Privacy-Aware Data Sharing Policies for Autonomous Vehicle Collaboration

By Dr. Lena Nilsson

Associate Professor of Information Technology, Linköping University, Sweden

1. Introduction

In recent years, privacy concerns have become a major obstacle to the widespread adoption of data sharing technologies. To address this, the ride-sharing fleet owners and operators will want to be able to put privacy preservation technologies in place as protection against these threats. In addition, legislators and government entities are enacting privacy laws and regulations aimed at the collection and processing of personal data. These laws are designing data sharing frameworks based on a number of principles related to data subjects' trust and the data life-cycle, such as the right to be forgotten and tight access rights to personally identifiable information (PII), also for third-party services accessing the PII under user consent [1].

ADVANCES in sensor technology, data storage and processing capacities, communication systems and artificial intelligence (AI) have lead to major renaissance in the use of autonomous vehicles (AVs) [2]. Among different AV environments, AV ride-sharing fleets are regarded as the most promising application in terms of energy efficiency, reduction in CO2 emissions, transportation cost, and improvement of traffic flow. However, transportation-related data, such as personally identifiable information (e.g., origin-destination locations and arrival times for every trip) is being collected by AVs in large quantities, and may be used for services such as location-based advertising. Furthermore, data of this nature could be vulnerable to a variety of attacks and privacy risks.

1.1. Background and Motivation

[3] Autonomous vehicles have attracted attention from industry and academia and it is widely expected that connected and autonomous vehicles (CAVs) will be part of daily life in a few years' time. In Large- Scale Connected and Autonomous Vehicle (CAV) infrastructure in the

future, many connected and autonomous vehicles (CAVs) are expected to share data through public communication networks. To this end, a lot of research has been done in the fields of data collection and analysis on vehicles like in-vehicle information systems (IVIS) and intelligent transportation system (ITS) in recent years. However, privacy protection in achieving such collaboration is a significant challenge. For example, the detection of COVID-19 patients via driving patterns and the exchange of spatial information in the environment pose significant threats to drivers' privacy because it is possible to exploit these information to infer their identity.[4] With the proliferation of autonomous vehicle (AV) transportation, the way people ride and share transport facilities in daily life changed dramatically, which gives rise to several privacy and security issues such as surveillance, theft, infiltrators and even malicious activities, such as spreading the COVID-19. In intelligent transportation systems (ITS), governments and companies have been collecting and transmitting various traffic data over vehicular networks to infer, predict, and control future traffic patterns in a desirable way. Autonomous vehicles interact with the environment during normal operation for safe and efficient driving. So, sometimes collecting or transmitting the health information of vehicle users, e.g., COVID-19 in some cases, should be considered as out-of-norm or malicious activity. On the other hand, it should be reported to the central authority and the relevant authorities protecting user privacy so that they can immediately prevent potential risks, e.g., fines for COVID-19 patients, the creation of health passports for users, creating green and red zones.

1.2. Research Objectives

In this context, we propose an approach for the management of privacy-aware data-sharing policies among a network of autonomous vehicles [5]. Formation of vehicles into collaborative groups is explored along with the introduction of communication policies that preserve the privacy of the vehicles involved. The main target is the enhancement of coordination and communication among the vehicles in a manner that guarantees that the proprietary information of each vehicle is as safe as possible, thus limiting the danger that arises from the sharing of sensitive information in wireless environments. Enablement of efficient collaborative perception scenarios under strict privacy requirements naturally leads to the on-board deployment of boundary computers that locally fuse data from the surrounding vehicles. The formed coalitions share information under privacy-preserving policies so as to preserve important aspects of privacy as k-anonymity and differential confidentiality.

