery, 2018, pp. 72–76, ISBN: 978-1-4503-6361-7. DOI: 10.1145/3199478.3199484. [Online]. Available: https://doi.org/10.1145/3199478.3199484.

[28] G. Avoine, L. Calderoni, J. Delvaux, *et al.*, "Passengers information in public transport and privacy: Can anonymous tickets prevent tracking?" *International Journal of Information Management*, vol. 34, no. 5, pp. 682–688, 2014, Publisher: Elsevier. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0268401214000620.

[29] H. Nicanfar, P. TalebiFard, S. Hosseininezhad, *et al.*, "Security and privacy of electric vehicles in the smart grid context: Problem and solution," in *Proceedings of the Third ACM International Symposium on Design and Analysis of Intelligent Vehicular Networks and Applications*, ser. DIVANet '13, event-place: Barcelona, Spain, New York, NY, USA: Association for Computing Machinery, 2013, pp. 45–54, ISBN: 978-1-4503-2358-1. DOI: 10.1145/2512921.2512926. [Online]. Available: https://doi.org/10.1145/2512921.2512926.

[30] F. M. Salem, M. H. Ibrahim, and I. Ibrahim, "Non-interactive authentication scheme providing privacy among drivers in vehicle-to-vehicle networks," in *2010 Sixth International Conference on Networking and Services*, IEEE, 2010, pp. 156–161. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/5460654.

[31] U. Ahmed, J. C.-W. Lin, and G. Srivastava, "Privacy-preserving deep reinforcement learning in vehicle ad hoc networks," *IEEE consumer electronics magazine*, vol. 11, no. 6, pp. 41–48, 2021, Publisher: IEEE. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/9451559.

[32] O. Abumansoor, A. Boukerche, B. Landfeldt, *et al.*, "Privacy preserving neighborhood awareness in vehicular ad hoc networks," in *Proceedings of the 7th ACM Symposium on QoS and Security for Wireless and Mobile Networks*, ser. Q2SWinet '11, event-place: Miami, Florida, USA, New York, NY, USA: Association for Computing Machinery, 2011, pp. 17–20, ISBN: 978-1-4503-0899-1. DOI: 10.1145/2069105.2069109. [Online]. Available: https://doi.org/10.1145/2069105.2069109.

[33] D. Angermeier, A. Kiening, and F. Stumpf, "PAL - privacy augmented LTE: A privacy-preserving scheme for vehicular LTE communication," in *Proceeding of the Tenth ACM International Workshop on Vehicular Inter-Networking, Systems, and Applications*, ser. VANET '13, event-place: Taipei, Taiwan, New York, NY, USA: Association for Computing Machinery, 2013, pp. 1–10, ISBN: 978-1-4503-2073-3. DOI: 10.1145/2482967.2482975. [Online]. Available: https://doi.org/10.1145/2482967.2482975.

[34] X. Liu and Y. Zhu, "Privacy and utility preserving trajectory data publishing for intelligent transportation systems," *IEEE Access*, vol. 8, pp. 176 454–176 466, 2020, ISSN: 2169-3536. DOI: 10.1109/ACCESS.2020.3027299.

[35] C. Zhou, T. Wang, H. Tian, *et al.*, "A top-k query scheme with privacy preservation for intelligent vehicle network in mobile IoT," *IEEE Access*, vol. 8, pp. 81 698–81 710, 2020. DOI: 10.1109/ACCESS.2020.2990932.

[36] Y. Y. Liu, A. Cooke, and P. Thulasiraman, "Location privacy preservation of vehicle data in internet of vehicles," [Online]. Available: http://personales.upv.es/thinkmind/dl/conferences/internet/internet_2020/internet_2020_1_100_40038.pdf.

[37] I. Gudymenko, "A privacy-preserving e-ticketing system for public transportation supporting fine-granular billing and local validation," in *Proceedings of the 7th International Conference on Security of Information and Networks*, 2014, pp. 101–108.

[38] D. Tabellion, M. Wolf, J. Britz, *et al.*, "Security, privacy and trust for a crowd-sourced semantic accessibility database for public transport," in *HCI International 2020–Late Breaking Papers: Universal Access and Inclusive Design: 22nd HCI International Conference, HCII 2020, Copenhagen, Denmark, July 19–24, 2020, Proceedings 22*, Springer, 2020, pp. 712–727. [Online]. Available: https://link.springer.com/chapter/10.1007/978-3-030-60149-2_54.

[39] F. M. Salem, M. H. Ibrahim, and I. Ibrahim, "Efficient noninteractive secure protocol enforcing privacy in vehicle-to-roadside communication networks," *International Journal of Vehicular Technology*, vol. 2012, 2012, Publisher: Hindawi. [Online]. Available: https://downloads.hindawi.com/archive/2012/862368.pdf.

[40] J. Rao, S. Gao, and X. Zhu, "VTSV: A privacy-preserving vehicle trajectory simulation and visualization platform using deep reinforcement learning," in *Proceedings of the 4th ACM SIGSPATIAL International Workshop on AI for Geographic Knowledge Discovery*, ser. GEOAI '21, event-place: Beijing, China, New York, NY, USA: Association for Computing Machinery, 2021, pp. 43–46, ISBN: 978-1-4503-9120-7. DOI: 10.1145/3486635.3491073. [Online]. Available: https://doi.org/10.1145/3486635.3491073.

[41] S. Chavhan, D. Gupta, S. Garg, *et al.*, "Privacy and security management in intelligent transportation system," *IEEE Access*, vol. 8, pp. 148 677–148 688, 2020, Publisher: IEEE. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/9162025.

[42] J. Y. Choi, M. Jakobsson, and S. Wetzel, "Balancing auditability and privacy in vehicular networks," in *Proceedings of the 1st ACM International Workshop on Quality of Service & Security in Wireless and Mobile Networks*, ser. Q2SWinet '05, event-place: Montreal, Quebec, Canada, New York, NY, USA: Association for Computing Machinery, 2005, pp. 79–87, ISBN: 1-59593-241-0. DOI: 10.1145/1089761.1089775. [Online]. Available: https://doi.org/10.1145/1089761.1089775.

[43] S. U. Hussain and F. Koushanfar, "P3: Privacy preserving positioning for smart automotive systems," *ACM Trans. Des. Autom. Electron. Syst.*, vol. 23, no. 6, Nov. 2018, Place: New York, NY, USA Publisher: Association for Computing Machinery, ISSN: 1084-4309. DOI: 10.1145/3236625. [Online]. Available: https://doi.org/10.1145/3236625.

[44] Q. Huang, X. Xu, H. Chen, *et al.*, "A vehicle trajectory privacy preservation method based on caching and dummy locations in the internet of vehicles," *Sensors*, vol. 22, no. 12, p. 4423, 2022, Publisher: MDPI. [Online]. Available: https://www.mdpi.com/1424-8220/22/12/4423.

[45] C. Qiu and A. C. Squicciarini, "Location privacy protection in vehicle-based spatial crowdsourcing via geo-indistinguishability," in *2019 IEEE 39th International Conference on Distributed Computing Systems (ICDCS)*, ISSN: 2575-8411, Jul. 2019, pp. 1061–1071. DOI: 10.1109/ICDCS.2019.00109. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/9259240.