The proposed approach is mainly motivated by the fact that privacy-preserving data sharing is crucial when multiple vehicles are involved in full collaboration scenarios (e.g., platooning, joint perception, etc.) [6]. Nowadays, data-sharing is often achieved by centralized cloud servers that process and store data from multiple vehicles. Despite advantages in terms of scalability and ease of management, a cloud-centric architecture may cause a significant loss in user privacy. As a matter of fact, a centralized cloud server is an appealing target for a variety of attacks and, as keeps sensitive real-world data from multiple vehicles in a unique storage, it naturally poses serious privacy concerns [2].

2. Autonomous Vehicles and Data Sharing

CAVs are inherently electronic devices that generate terabytes of data continuously and can be quite vulnerable to cyber-attacks [7]. In scenario where CAVs can exchange information in a vehicular ad-hoc mesh network, this inherently creates data sharing concerns, particularly as long as one cannot trust whether the nodes distributing and consuming data are benign nodes or malicious nodes. From a privacy viewpoint, the situation is equally disturbing since the agile nature of this vehicular ad-hoc network can enable adversaries to capture and analytically reveal real-time information such as from how to drive to someone's daily routines. Intruders have been known to illegally re-route vehicle trajectories, which can lead to unsafe scenarios and have catastrophic consequences. At a national level, these untrusted scenarios can have impacts on the fundamental right to privacy for citizens and create potential new opportunities for industrial espionage. At another level, even if we assume a system-level trust between nodes, the ultimate decision on how to react on received information is still either overly expensive (because we react on individual falsified messages by sending additional confirmatory messages) or unsafe because we include the vehicle-to-vehicle messages directly into our immediate decision making process without a careful verification process.

Connected and Autonomous Vehicles (CAVs) are an emerging technology that has the potential to significantly impact our driving experiences, road safety, and the automobile industry as whole [5]. Through the sharing of information, CAVs could revolutionize how we build, use, and manage transportation networks. This might result in improvements to transportation efficiency, safety and the reduction in emissions. It is also anticipated that CAVs will be able to directly communicate with each other and with the surrounding road

infrastructure over Vehicle to Vehicle (V2V), Vehicle to Infrastructure (V2I) and Vehicle to Everything (V2X) communication channels [8]. By sharing their motion plans, sensor measurements, and allowed driving volumes, CAVs can enable smoother human-safe trajectories, provide early warnings of dangerous situations and allow the road infrastructure to adapt to the traffic state in real-time.

2.1. Overview of Autonomous Vehicle Technology

These challenges represent data that raise intense conversations on user information privacy. For instance, the information from occupants of a car or pedestrians who have been exposed to a danger generated by an autonomous car must be analyzed. In the emergency procedure, in an emergency, to share information quickly to realize a prediction algorithm to avoid the next accident, the autonomous car must be capable of sharing data from other cars [9]. A driving car is a sensor-equipped vehicle and the sensors, including cameras and LiDARs, record thousands of samples each second. These recordings are enough to unveil the patterns and behaviors of the passengers as well as the pedestrians on the streets. For privacy regulations, the marks and sounds of any characters enclosed in the data must be hidden.

Manufacturers are integrating connected vehicle features into vehicles to offer advanced intelligence, awareness, and control, luring the public with the futuristic promise of complete autonomous vehicle travel. Automakers are actively seeking to develop and establish the greatest security segmentation between connected autonomous vehicles (CAVs) and potential threats [10]. With connected device labor-saving increased to high levels, the comfort of cognitive service interventions and connected car safety concerns have increased. To guarantee the precision of systems and programs, car manufacturer obligations to integrate original equipment and connected services have emerged at high levels to uphold privacy and protection concerns [11].

2.2. Types of Data Generated by Autonomous Vehicles

Consequently, the data are obtained from different sensors and multiple modalities that may include (a) a camera to capture the dynamic state of objects over time which are the trackmarks of the object, XIGRU will be able to output the object features that it is needed through passing information to RPN module, (b) Inertial Measurement Unit (IMU) to capture driving state and (c) a GPS/Can-Bus system to capture vehicle states and help in localization. All of these data

are further digitalized via onboard processors and transmitted over a local wireless service. Given the variety of sensors, the data should not only be rich in various modality, but it is also a challenge formally combining information.

Intelligent vehicles (IVs) are loaded severely with various types of sensors, and they generate a large amount of driving data from scenes and driving behaviors [12]. Tesla's Shadow-Mode technology provides a novel solution by recording data from daily driving and delivering the data to the cloud with the consent and support of vehicle users to train decentralized algorithms, the privacy policy of which allows data collection during driving with full user consent and no personal data upload at the server side. This is to overcome the testing and verification barrier. Various IV manufacturers are also involved in building driving datasets for competitive edge [13].

3. Privacy Concerns in Data Sharing

The autonomous car is designed to collect lots of data related to the car's driver in order to meet the driver's requirement. With CAVs, the information privacy is of direct concern as the vehicle collects more than simple GPS location and also stores the driver car-driving capability, habits, instant information, etc. CIIRC is involved in identification of privacy threats: UICJVT-RAVT-3-21-2018-7- and later the improvement of detection of MADIK control system with a mechanism able to protect the MADIK control system from certain cyber threats2. As is logical to expect, several communication protocols and networks are developed by companies globally. This separation in communication protocols and networks can derive in not sharing important information. The secure and efficient data management will provide better performance and efficient communication between CAVs.

[7] The preservation of privacy and data security within connected and autonomous vehicles (CAVs) is of paramount importance [14]. It is well understood that as these new technologies become more prevalent in the market, privacy and data security concerns will become increasingly more important [15].

3.1. Data Privacy and Security Risks

Despite the event-driven policy focus on privacy, there are numerous reasons to adopt a broad perspective. This may illuminate how other high-level concerns interact with privacy, as well as better relate to alternative policy processes driven where privacy is less frequently the

primary concern. The potential range of broader policy and governance concerns and how they relate to privacy have received significantly limited attention. This paper presents a research findings in a multidisciplinary project which set out to create a prioritisation framework through which distinct sets of public interest perspectives—referred to as 'Impact Perspectives'—can be identified in order to understand and enable means of prioritising the public interest. The main finding is a comprehensive overview of the impact universe of suggested public interest concerns in the evolving applications of various IoT (Internet of Things) technologies and systems, including CAVs. The research also identified gaps in prioritising the public interest, e.g., data protection as an initial framing priority and only limited recognition of other privacy issues. It highlights privacy-by-necessity tensions that should be considered in the generation of intelligent systems across a range of existing and emergent policy [10].

Privacy impacts on policy in many ways, including in close relationships with, or even as a significant outcome of, the enactment of, particular policy (Bennett Coller 2014; Clarke 2015). One mechanism that has received a great deal of attention is data protection policy. Most data-dependent applications, such as autonomous driving and smart cities, implement privacy first, together with data protection, in their designs. Numerous alternative privacy frameworks exist, including privacy-by-design, privacy-preserving AI, privacy-enhancing technologies, and privacy-aware policies. This emphasis on privacy in data protection policy reflects understandable public concerns about information technology threats to personal data privacy and security [16].

3.2. Regulatory Frameworks and Compliance

[4] The autonomous transportation system entirely operated without human intervention is a potential future. Due to their high capacity to communicate and the fact that they are expected to travel long distances and durations, autonomous vehicles will circumstantially play a significant role in exchanging digital information. At the same time, they may collect a significant amount of passengers' data as well, posing new legal, regulatory and technical challenges to preserve the appropriate balance in ensuring public health without compromising the fundamental right to privacy. This concern is more relevant in the process of transformation of the Covid-19 pandemic, and it does not significantly change after the development of widespread vaccinations and the end of restrictive measures.[17] The existing

legal framework, particularly in the European Union (EU), requires policy-makers to defend privacy rights and apply the principle of data minimisation. The latter means that controllers must store data only for as long as needed, guaranteeing its proportionality to the scope of the legitimate purpose. Regardless of the medical analysis and decisions that could be improved while leveraging the large volumes of mobility data, the right to privacy and personal data protection should be untouched, and even strengthened. The enactment of such innovative legal regimes shall also support the level of public trust and openness, which are fundamental to the success of coronavirus containment strategies. The absence of rigorous legal schemes should be widely perceived as a further contagion driver, exacerbating general scepticism and suspicion.