[46] C. Qiu, A. Squicciarini, C. Pang, *et al.*, "Location privacy protection in vehicle-based spatial crowdsourcing via geo-indistinguishability," *IEEE Transactions on Mobile Computing*, vol. 21, no. 7, pp. 2436–2450, Jul. 2022, ISSN: 1558-0660. DOI: 10.1109/TMC.2020.3037911.

[47] C. Qiu, L. Yan, A. Squicciarini, *et al.*, "TrafficAdaptor: An adaptive obfuscation strategy for vehicle location privacy against traffic flow aware attacks," in *Proceedings of the 30th International Conference on Advances in Geographic Information Systems*, ser. SIGSPATIAL '22, event-place: Seattle, Washington, New York, NY, USA: Association for Computing Machinery, 2022, ISBN: 978-1-4503-9529-8. DOI: 10.1145/3557915.3560938. [Online]. Available: https://doi.org/10.1145/3557915.3560938.

[48] X. Ding, S. Cao, F. Dou, *et al.*, "Certificateless aggregate signature scheme with conditional privacy protection in vehicle networking," in *Journal of Physics: Conference Series*, Issue: 1, vol. 2026, IOP Publishing, 2021, p. 012 044. [Online]. Available: https://iopscience.iop.org/article/10.1088/1742-6596/2026/1/012044/meta.

[49] L. Zhang, J. Wang, and Y. Mu, "Secure and privacy-preserving attribute-based sharing framework in vehicles ad hoc networks," *IEEE Access*, vol. 8, pp. 116 781–116 795, 2020, ISSN: 2169-3536. DOI: 10.1109/ACCESS.2020.3004247.

[50] S. Duri, M. Gruteser, X. Liu, *et al.*, "Framework for security and privacy in automotive telematics," in *Proceedings of the 2nd International Workshop on Mobile Commerce*, ser. WMC '02, event-place: Atlanta, Georgia, USA, New York, NY, USA: Association for Computing Machinery, 2002, pp. 25–32, ISBN: 1-58113-600-5. DOI: 10.1145/570705.570711. [Online]. Available: https://doi.org/10.1145/570705.570711.

[51] J. Guo and J. P. Baugh, "Security and privacy in vehicle safety communication applications," *SAE Transactions*, pp. 721–727, 2006, Publisher: JSTOR. [Online]. Available: https://www.jstor.org/stable/44700103?seq=2.

[52] Y. Guan, R. Lu, Y. Zheng, *et al.*, "Achieving privacy-preserving vehicle selection for effective content dissemination in smart cities," in *GLOBECOM 2020-2020 IEEE Global Communications Conference*, IEEE, 2020, pp. 1–6. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/9348253.

[53] T. Li, S. Xie, Z. Zeng, *et al.*, "ATPS: An AI based trust-aware and privacy-preserving system for vehicle managements in sustainable VANETs," *IEEE Transactions on Intelligent Transportation Systems*, vol. 23, no. 10, pp. 19 837–19 851, 2022, Publisher: IEEE. [Online].

Available: https://ieeexplore.ieee.org/abstract/document/9851637.

[54] A. Zierfuss and R. Sendag, "The impact of data complexity on privacy management in vehicle to infrastructure applications," in *2013 International Conference on Connected Vehicles and Expo (ICCVE)*, IEEE, 2013, pp. 753–760. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/6799890.

[55] D. Kopanaki, N. Pelekis, A. Gkoulalas-Divanis, *et al.*, "A framework for mobility pattern mining and privacy-aware querying of trajectory data," in *Hellenic Data Management Symposium*, 2012. [Online]. Available: https://www.uhasselt.be/documents/datasim/papers/a-framework-for-mobility-pattern-mining.pdf.

[56] A. Monreale, R. Trasarti, C. Renso, *et al.*, "Preserving privacy in semantic-rich trajectories of human mobility," in *Proceedings of the 3rd ACM SIGSPATIAL International Workshop on Security and Privacy in GIS and LBS*, ser. SPRINGL '10, event-place: San Jose, California, New York, NY, USA: Association for Computing Machinery, 2010, pp. 47–54, ISBN: 978-1-4503-0435-1. DOI: 10.1145/1868470.1868481. [Online]. Available: https://doi.org/10.1145/1868470.1868481.

[57] R. Shigetomi, M. Sato, K. Uehara, *et al.*, "An efficient scheme to protect privacy in probe vehicle information system," in *2008 8th International Conference on ITS Telecommunications*, IEEE, 2008, pp. 84–88. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/4740232.

[58] I. U. Din, K. A. Awan, and A. Almogren, "Secure and privacy-preserving trust management system for trustworthy communications in intelligent transportation systems," *IEEE Access*, 2023, Publisher: IEEE. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/10168094.

[59] A. Dorri, M. Steger, S. S. Kanhere, *et al.*, "Blockchain: A distributed solution to automotive security and privacy," *IEEE Communications Magazine*, vol. 55, no. 12, pp. 119–125, 2017, Publisher: IEEE. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/8198814.

[60] L. ShanGuo, "Efficient privacy protection authentication scheme in vehicle ad hoc networks," in *Cyberspace Safety and Security: 11th International Symposium, CSS 2019, Guangzhou, China, December 1–3, 2019, Proceedings, Part I 11*, Springer, 2019, pp. 279–288. [Online]. Available: https://link.springer.com/chapter/10.1007/978-3-030-37337-5_23.

[61] N. M. Rabadi and S. M. Mahmud, "Privacy protection among drivers in vehicle-to-vehicle communication networks," in *2007 4th IEEE Consumer Communications and Networking Conference*, IEEE, 2007, pp. 281–286. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/4199150.

[62] R. Seidel, N. Jahn, S. Seo, *et al.*, "NAPC: A neural algorithm for automated passenger counting in public transport on a privacy-friendly dataset," *IEEE Open Journal of Intelligent Transportation Systems*, vol. 3, pp. 33–44, 2021, Publisher: IEEE. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/9665722.

[63] S. Löbner, C. Gartner, and F. Tronnier, "Privacy preserving data analysis with the encode, shuffle, analyse architecture in vehicular data sharing," in *Proceedings of the 2023 European Interdisciplinary Cybersecurity Conference*, ser. EICC '23, event-place: Stavanger, Norway, New York, NY, USA: Association for Computing Machinery, 2023, pp. 85–91, ISBN: 978-1-4503-9829-9. DOI: 10.1145/3590777.3590791. [Online]. Available: https://doi.org/10.1145/3590777.3590791.

[64] G. Oh, D. J. Leblanc, and H. Peng, "Vehicle energy dataset (ved), a large-scale dataset for vehicle energy consumption research," *IEEE Transactions on Intelligent Transportation Systems*, vol. 23, no. 4, pp. 3302–3312, 2022. DOI: 10.1109/TITS.2020.3035596.

[65] T. Brinkhoff, "A framework for generating network-based moving objects," *GeoInformatica*, vol. 6, no. 2, pp. 153–180, 2002.

[66] J. Singh, "Technique for privacy preserving real-time vehicle tracking using 802.11p technology," in *Proceedings of the 9th International Conference on Advances in Mobile Computing and Multimedia*, ser. MoMM '11, event-place: Ho Chi Minh City, Vietnam, New York, NY, USA: Association for Computing Machinery, 2011, pp. 206–209, ISBN: 978-1-4503-0785-7. DOI: 10.1145/2095697.2095736. [Online]. Available: https://doi.org/10.1145/2095697.2095736.

[67] S. Righini, L. Calderoni, and D. Maio, "A privacy-aware zero interaction smart mobility system," *IEEE Access*, vol. 10, pp. 11 924–11 937, 2022, Publisher: IEEE. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/9693973/.