4. Existing Data Sharing Policies

Connected autonomous vehicles (CAVs) have demonstrated the capability of transforming the transportation industry. However, without appropriate government regulations, the resulting safety, security, and privacy challenges may cripple the wide adoption of these vehicles. One of the most crucial issues affecting CAVs is the provision of security for the two key components of their value proposition: connectivity and autonomy. Recognizing the severity of the CAV cybersecurity challenge, governments and regulatory authorities are already taking multiple steps to impose security obligations on the manufacturers and to mandate standardization of a variety of security measures focused on the vehicle's electronic control unit (ECU) ecosystem. This article maps over 600 legal and regulatory documents on CAVs and IoT languages to a public interest framework known as the Impact Universe and the disclosure of informational and functional technologies that lighten the role of CAV cybersecurity standards in the discussion from the public interest perspective [10].

Blockchain is a distributed ledger technology that is transparent and immutable, and thus it can facilitate the creation, distribution, and sharing of trustless data transactions between individual users, corporations, and the government infrastructure. With the emerging technologies, such as 5G, IoT, cloud computing, Artificial Intelligence (AI), and big data, secure and efficient data storage and sharing among multiple service providers are becoming increasingly important. Different with the traditional certificate-based systems, the blockchain system can maintain users' data privacy by establishing a peer-to-peer (P2P) encrypted connection without requiring certification authorities (CA) to be involved. Since these

technologies can provide increased system reliability, system capability, and crucial evidence for forensics, they can extend existing systems' capabilities and thus improve a variety of public services such as in-vehicle traffic accidents and incident warning systems [18].

4.1. Case Studies of Data Sharing Policies in Autonomous Vehicle Industry

I. INTRODUCTION The keywords in the introduction express an effort to channel the automotive results of their hard work, resources, details and hard-gained knowledge in-house. The accepted common norms: prioritized scalability, lean iterations and agile innovation, to the retained culture; domestic building of new abilities to re-grasp and maintain the dedicated complexity inherent in the domain-specific profile businesses, global academy with quantum technology deep dives and connected mobility as a service. The System triggers at the research-university such applications. Not in the least for obtaining, gathering, evaluating, querying and sharing: close Circulation: the entire production line, with international commitment. We will examine the available "the potential of high-skilled workforces at a practical level, not in an idealized way; our aim is to learn how well the smart networking of the existing competences; catch and stop this ability, and build a networked product capability." This grandiose statement by Willy S. (Audi Volkswagen) should not be misunderstood. An academic world only finds its existential niche – such that at the University every factual or conceptual abstract knowledge learns to be managed and formulated – in the time of renaissance of engineering-the-man-man way of thinking and deciding. No, the branch-oriented economies are the first to need an(other) mind, but, in so doing, the social order does not change until a new technology enters the economic sphere of ownership. (Confidential agreements, all kinds of NDAs and conventional business models) will be completed when the turbo-capitalism tail reaches the zero class velocity stop without stalling the (mass) occupied Autonomous Mobility Elephant however, only participatory and the secure exchange of ethically consensual use of knowledge power will be able to further develop our society. However, the qualitative and quantitative demand for information-liberation and articles is constantly growing. The respectful and therefore complementary and standardizing responsibility of large, experimentally chance-proofed public and private service responsibility is very development driven. However, it must be emphasized once again that application, advocacy and development work must always match the mediums geomorphic and society-specific situation awareness. Only in this way do we avoid the adverse effects of special contributions, careful mimicry treatment, and misguiding one alone

care. The aim is not by any means to test whether the classical-type company or the now-emerging platform-based economy is now the better! This letter would like to point out that the techno-balance between these dipoles may be missing, but restitution for the excessive autonomy of identical interests is lacking. This corrective inherent in the relationship between them is situated in the area of the crowd from which the development of synergies is derived that are truly proportional to both. (Author name redacted) reached out and reassured me that that is why he came up with the topic and this was my luck to have been involved in the special research programme. If we go on as before, the upcoming new technologies will not interrogate and after-disqualify us minimal (e.g. big n). At least now things have become commonplace: without content digitization project, without OPC UA companions, without the Sustainable development Concept 2.0 some hybrid progress; our science and our engineering will only do what the "established" precursors will lean towards most easily, quickly and cheaply. To do to them also is to know the article is not at all an activity-limitation, as we already have the knowledge, acquisition and communication methods and the matter-dependent habits and engagement that need to be more our own: product-value, complementary transformation dynamics and legislative level parity studies. Data sharing policies are not more than (digital) workplace accident and healthy ecosystems or payment information encumbrances postulate nearly par information fuel Full variety.

Abstract—The revolutionary changes triggered by the volatility, uncertainty, complexity, and ambiguity of the markets created by the multiple waves of technological transformation continuously swung the managers' focus from automotive products and their physical sales distribution to mobility solutions and related digital transactions. Consequently, established Original Equipment Manufacturers (OEMs) are now not only fighting for maintaining or extending their leading market share in the competition with each other but also for getting ahead of the new and agile mobility 4.0 start-ups and platform providers. Data sharing policies and token-exchange systems among the valuable stakeholders of this ecosystem are being considered as the key enablers that have the potential to dynamically skill the sharing shift from traditional walking-around data to data in motion, at rest, and knowledge, from centralized systems to edge and decentralized environments, from unilateral relationships to mutual and multi-stakeholder transactions and from physical duty-fulfilment to cognitive service experience. To understand the role of data sharing policies and related user-centric value propositions, we chose a two-step empirical research methodology. Based on a

structured scanning of the webpages, we identified twelve data-sharing use cases at Audi and Mercedes Benz. We analyzed the functions and features of the overall distributed key register and market regulation functions in the autonomous blockchain system based on which our application related functionalities would grow. Lastly, we obtained insights and conclusions to spur further research.

In this community-centric research article, we aim to discuss the necessity, development, and jobs-to-be-done (JTBD) of data sharing policies in AB4 companies by carrying out a case study with two globally leading car manufacturers Audi and Mercedes Benz. We identify multiple use cases, policies under construction, and customer-centric value propositions of data sharing policies and tokens in the context of a blockchain-based AB4 knowledge exchange change platform. We instrument a research model based on the JTBD theory and our findings support that emerging privacy-enhancing technologies (PETs) like blockchain have the potential to effectively target user-centric needs, values, and goals of car manufacturers and AB4 customers with respect to data sharing.

5. Designing Privacy-Aware Data Sharing Policies

The proposed problem can contribute towards a brand-new methodology in improving privacy of differentially private, multi-party, privacy-aware collaborative data analysis by spatial and temporal properties of the contributions.Automated learning algorithms and associated computer efforts have been perceived as synergistic ways to resolve the existing privacy challenges. Two mechanisms are considered. Differential privacy as a strong privacy notion wherein an adversary has restricted power of querying the learner probabilistic queries are extracted and communicated to the adversary about the learner's learned concept [6]. By Privacy association Attack Model the practice of assigning a private attribute into an unlabeled cluster, and then exploit the Bayesian clustering algorithms from the priors to learn the private attribute is identified as a threat against multiview learning. A three-level privacy model is defined. Privacy-association phase: an adversarial AV-Physicists cluster, which exploits a semi-supervised learning algorithm to establish the associations of the noisy sensors and the physical skill measurements of autonomous vehicles for hypothesis generation. Differential privacy association phase: a Bayesian attack generation when a non-parametric Bayesian method is used to choose the optimal budget to query the differentially-privatized sensor data + physical skill measurements at each iteration. Privacy-association model:

Markov chain-based Bayesian privacy association model reports the clusters that contain the target vehicle's data at optimal iterations. The differential privacy association linkable association defense model is used to thwart all the privacy associations with the target vehicle autonomously.