[68] A. Rupp, F. Baldimtsi, G. Hinterwälder, *et al.*, "Cryptographic theory meets practice: Efficient and privacy-preserving payments for public transport," *ACM Trans. Inf. Syst. Secur.*, vol. 17, no. 3, Mar. 2015, Place: New York, NY, USA Publisher: Association for Computing Machinery, ISSN: 1094-9224. DOI: 10.1145/2699904. [Online]. Available: https://doi.org/10.1145/2699904.

[69] S. Sciancalepore and D. R. George, "Privacy-preserving trajectory matching on autonomous unmanned aerial vehicles," in *Proceedings of the 38th ACSAC '22*, event-place: Austin, TX, USA, New York, NY, USA: Association for Computing Machinery, 2022, pp. 1–12, ISBN: 978-1-4503-9759-9. DOI: 10.1145/3564625.3564626.

[70] H. Taslimasa, S. Dadkhah, E. C. P. Neto, *et al.*, "ImageFed: Practical privacy preserving intrusion detection system for in-vehicle CAN bus protocol," in *2023 IEEE 9th Intl Conference on Big Data Security on Cloud (BigDataSecurity), IEEE Intl Conference on High Performance and Smart Computing,(HPSC) and IEEE Intl Conference on Intelligent Data and Security (IDS)*, IEEE, 2023, pp. 122–129. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/10132145.

[71] D. Da Silva, T. Ann Kosa, S. Marsh, *et al.*, "Examining privacy in vehicular ad-hoc networks," in *Proceedings of the Second ACM International Symposium on Design and Analysis of Intelligent Vehicular Networks and Applications*, ser. DIVANet '12, event-place: Paphos, Cyprus, New York, NY, USA: Association for Computing Machinery, 2012, pp. 105–110, ISBN: 978-1-4503-1625-5. DOI: 10.1145/2386958.2386974. [Online]. Available: https://doi.org/10.1145/2386958.2386974.

[72] J. Joy and M. Gerla, "Privacy risks in vehicle grids and autonomous cars," in *Proceedings of the 2nd ACM International Workshop on Smart, Autonomous, and Connected Vehicular Systems and Services*, ser. CarSys '17, event-place: Snowbird, Utah, USA, New York, NY, USA: Association for Computing Machinery, 2017, pp. 19–23, ISBN: 978-1-4503-5146-1. DOI: 10.1145/3131944.3133938. [Online]. Available: https://doi.org/10.1145/3131944.3133938.

[73] L. Malina, P. Seda, Z. Martinasek, *et al.*, "On security and privacy in vehicle speed-limiting services in the internet of vehicles," *IEEE Intelligent Transportation Systems Magazine*, vol. 15, no. 1, pp. 8–22, 2022, Publisher: IEEE. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/9893214.

[74] K. Mankar and C. T. Wasnik, "Improved conditional privacy protection in vehicle ad-hoc networks," in *2019 3rd International Conference on Computing Methodologies and Communication (ICCMC)*, IEEE, 2019, pp. 328–334. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/8819827.

[75] M. Konersmann, A. Kaplan, T. Kühn, *et al.*, "Evaluation methods and replicability of software architecture research objects," in *2022 IEEE 19th International Conference on Software Architecture (ICSA)*, 2022, pp. 157–168. DOI: 10.1109/ICSA53651.2022.00023.

Appendix

Included Publications

S. Duri, M. Gruteser, X. Liu, *et al.*, "Framework for security and privacy in automotive telematics," in *Proceedings of the 2nd International Workshop on Mobile Commerce*, ser. WMC '02, event-place: Atlanta, Georgia, USA, New York, NY, USA: Association for Computing Machinery, 2002, pp. 25–32, ISBN: 1-58113-600-5. DOI: 10.1145/570705.570711. [Online]. Available: https://doi.org/10.1145/570705.570711.

J. Y. Choi, M. Jakobsson, and S. Wetzel, "Balancing auditability and privacy in vehicular networks," in *Proceedings of the 1st ACM International Workshop on Quality of Service & Security in Wireless and Mobile Networks*, ser. Q2SWinet '05, event-place: Montreal, Quebec, Canada, New York, NY, USA: Association for Computing Machinery, 2005, pp. 79–87, ISBN: 1-59593-241-0. DOI: 10.1145/1089761.1089775. [Online]. Available: https://doi.org/10.1145/1089761.1089775.

C. H. Cheong and M. H. Wong, "Mining popular paths in a transportation database system with privacy protection," in *22nd International Conference on Data Engineering Workshops (ICDEW'06)*, IEEE, 2006, pp. x122–x122. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/1623917.

J. Guo and J. P. Baugh, "Security and privacy in vehicle safety communication applications," *SAE Transactions*, pp. 721–727, 2006, Publisher: JSTOR. [Online]. Available: https://www.jstor.org/stable/44700103?seq=2.

N. M. Rabadi and S. M. Mahmud, "Privacy protection among drivers in vehicle-to-vehicle communication networks," in *2007 4th IEEE Consumer Communications and Networking Conference*, IEEE, 2007, pp. 281–286. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/4199150.

P. Cencioni and R. Di Pietro, "A mechanism to enforce privacy in vehicle-to-infrastructure communication," *Computer communications*, vol. 31, no. 12, pp. 2790–2802, 2008, Publisher: Elsevier. DOI: 10.1016/j.comcom.2007.12.009.

C.-I. Fan, R.-H. Hsu, and C.-H. Tseng, "Pairing-based message authentication scheme with privacy protection in vehicular ad hoc networks," in *Proceedings of the International Conference on Mobile Technology, Applications, and Systems*, ser. Mobility '08, event-place: Yilan, Taiwan, New York, NY, USA: Association for Computing Machinery, 2008, ISBN: 978-1-60558-089-0. DOI: 10.1145/1506270.1506372. [Online]. Available: https://doi.org/10.1145/1506270.1506372.

R. Shigetomi, M. Sato, K. Uehara, *et al.*, "An efficient scheme to protect privacy in probe vehicle information system," in *2008 8th International Conference on ITS Telecommunications*, IEEE, 2008, pp. 84–88. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/4740232.

Q. Wu, J. Domingo-Ferrer, and U. Gonzalez-Nicolas, "Balanced trustworthiness, safety, and privacy in vehicle-to-vehicle communications," *IEEE Transactions on Vehicular Technology*, vol. 59, no. 2, pp. 559–573, 2009, Publisher: IEEE. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/5290062.

A. Monreale, R. Trasarti, C. Renso, *et al.*, "Preserving privacy in semantic-rich trajectories of human mobility," in *Proceedings of the 3rd ACM SIGSPATIAL International Workshop on Security and Privacy in GIS and LBS*, ser. SPRINGL '10, event-place: San Jose, California, New York, NY, USA: Association for Computing Machinery, 2010, pp. 47–54, ISBN: 978-1-4503-0435-1. DOI: 10.1145/1868470.1868481. [Online]. Available: https://doi.org/10.1145/1868470.1868481.

F. M. Salem, M. H. Ibrahim, and I. Ibrahim, "Non-interactive authentication scheme providing privacy among drivers in vehicle-to-vehicle networks," in *2010 Sixth International Conference on Networking and Services*, IEEE, 2010, pp. 156–161. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/5460654.