Trusted autonomous vehicles (AV) need to share some of their data to maximize their collaboration potential. However, data sharing imposes an underlying threat to AV passengers' safety and privacy. Privacy-association attack models are proposed, which is fundamental to define privacy-preserving learning problems that involve multiple data providers, such as independent learning, both parties contribute information to a shared model, as well as a privacy-preserving model. A performance trade-off is evaluated and it portrays a widespread privacy leak when an AV is adopted by well-protected AV in the first-tier stage when colluded in the latter-tier.

5.1. Key Considerations and Principles

Privacy-Preferences and Data representation are a proprietary context that is usually different from transportation data. Releasing raw data will lead to excessive information outsourcing which should be held in a private repository or accessed on client-owned servers containing scalable data structures. According to participative consent dynamics, when computing partner information, a mediator should leverage confidential data verification and updating safety when requesting or using data it collects between sharing alliance participants. [1] Shared-Data should be highly modular, allowing those in the sharing alliance to exchange granular pieces regarding themselves and their information. Non-disclosure incorrectly occurred around breaks, sectors, and arrangements that can be involved in dynamic factors and logistics represented pieces, both in logistics and security methods calculated in a number of auto compositions. Privacy should be modulated in the disability company where the mediator has a piece of the data regarding the fleet. RainbowsInTheWorld Model service, the motivation for Cartopia epiCotch, have an invariant component regarding partnerships or a design shared color data safety property increasing the defect occurrence for finding solutions.

In addition to producing truly dynamic and secure methods of consent, it is important that autonomous vehicle (AV) consortia/ collaborations appropriately control and integrate the disaggregated data from the AVs and corresponding commercial fleets that move, aggregate,

and process that data. This includes tracking, claiming, and protecting the privacy of data for individual passengers (and optionally for drivers) in a subset of sharing alliance models, the privacy of operational data for the variety of participants in many cases, as well as the privacy of business data when managing business models and related strategies within the alliance. To see the need to protect passengers' privacy, we focus on a specific type of sharing alliance: a privacy-preserving pooling alliance system. In this system, each member company interacts with a common mediator, which matches the passengers 'requests for rides to the vehicles participating in the shared rides. Privacy is especially important in these alliance systems when matching between these vehicles and passenger requests depends on the physical position of both product service providers or clients due to incremental differences in pricing and purchases for these matching.

5.2. Technical Solutions for Privacy-Preserving Data Sharing

We consider information-theoretically secure pseudonyms based on physical characteristics of the car with the appropriate costs, generation, distribution and management of such physical pseudonyms in the autonomous car. By making use of the pseudonyms we fulfil the needs of the data producer to preserve data privacy, whereas the data consumer shall be able to trust that the data is really provided by an authentic car. The dependability and correct use of the pseudonym must be ensured by a trustworthy device inside the car. Strict data customizability together with the possibility to change services lived in the car require feasibility and practicability of applied pseudonym-switching constraints. Incoming bookings by different insurance companies can lead to loosely coupled switches enforceable to run parallel sessions concurrently. Furthermore, incoming demands by travelling service and entertainment applications may necessitate joint pseudonym usages, besides private ones. Reflecting on these conditions, it can be concluded that the pseudonym juggling process must be realized dynamically to ensure both, the Structural Alignment and Structural Ambidexterity of the environment.

Besides privacy-preserving authentication, an IoT-based authentication protocol based on symmetric encryption mechanisms improves the authentication process to ensure comprehensive security for applied standardized signal lights and warning signals. The mobility offered by the concept of service-oriented IN based on cloud and sensor technologies for the realization of collaboration between autonomous vehicles is realized through the

authentication and a security measure framework. The authentication of the services is realized using pseudonyms based on the concept of privacy-preserving location proofs, which guarantee the anonymity of the collaborating vehicles. In this regard, mutual authentication by exchanging the digital signatures with the pseudonym of the vehicle is implemented. The security measure protocol is utilized to ensure the secure communication between vehicles and the service providers.

Despite mandatory data anonymization requirements by European law, insurance companies are currently requesting access to personalized data when collaborating with car manufacturers. Moreover, great financial interest of the insurance companies leads to illegal and unauthorized access to such data. This data might include personally identifiable information, telemetry data capturing driving patterns, and context-related data about the driving environment. [19]In order to prevent unauthorized access to personalized data, a fine-granular and dynamic access mechanism is introduced which allows each user to define, which secondary systems of the car are allowed to process data and under which circumstances. When applying an IoT-based access control protocol, we have to acknowledge that identity-based data access needs identity authentication and thus reveals personal information. To address this issue, privacy-preserving authentication mechanisms have been proposed in the related literature. Bia et al. overviewed both proposed symmetric-key-based and public-key-based privacy-preserving authentication protocol, and they systematically evaluated the existing proposals and identified their vulnerabilities. It can be concluded that due to the performance overhead and device constraints, identity authentication of car and insurance companies via pre-shared key exchange requires more advanced protocols. The use of asymmetric authentication mechanisms seemsmore feasible for resource-constrained IoT devices for identity-based data access. Dynamic read access of cars and insurance companies to the personalized data is possible due to the fact that the actual policy holder can authenticate himself without revealing his identity to the corresponding smart system. Furthermore, the car is differentiated from others through a revocable privacy-preserving location proof which prevents targeted anonymity setting an individual car apart from other participating cars. The generated discrete timeslot is used as an identifier for the communication partner in the context of a privacy-preserving authentication.

6. Evaluation of Privacy-Aware Data Sharing Policies

In the context of autonomous vehicles (AVs), a vehicle hailing service could learn, among other things, spatio- temporal travel behavior, driver availability, and key property-based attributes shared by cooperative vehicles. Following the traffic model approach by Foschini and Rowe, we used a Mace-Mobility Context Aware Perfect Mobility model to simulate a simple and reliable mobility pattern.Thirdly, a withdrawal system without data erasure of geospatial and trajectory data when time and travel history are unknown over a limited billing time frame is a sustainability issue. If someone decides to join the system, then the membership start date can be known, because all transactions are stored to ensure data integrity.

[6] In this section evaluates the proposed data aggregation approach. It considers privacy preservation, communication overheads, and round processing times. Metrics to evaluate the performance of the VGI manager are defined in, considering the amount by which the privacy preservation technique makes the sensor data inaccurate for the purpose of data sharing. Each application selects one of the privacy-related attributes and one solution for privacy level targets, by specifying privacy property (i.e., User, Data, Query, and Disclosure-k) and Opt-K, w.r.t. the state-of-the-art solution based on the space, that suits the services for the given privacy target in terms of computational complexities and data dimension scalability. Thereafter, the chosen privacy property of each application class is checked against the collected sensitive and non-sensitive data to form the privacy-preserving function.[20] The presented work contributes both in terms of a novel thermometer design for sharing temperature readings and the identification of privacy issues associated with in-car HVE. Although not all sensitive information can be removed, the HVE has a model that also includes commands and inferred future locations of drivers. If the SSL connection is compromised and under attack by an adversary, which has taken over the model server and cannot be detected (as the model server is most probably the point of trust), this issue could be mitigated.