O. Abumansoor, A. Boukerche, B. Landfeldt, *et al.*, "Privacy preserving neighborhood awareness in vehicular ad hoc networks," in *Proceedings of the 7th ACM Symposium on QoS and Security for Wireless and Mobile Networks*, ser. Q2SWinet '11, event-place: Miami, Florida, USA, New York, NY, USA: Association for Computing Machinery, 2011, pp. 17–20, ISBN: 978-1-4503-0899-1. DOI: 10.1145/2069105.2069109. [Online]. Available: https://doi.org/10.1145/2069105.2069109.

J. Singh, "Technique for privacy preserving real-time vehicle tracking using 802.11p technology," in *Proceedings of the 9th International Conference on Advances in Mobile Computing and Multimedia*, ser. MoMM '11, event-place: Ho Chi Minh City, Vietnam, New York, NY, USA: Association for Computing Machinery, 2011, pp. 206–209, ISBN: 978-1-4503-0785-7. DOI: 10.1145/2095697.2095736. [Online]. Available: https://doi.org/10.1145/2095697.2095736.

N. Asaj, B. Wiedersheim, A. Held, *et al.*, "Towards an identity-based data model for an automotive privacy process," in *2012 International Conference on Privacy, Security, Risk and Trust and 2012 International Confernece on Social Computing*, IEEE, 2012, pp. 789–796. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/6406325.

D. Da Silva, T. Ann Kosa, S. Marsh, *et al.*, "Examining privacy in vehicular ad-hoc networks," in *Proceedings of the Second ACM International Symposium on Design and Analysis of Intelligent Vehicular Networks and Applications*, ser. DIVANet '12, event-place: Paphos, Cyprus, New York, NY, USA: Association for Computing Machinery, 2012, pp. 105–110, ISBN: 978-1-4503-1625-5. DOI: 10.1145/2386958.2386974. [Online]. Available: https://doi.org/10.1145/2386958.2386974.

S. Hendrik and R. Yves, "Security and privacy for in-vehicle networks," in *2012 IEEE 1st International Workshop on Vehicular Communications, Sensing, and Computing (VCSC), Seoul, Korea (South), Jun 18*, vol. 18, 2012, pp. 12–17. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/6281235.

D. Kopanaki, N. Pelekis, A. Gkoulalas-Divanis, *et al.*, "A framework for mobility pattern mining and privacy-aware querying of trajectory data," in *Hellenic Data Management Symposium*, 2012. [Online]. Available: https://www.uhasselt.be/documents/datasim/papers/a-framework-for-mobility-pattern-mining.pdf.

L. Malina, J. Hajný, and V. Zeman, "Group signatures for secure and privacy preserving vehicular ad hoc networks," in *Proceedings of the 8h ACM Symposium on QoS and Security for Wireless and Mobile Networks*, ser. Q2SWinet '12, event-place: Paphos, Cyprus, New York, NY, USA: Association for Computing Machinery, 2012, pp. 71–74, ISBN: 978-1-4503-1619-4. DOI: 10.1145/2387218.2387232. [Online]. Available: https://doi.org/10.1145/2387218.2387232.

F. M. Salem, M. H. Ibrahim, and I. Ibrahim, "Efficient noninteractive secure protocol enforcing privacy in vehicle-to-roadside communication networks," *International Journal of Vehicular Technology*, vol. 2012, 2012, Publisher: Hindawi. [Online]. Available: https://downloads.hindawi.com/archive/2012/862368.pdf.

M. Stegelmann and D. Kesdogan, "V2gpriv: Vehicle-to-grid privacy in the smart grid," in *Cyberspace Safety and Security: 4th International Symposium, CSS 2012, Melbourne, Australia, December 12-13, 2012. Proceedings 4*, Springer, 2012, pp. 93–107. [Online]. Available: https://link.springer.com/chapter/10.1007/978-3-642-35362-8_9.

N. Alexiou, M. Laganà, S. Gisdakis, *et al.*, "VeSPA: Vehicular security and privacy-preserving architecture," in *Proceedings of the 2nd ACM Workshop on Hot Topics on Wireless Network Security and Privacy*, ser. HotWiSec '13, event-place: Budapest, Hungary, New York, NY, USA: Association for Computing Machinery, 2013, pp. 19–24, ISBN: 978-1-4503-2003-0. DOI: 10.1145/2463183.2463189. [Online]. Available: https://doi.org/10.1145/2463183.2463189.

D. Angermeier, A. Kiening, and F. Stumpf, "PAL - privacy augmented LTE: A privacy-preserving scheme for vehicular LTE communication," in *Proceeding of the Tenth ACM International Workshop on Vehicular Inter-Networking, Systems, and Applications*, ser. VANET '13, event-place: Taipei, Taiwan, New York, NY, USA: Association for Computing Machinery, 2013, pp. 1–10, ISBN: 978-1-4503-2073-3. DOI: 10.1145/2482967.2482975. [Online]. Available: https://doi.org/10.1145/2482967.2482975.

H. Nicanfar, P. TalebiFard, S. Hosseininezhad, *et al.*, "Security and privacy of electric vehicles in the smart grid context: Problem and solution," in *Proceedings of the Third ACM International Symposium on Design and Analysis of Intelligent Vehicular Networks and Applications*, ser. DIVANet '13, event-place: Barcelona, Spain, New York, NY, USA: Association for Computing Machinery, 2013, pp. 45–54, ISBN: 978-1-4503-2358-1. DOI: 10.1145/2512921.2512926. [Online]. Available: https://doi.org/10.1145/2512921.2512926.

C. Patsakis and A. Solanas, "Privacy-aware event data recorders: Cryptography meets the automotive industry again," *IEEE Communications Magazine*, vol. 51, no. 12, pp. 122–128, 2013, Publisher: IEEE. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/6685767.

H. Wu, W. S. Ng, K.-L. Tan, *et al.*, "A privacy preserving framework for managing vehicle data in road pricing systems," in *Proceedings of the 19th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, ser. KDD '13, event-place: Chicago, Illinois, USA, New York, NY, USA: Association for Computing Machinery, 2013, pp. 1427–1435, ISBN: 978-1-4503-2174-7. DOI: 10.1145/2487575.2488206. [Online]. Available: https://doi.org/10.1145/2487575.2488206.

A. Zierfuss and R. Sendag, "The impact of data complexity on privacy management in vehicle to infrastructure applications," in *2013 International Conference on Connected Vehicles and Expo (ICCVE)*, IEEE, 2013, pp. 753–760. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/6799890.

G. Avoine, L. Calderoni, J. Delvaux, *et al.*, "Passengers information in public transport and privacy: Can anonymous tickets prevent tracking?" *International Journal of Information Management*, vol. 34, no. 5, pp. 682–688, 2014, Publisher: Elsevier. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0268401214000620.

F. Callegati, A. Campi, M. Prandini, *et al.*, "PRIVACY ISSUES IN a CLEARING SYSTEM FOR a REGIONAL-SCALE PUBLIC TRANSPORT NETWORK," in *Proceedings of the 5th INTERNATIONAL CONFERENCE ON INTERNET TECHNOLOGIES & SOCIETY*, IADIS Press, 2014,

pp. 11–22. [Online]. Available: https://cris.unibo.it/handle/11585/462589.

I. Gudymenko, "A privacy-preserving e-ticketing system for public transportation supporting fine-granular billing and local validation," in *Proceedings of the 7th International Conference on Security of Information and Networks*, 2014, pp. 101–108.

C. Rottondi, S. Fontana, and G. Verticale, "Enabling privacy in vehicle-to-grid interactions for battery recharging," *Energies*, vol. 7, no. 5, pp. 2780–2798, 2014, Publisher: Molecular Diversity Preservation International (MDPI). [Online]. Available: https://www.mdpi.com/1996-1073/7/5/2780.

F. Callegati, A. Campi, A. Melis, *et al.*, "Privacy-preserving design of data processing systems in the public transport context," *Pacific Asia Journal of the Association for Information Systems*, vol. 7, no. 4, p. 4, 2015.

M. Milutinovic, K. Decroix, V. Naessens, *et al.*, "Privacy-preserving public transport ticketing system," in *Data and Applications Security and Privacy XXIX: 29th Annual IFIP WG 11.3 Working Conference, DBSec 2015, Fairfax, VA, USA, July 13-15, 2015, Proceedings 29*, Springer, 2015, pp. 135–150.

A. Rupp, F. Baldimtsi, G. Hinterwälder, *et al.*, "Cryptographic theory meets practice: Efficient and privacy-preserving payments for public transport," *ACM Trans. Inf. Syst. Secur.*, vol. 17, no. 3, Mar. 2015, Place: New York, NY, USA Publisher: Association for Computing Machinery, ISSN: 1094-9224. DOI: 10.1145/2699904. [Online]. Available: https://doi.org/10.1145/2699904.

K. Singh, P. Saini, S. Rani, *et al.*, "Authentication and privacy preserving message transfer scheme for vehicular ad hoc networks (VANETs)," in *Proceedings of the 12th ACM International Conference on Computing Frontiers*, ser. CF '15, event-place: Ischia, Italy, New York, NY, USA: Association for Computing Machinery, 2015, ISBN: 978-1-4503-3358-0. DOI: 10.1145/2742854.2745718. [Online]. Available: https://doi.org/10.1145/2742854.2745718.

H. Wang, B. Qin, Q. Wu, *et al.*, "TPP: Traceable privacy-preserving communication and precise reward for vehicle-to-grid networks in smart grids," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 11, pp. 2340–2351, 2015, Publisher: IEEE. [Online]. Available: https://ieeexplore.ieee.org/document/7155558.

S. U. Hussain and F. Koushanfar, "Privacy preserving localization for smart automotive systems," in *Proceedings of the 53rd Annual Design Automation Conference*, ser. DAC '16, event-place: Austin, Texas, New York, NY, USA: Association for Computing Machinery, 2016, ISBN: 978-1-4503-

4236-0. DOI: 10.1145/2897937.2898071. [Online]. Available: https://doi.org/10.1145/2897937.2898071.

Z. Wan, W.-T. Zhu, and G. Wang, "PRAC: Efficient privacy protection for vehicle-to-grid communications in the smart grid," *Computers & security*, vol. 62, pp. 246–256, 2016, Publisher: Elsevier. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0167404816300761.

A. Dorri, M. Steger, S. S. Kanhere, *et al.*, "Blockchain: A distributed solution to automotive security and privacy," *IEEE Communications Magazine*, vol. 55, no. 12, pp. 119–125, 2017, Publisher: IEEE. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/8198814.

J. Joy and M. Gerla, "Privacy risks in vehicle grids and autonomous cars," in *Proceedings of the 2nd ACM International Workshop on Smart, Autonomous, and Connected Vehicular Systems and Services*, ser. CarSys '17, event-place: Snowbird, Utah, USA, New York, NY, USA: Association for Computing Machinery, 2017, pp. 19–23, ISBN: 978-1-4503-5146-1. DOI: 10.1145/3131944.3133938. [Online]. Available: https://doi.org/10.1145/3131944.3133938.

B. Nelson and T. Olovsson, "Introducing differential privacy to the automotive domain: Opportunities and challenges," in *2017 IEEE 86th Vehicular Technology Conference (VTC-Fall)*, IEEE, 2017, pp. 1–7.

C. Plappert, D. Zelle, C. Krauß, *et al.*, "A privacy-aware data access system for automotive applications," in *15th ESCAR Embedded Security in Cars Conference*, 2017, pp. 27–65. [Online]. Available: https://sedafa-projekt.de/media/EscarEU2017_Zelle.pdf.

P. Sui, X. Li, and Y. Bai, "A study of enhancing privacy for intelligent transportation systems: K -correlation privacy model against moving preference attacks for location trajectory data," *IEEE Access*, vol. 5, pp. 24 555–24 567, 2017, ISSN: 2169-3536. DOI: 10.1109/ACCESS.2017.2767641. [Online]. Available: https://ieeexplore.ieee.org/document/8089343.

V. Damjanovic-Behrendt, "A digital twin-based privacy enhancement mechanism for the automotive industry," in *2018 International Conference on Intelligent Systems (IS)*, IEEE, 2018, pp. 272–279. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/8710526.

Z. Hong, F. Tang, and W. Luo, "Privacy-preserving aggregate signcryption for vehicular ad hoc networks," in *Proceedings of the 2nd International Conference on Cryptography, Security and Privacy*, ser. ICCSP 2018, event-place: Guiyang, China, New York, NY, USA: Association for Computing Machinery, 2018, pp. 72–76, ISBN: 978-1-4503-6361-7. DOI:

10.1145/3199478.3199484. [Online]. Available: https://doi.org/10.1145/3199478.3199484.

S. U. Hussain and F. Koushanfar, "P3: Privacy preserving positioning for smart automotive systems," *ACM Trans. Des. Autom. Electron. Syst.*, vol. 23, no. 6, Nov. 2018, Place: New York, NY, USA Publisher: Association for Computing Machinery, ISSN: 1084-4309. DOI: 10.1145/3236625. [Online]. Available: https://doi.org/10.1145/3236625.

Z. Lu, Z. H. Du Suguo, C. Cailian, *et al.*, "Location privacy in usage-based automotive insurance: Attack and countermeasures," *IEEE Trans. Inf. Forensics Secur.*, pp. 1–1, 2018. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/8387782.

S. O. Ogundoyin, "An anonymous and privacy-preserving scheme for efficient traffic movement analysis in intelligent transportation system," *security and privacy*, vol. 1, no. 6, e50, 2018, Publisher: Wiley Online Library. [Online]. Available: https://onlinelibrary.wiley.com/doi/full/10.1002/spy2.50.

A. Jolfaei and K. Kant, "Privacy and security of connected vehicles in intelligent transportation system," in *2019 49th Annual IEEE/IFIP International Conference on Dependable Systems and Networks–Supplemental Volume (DSN-S)*, IEEE, 2019, pp. 9–10. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/8805750/.

H. Li, D. Ma, B. Medjahed, *et al.*, "Analyzing and preventing data privacy leakage in connected vehicle services," *SAE International Journal of Advances and Current Practices in Mobility*, vol. 1, no. 2019, pp. 1035–1045, 2019. [Online]. Available: https://saemobilus.sae.org/content/2019-01-0478.

X. Liu, Q. Bing, X. Lu, *et al.*, "An identity privacy protection strategy in vehicle named data network," in *2019 IEEE International Conferences on Ubiquitous Computing & Communications (IUCC) and Data Science and Computational Intelligence (DSCI) and Smart Computing, Networking and Services (SmartCNS)*, IEEE, 2019, pp. 818–822. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/8982705/.

W. Ma and L. Mashayekhy, "Privacy-by-design distributed offloading for vehicular edge computing," in *Proceedings of the 12th IEEE/ACM International Conference on Utility and Cloud Computing*, ser. UCC'19, event-place: Auckland, New Zealand, New York, NY, USA: Association for Computing Machinery, 2019, pp. 101–110, ISBN: 978-1-4503-6894-0. DOI: 10.1145/3344341.3368804. [Online]. Available: https://doi.org/10.1145/3344341.3368804.

K. Mankar and C. T. Wasnik, "Improved conditional privacy protection in vehicle ad-hoc networks," in *2019 3rd International Conference on Computing Methodologies and Communication (ICCMC)*, IEEE, 2019, pp. 328–334. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/8819827.

T. Meuser, D. Bischoff, and R. Steinmetz, "Location privacy in heterogeneous vehicular networks," in *Proceedings of the 13th ACM International Conference on Distributed and Event-Based Systems*, ser. DEBS '19, event-place: Darmstadt, Germany, New York, NY, USA: Association for Computing Machinery, 2019, pp. 260–261, ISBN: 978-1-4503-6794-3. DOI: 10.1145/3328905.3332515. [Online]. Available: https://doi.org/10.1145/3328905.3332515.

C. Qiu and A. C. Squicciarini, "Location privacy protection in vehicle-based spatial crowdsourcing via geo-indistinguishability," in *2019 IEEE 39th International Conference on Distributed Computing Systems (ICDCS)*, ISSN: 2575-8411, Jul. 2019, pp. 1061–1071. DOI: 10.1109/ICDCS.2019.00109. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/9259240.

L. ShanGuo, "Efficient privacy protection authentication scheme in vehicle ad hoc networks," in *Cyberspace Safety and Security: 11th International Symposium, CSS 2019, Guangzhou, China, December 1–3, 2019, Proceedings, Part I 11*, Springer, 2019, pp. 279–288. [Online]. Available: https://link.springer.com/chapter/10.1007/978-3-030-37337-5_23.

S. Chavhan, D. Gupta, S. Garg, *et al.*, "Privacy and security management in intelligent transportation system," *IEEE Access*, vol. 8, pp. 148 677–148 688, 2020, Publisher: IEEE. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/9162025.

Y. Guan, R. Lu, Y. Zheng, *et al.*, "Achieving privacy-preserving vehicle selection for effective content dissemination in smart cities," in *GLOBECOM 2020-2020 IEEE Global Communications Conference*, IEEE, 2020, pp. 1–6. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/9348253.

B. V. Kumar, A. Ravishankar, A. Karan, *et al.*, "A smart public transportation system for reliable and hassle free conveyance in sustainable smart cities," in *2020 International Conference on Computer Communication and Informatics (ICCCI)*, 2020, pp. 1–6. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/9104094.

Y. Li, K. Ouyang, N. Li, *et al.*, "A blockchain-assisted intelligent transportation system promoting data services with privacy protection," *Sensors*, vol. 20, no. 9, p. 2483, 2020, Publisher: MDPI.

X. Liu and Y. Zhu, "Privacy and utility preserving trajectory data publishing for intelligent transportation systems," *IEEE Access*, vol. 8, pp. 176 454–176 466, 2020, ISSN: 2169-3536. DOI: 10.1109/ACCESS.2020.3027299.

D. Tabellion, M. Wolf, J. Britz, *et al.*, "Security, privacy and trust for a crowd-sourced semantic accessibility database for public transport," in *HCI International 2020–Late Breaking Papers: Universal Access and Inclusive Design: 22nd HCI International Conference, HCII 2020, Copenhagen, Denmark, July 19–24, 2020, Proceedings 22*, Springer, 2020, pp. 712–727. [Online]. Available: https://link.springer.com/chapter/10.1007/978-3-030-60149-2_54.

H. Tian, X. Li, H. Quan, *et al.*, "A lightweight attribute-based access control scheme for intelligent transportation system with full privacy protection," *IEEE Sensors Journal*, vol. 21, no. 14, pp. 15 793–15 806, 2020, Publisher: IEEE. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/9222175.

Q. Wang, M. Ou, Y. Yang, *et al.*, "Conditional privacy-preserving anonymous authentication scheme with forward security in vehicle-to-grid networks," *IEEE Access*, vol. 8, pp. 217 592–217 602, 2020, Publisher: IEEE. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/9268941/.

L. Zhang, J. Wang, and Y. Mu, "Secure and privacy-preserving attribute-based sharing framework in vehicles ad hoc networks," *IEEE Access*, vol. 8, pp. 116 781–116 795, 2020, ISSN: 2169-3536. DOI: 10.1109/ACCESS.2020.3004247.

Y. Zhao, X. Meng, and B. Kang, "A task allocation scheme for protecting location privacy in vehicle ad hoc networks," in *2020 IEEE 3rd International Conference on Automation, Electronics and Electrical Engineering (AUTEEE)*, IEEE, 2020, pp. 395–402.

C. Zhou, T. Wang, H. Tian, *et al.*, "A top-k query scheme with privacy preservation for intelligent vehicle network in mobile IoT," *IEEE Access*, vol. 8, pp. 81 698–81 710, 2020. DOI: 10.1109/ACCESS.2020.2990932.

Y. Abdelwahed, O. Khaled, A. Elhamahmi, *et al.*, "Privacy-centric AI-based real-time storage-less edge computing approaches for passenger counting and action classification on public transport vehicles," in *2021 IEEE International Intelligent Transportation Systems Conference (ITSC)*, IEEE, 2021, pp. 3116–3121. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/9564830.

U. Ahmed, J. C.-W. Lin, and G. Srivastava, "Privacy-preserving deep reinforcement learning in vehicle ad hoc networks," *IEEE consumer electronics magazine*, vol. 11, no. 6, pp. 41–48, 2021, Publisher: IEEE. [On-

line]. Available: https://ieeexplore.ieee.org/abstract/document/9451559.

B. S. Bhati, J. Ivanchev, I. Bojic, *et al.*, "Utility-driven k-anonymization of public transport user data," *IEEE Access*, vol. 9, pp. 23 608–23 623, 2021, Publisher: IEEE. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/9340178.

G. Costantino, F. Martinelli, I. Matteucci, *et al.*, "A privacy-preserving infrastructure for driver's reputation aware automotive services," in *Socio-Technical Aspects in Security and Trust: 9th International Workshop, STAST 2019, Luxembourg City, Luxembourg, September 26, 2019, Revised Selected Papers 9*, Springer, 2021, pp. 159–174. [Online]. Available: https://link.springer.com/chapter/10.1007/978-3-030-55958-8_9.

X. Ding, S. Cao, F. Dou, *et al.*, "Certificateless aggregate signature scheme with conditional privacy protection in vehicle networking," in *Journal of Physics: Conference Series*, Issue: 1, vol. 2026, IOP Publishing, 2021, p. 012 044. [Online]. Available: https://iopscience.iop.org/article/10.1088/1742-6596/2026/1/012044/meta.

P. Franke, M. Kreutzer, and H. Simo, "Privacy-preserving IDS for in-vehicle networks with local differential privacy," in *Privacy and Identity Management: 15th IFIP WG 9.2, 9.6/11.7, 11.6/SIG 9.2. 2 International Summer School, Maribor, Slovenia, September 21–23, 2020, Revised Selected Papers 15*, Springer, 2021, pp. 58–77. [Online]. Available: https://link.springer.com/chapter/10.1007/978-3-030-72465-8_4.

X. Han, D. Tian, X. Duan, *et al.*, "A dual mode privacy-preserving scheme enabled secure and anonymous for edge computing assisted internet of vehicle networks," in *Proceedings of the 11th ACM Symposium on Design and Analysis of Intelligent Vehicular Networks and Applications*, ser. DIVANet '21, event-place: Alicante, Spain, New York, NY, USA: Association for Computing Machinery, 2021, pp. 65–70, ISBN: 978-1-4503-9081-1. DOI: 10.1145/3479243.3487310. [Online]. Available: https://doi.org/10.1145/3479243.3487310.

T. Jannusch, F. David-Spickermann, D. Shannon, *et al.*, "Surveillance and privacy–beyond the panopticon. an exploration of 720-degree observation in level 3 and 4 vehicle automation," *Technology in Society*, vol. 66, p. 101 667, 2021, Publisher: Elsevier. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0160791X21001421.

R. Kumar, P. Kumar, R. Tripathi, *et al.*, "BDTwin: An integrated framework for enhancing security and privacy in cybertwin-driven automotive industrial internet of things," *IEEE Internet of Things Journal*, vol. 9, no. 18, pp. 17 110–17 119, 2021, Publisher: IEEE. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/9583667.

Y. Qian, Y. Ma, J. Chen, *et al.*, "Optimal location privacy preserving and service quality guaranteed task allocation in vehicle-based crowdsensing networks," *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 7, pp. 4367–4375, 2021, Publisher: IEEE. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/9477299.

G. Qiu and Y. Shen, "Mobility-aware differentially private trajectory for privacy-preserving continual crowdsourcing," *IEEE Access*, vol. 9, 2021, ISSN: 2169-3536. DOI: 10.1109/ACCESS.2021.3058211.

J. Rao, S. Gao, and X. Zhu, "VTSV: A privacy-preserving vehicle trajectory simulation and visualization platform using deep reinforcement learning," in *Proceedings of the 4th ACM SIGSPATIAL International Workshop on AI for Geographic Knowledge Discovery*, ser. GEOAI '21, event-place: Beijing, China, New York, NY, USA: Association for Computing Machinery, 2021, pp. 43–46, ISBN: 978-1-4503-9120-7. DOI: 10.1145/3486635.3491073. [Online]. Available: https://doi.org/10.1145/3486635.3491073.

A.-S. Roman, B. Genge, A.-V. Duka, *et al.*, "Privacy-preserving tampering detection in automotive systems," *Electronics*, vol. 10, no. 24, p. 3161, 2021, Publisher: MDPI. [Online]. Available: https://www.mdpi.com/2079-9292/10/24/3161.

R. Seidel, N. Jahn, S. Seo, *et al.*, "NAPC: A neural algorithm for automated passenger counting in public transport on a privacy-friendly dataset," *IEEE Open Journal of Intelligent Transportation Systems*, vol. 3, pp. 33–44, 2021, Publisher: IEEE. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/9665722.

I. S. Shaleesh, A. A. Almohammedi, N. I. Mohammad, *et al.*, "Cooperation and radio silence strategy in mix zone to protect location privacy of vehicle in VANET," *Tikrit Journal of Engineering Sciences*, vol. 28, no. 1, pp. 31–39, 2021.

Z. Xu, J. Zhang, P.-w. Tsai, *et al.*, "Spatiotemporal mobility based trajectory privacy-preserving algorithm in location-based services," *Sensors*, vol. 21, no. 6, p. 2021, 2021, Publisher: MDPI. [Online]. Available: https://www.mdpi.com/1424-8220/21/6/2021.

Y. Yang, J. Wu, C. Long, *et al.*, "A blockchain-based cross-domain authentication for conditional privacy preserving in vehicular ad-hoc network," in *2021 The 3rd International Conference on Blockchain Technology*, ser. ICBCT '21, event-place: Shanghai, China, New York, NY, USA: Association for Computing Machinery, 2021, pp. 183–188, ISBN: 978-1-4503-8962-4. DOI: 10.1145/3460537.3460545. [Online]. Available: https://doi.org/10.1145/3460537.3460545.

L. Agilandeeswari, S. Paliwal, A. Chandrakar, *et al.*, "A new lightweight conditional privacy preserving authentication and key–agreement protocol in social internet of things for vehicle to smart grid networks," *Multimedia Tools and Applications*, vol. 81, no. 19, pp. 27 683–27 710, 2022, Publisher: Springer. [Online]. Available: https://link.springer.com/article/10.1007/s11042-022-12946-5.

P. Barbecho Bautista, L. F. Urquiza-Aguiar, and M. Aguilar Igartua, "Privacy-aware vehicle emissions control system for traffic light intersections," in *Proceedings of the 19th ACM International Symposium on Performance Evaluation of Wireless Ad Hoc, Sensor, & Ubiquitous Networks*, ser. PE-WASUN '22, event-place: Montreal, Quebec, Canada, New York, NY, USA: Association for Computing Machinery, 2022, pp. 99–106, ISBN: 978-1-4503-9483-3. DOI: 10.1145/3551663.3558686. [Online]. Available: https://doi.org/10.1145/3551663.3558686.

M. He, F. Bai, C. Zhang, *et al.*, "A blockchain-enabled location privacy-preserving under local differential privacy for internet of vehicles," in *Proceedings of the 2022 4th Blockchain and Internet of Things Conference*, ser. BIOTC '22, event-place: Tokyo, China, New York, NY, USA: Association for Computing Machinery, 2022, pp. 84–91, ISBN: 978-1-4503-9662-2. DOI: 10.1145/3559795.3559807. [Online]. Available: https://doi.org/10.1145/3559795.3559807.

Q. Huang, X. Xu, H. Chen, *et al.*, "A vehicle trajectory privacy preservation method based on caching and dummy locations in the internet of vehicles," *Sensors*, vol. 22, no. 12, p. 4423, 2022, Publisher: MDPI. [Online]. Available: https://www.mdpi.com/1424-8220/22/12/4423.

F. Klement, H. C. Pöhls, and S. Katzenbeisser, "Man-in-the-obd: A modular, protocol agnostic firewall for automotive dongles to enhance privacy and security," in *International Workshop on Attacks and Defenses for Internet-of-Things*, Springer, 2022, pp. 143–164. [Online]. Available: https://link.springer.com/chapter/10.1007/978-3-031-21311-3_7.

S. Li and M. Han, "Priv-IDS: A privacy protection and intrusion detection framework for in-vehicle network," in *International Conference on Machine Learning for Cyber Security*, Springer, 2022, pp. 165–179. [Online]. Available: https://link.springer.com/chapter/10.1007/978-3-031-20099-1_14.

T. Li, S. Xie, Z. Zeng, *et al.*, "ATPS: An AI based trust-aware and privacy-preserving system for vehicle managements in sustainable VANETs," *IEEE Transactions on Intelligent Transportation Systems*, vol. 23, no. 10, pp. 19 837–19 851, 2022, Publisher: IEEE. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/9851637.

L. Malina, P. Seda, Z. Martinasek, *et al.*, "On security and privacy in vehicle speed-limiting services in the internet of vehicles," *IEEE Intelligent Transportation Systems Magazine*, vol. 15, no. 1, pp. 8–22, 2022, Publisher: IEEE. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/9893214.

S. O. Ogundoyin, "A privacy-preserving multisubset data aggregation scheme with fault resilience for intelligent transportation system," *Information Security Journal: A Global Perspective*, vol. 31, no. 4, pp. 387–410, 2022, Publisher: Taylor & Francis. [Online]. Available: https://www.tandfonline.com/doi/full/10.1080/19393555.2022.2036879.

R. P. Parameswarath, P. Gope, and B. Sikdar, "User-empowered privacy-preserving authentication protocol for electric vehicle charging based on decentralized identity and verifiable credential," *ACM Trans. Manage. Inf. Syst.*, vol. 13, no. 4, Aug. 2022, Place: New York, NY, USA Publisher: Association for Computing Machinery, ISSN: 2158-656X. DOI: 10.1145/3532869. [Online]. Available: https://doi.org/10.1145/3532869.

C. Qiu, A. Squicciarini, C. Pang, *et al.*, "Location privacy protection in vehicle-based spatial crowdsourcing via geo-indistinguishability," *IEEE Transactions on Mobile Computing*, vol. 21, no. 7, pp. 2436–2450, Jul. 2022, ISSN: 1558-0660. DOI: 10.1109/TMC.2020.3037911.

C. Qiu, L. Yan, A. Squicciarini, *et al.*, "TrafficAdaptor: An adaptive obfuscation strategy for vehicle location privacy against traffic flow aware attacks," in *Proceedings of the 30th International Conference on Advances in Geographic Information Systems*, ser. SIGSPATIAL '22, event-place: Seattle, Washington, New York, NY, USA: Association for Computing Machinery, 2022, ISBN: 978-1-4503-9529-8. DOI: 10.1145/3557915.3560938. [Online]. Available: https://doi.org/10.1145/3557915.3560938.

V. Renganathan, E. Yurtsever, Q. Ahmed, *et al.*, "Valet attack on privacy: A cybersecurity threat in automotive bluetooth infotainment systems," *Cybersecurity*, vol. 5, no. 1, p. 30, 2022, Publisher: Springer. [Online]. Available: https://link.springer.com/article/10.1186/s42400-022-00132-x.

S. Righini, L. Calderoni, and D. Maio, "A privacy-aware zero interaction smart mobility system," *IEEE Access*, vol. 10, pp. 11 924–11 937, 2022, Publisher: IEEE. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/9693973/.

S. Sciancalepore and D. R. George, "Privacy-preserving trajectory matching on autonomous unmanned aerial vehicles," in *Proceedings of the 38th ACSAC '22*, event-place: Austin, TX, USA, New York, NY, USA: Association for Computing Machinery, 2022, pp. 1–12, ISBN: 978-1-4503-9759-9. DOI: 10.1145/3564625.3564626.

R. Sun, Y. Zhang, Z. Wang, *et al.*, "Design of privacy-preserving in multi-link vehicle-ground communication," in *International Conference on Emerging Networking Architecture and Technologies*, Springer, 2022, pp. 209–220. [Online]. Available: https://link.springer.com/chapter/10.1007/978-981-19-9697-9_17.

A. K. Tyagi and M. M. Nair, "Preserving privacy using distributed ledger technology in intelligent transportation system," in *Proceedings of the 2022 Fourteenth International Conference on Contemporary Computing*, ser. IC3-2022, event-place: Noida, India, New York, NY, USA: Association for Computing Machinery, 2022, pp. 582–590, ISBN: 978-1-4503-9675-2. DOI: 10.1145/3549206.3549306. [Online]. Available: https://doi.org/10.1145/3549206.3549306.

K. Wang, C.-M. Chen, M. Shojafar, *et al.*, "AFFIRM: Provably forward privacy for searchable encryption in cooperative intelligent transportation system," *IEEE Transactions on Intelligent Transportation Systems*, vol. 23, no. 11, pp. 22 607–22 618, 2022, Publisher: IEEE. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/9788514.

Z. Ying, S. Cao, X. Liu, *et al.*, "PrivacySignal: Privacy-preserving traffic signal control for intelligent transportation system," *IEEE Transactions on Intelligent Transportation Systems*, vol. 23, no. 9, pp. 16 290–16 303, 2022, Publisher: IEEE. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/9713758.

I. U. Din, K. A. Awan, and A. Almogren, "Secure and privacy-preserving trust management system for trustworthy communications in intelligent transportation systems," *IEEE Access*, 2023, Publisher: IEEE. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/10168094.

R. Khan, A. Mehmood, Z. Iqbal, *et al.*, "Security and privacy in connected vehicle cyber physical system using zero knowledge succinct non interactive argument of knowledge over blockchain," *Applied Sciences*, vol. 13, no. 3, p. 1959, 2023, Publisher: MDPI. [Online]. Available: https://www.mdpi.com/2076-3417/13/3/1959.

J. Li and X. Yang, "Privacy-preserving charging station recommendation system for electric vehicles over blockchain," in *Proceedings of the 2022 5th International Conference on Blockchain Technology and Applications*, ser. ICBTA '22, event-place: Xi'an, China, New York, NY, USA: Association for Computing Machinery, 2023, pp. 140–146, ISBN: 978-1-4503-9757-5. DOI: 10.1145/3581971.3581991. [Online]. Available: https://doi.org/10.1145/3581971.3581991.

Y. Li, P. Hirmer, C. Stach, *et al.*, "Ensuring situation-aware privacy for connected vehicles," in *Proceedings of the 12th International Conference on the Internet of Things*, ser. IoT '22, event-place: Delft, Netherlands, New York, NY, USA: Association for Computing Machinery, 2023, pp. 135–138, ISBN: 978-1-4503-9665-3. DOI: 10.1145/3567445.3569163. [Online]. Available: https://doi.org/10.1145/3567445.3569163.

S. Löbner, C. Gartner, and F. Tronnier, "Privacy preserving data analysis with the encode, shuffle, analyse architecture in vehicular data sharing," in *Proceedings of the 2023 European Interdisciplinary Cybersecurity Conference*, ser. EICC '23, event-place: Stavanger, Norway, New York, NY, USA: Association for Computing Machinery, 2023, pp. 85–91, ISBN: 978-1-4503-9829-9. DOI: 10.1145/3590777.3590791. [Online]. Available: https://doi.org/10.1145/3590777.3590791.

H. Ruan, Q. Gong, Y. Chen, *et al.*, "Poster: A privacy-preserving heart rate prediction system for drivers in connected vehicles," in *Proceedings of the 21st Annual International Conference on Mobile Systems, Applications and Services*, ser. MobiSys '23, event-place: Helsinki, Finland, New York, NY, USA: Association for Computing Machinery, 2023, pp. 557–558. DOI: 10.1145/3581791.3597364. [Online]. Available: https://doi.org/10.1145/3581791.3597364.

H. Taslimasa, S. Dadkhah, E. C. P. Neto, *et al.*, "ImageFed: Practical privacy preserving intrusion detection system for in-vehicle CAN bus protocol," in *2023 IEEE 9th Intl Conference on Big Data Security on Cloud (BigDataSecurity), IEEE Intl Conference on High Performance and Smart Computing,(HPSC) and IEEE Intl Conference on Intelligent Data and Security (IDS)*, IEEE, 2023, pp. 122–129. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/10132145.

Y. Y. Liu, A. Cooke, and P. Thulasiraman, "Location privacy preservation of vehicle data in internet of vehicles," [Online]. Available: http://personales.upv.es/thinkmind/dl/conferences/internet/internet_2020/internet_2020_1_100_40038.pdf.