6.1. Metrics for Assessing Privacy Protection

To this end, the alliance system supports the following essential modules: - The company configures a view-based mediator, which accepts plausible queries from passengers and then responds with appropriate results. The views defining a mediator are periodically computed and uploaded to the companies. - Each company controls its own view-based materialized

view which is used by the mediator to produce approximate answers to plausible queries. - A company can control how its new vehicle position data is input into the materialized view. This includes the suspected position area with respect to the precision of the coordinates and the frequency of data updates. - A proxy stands between a passenger's interface app and the mediator to hold the hidden-object protocol and to allow the company to control the precision of the given data points.

Ride-sharing services such as Uber and Lyft have disrupted the traditional taxi industry by leveraging the power of digital technologies to connect passengers with drivers in real-time. In decentralized ride-sharing systems, users/vehicles and ride-sharing company are mutually distrustful. Thus, to ensure the privacy of passengers and drivers, the precise locations of vehicles must remain hidden from the company, while at the same time ensuring that passengers are matched with appropriate drivers [1]. This can be achieved if allowed to be accomplished by integrated data of approximate areas of vehicles.

6.2. Case Studies of Policy Effectiveness

In this paper, considering multiple types of data being stored in the CDAVs, a potential proposition is to utilize Blockchain for data supply chain management in CDAVs, especially for the sharing of real-time data to assist the collaboration behaviors of CDAVs. Serving as a world model of cognitive autonomous vehicles, decentralized agents are capable of making sophisticated coordination under limited data processing constraint. Sensitivity of the energy consumption performance and communication overhead of the case studies of data-co-driving strategy and data-energy trading have been quantified to evaluate the effectiveness of the privacy-aware data sharing policies. The effectiveness of such mechanisms will be illustrated via four real-world case studies: privacy impact of vehicle location sharing, privacy impact of driving behavior data sharing, privacy impact of environment image database service and the trade-off between privacy preservation and the level of autonomous vehicle control collaboration [15].

Many smart urban cities have unveiled their ambitions to develop autonomous vehicles with self-driving and Internet access capabilities. In a such smart city, it is possible for individual vehicle owners to share their real-time data with autonomous vehicles and cloud servers to assist the optimal operation of autonomous vehicles. In this paper, we will be presenting the privacy impacts, requirements and protection mechanisms for the sharing of real-time data

by individual vehicle owners [2]. Four case studies have been conducted to evaluate the impact of data privacy-aware sharing policies on the collaboration capability of energy sharing autonomous vehicles in a micro grid environment and a co-driving strategy of two autonomous vehicles in a connected traffic environment. Furthermore, it is discussed that the data consumer vehicles can utilize homomorphic encryption measures to construct digital twins of the data provider vehicles for EV maintenance and traffic control applications and for intelligent navigation decisions in query-based connected traffic environment and vehicular ad hoc network environments, respectively using the proposed policies.

7. Challenges and Future Directions

Switching focus from the user to the system, i.e., V2V and V2X, a natural protection approach would be to adopt a central system, that could monitor the system state (hence effectively any privacy breach) and take measures (e.g., intervention, prevention, consequent fines) when necessary. Therefore nowadays, encouraging data minimization is of utmost importance. Similar to the system, even for the user, a central approach (e.g., a personal mitigation mechanism, automatically guaranteeing privacy) could be the simplest solution, but our approach does not force the user to rely on it. In accordance with the principles of the Notice-and-Consent model, the user can explicitly give the consent/deny sharing of her data (an approach which is perfected also with informed consent) and, if non-cooperativeness is checked and anonymity is compromised, mitigation measures are applied ad-hoc to compensate (at software side) for the anonymization insufficiency for the specific environment [21].

According to [22] social, environmental and transportation-related trends, in particular the age and financial income distribution of the population, urbanization, congestion and pollution, automation and digitalization, safety and the adoption of shared and electric vehicles also played a key role in the analysis and conclusions of the Conceptual Autonomous Vehicle (CAV) Data Protection Impact Assessment (DPIA).

7.1. Emerging Technologies and Their Impact on Data Sharing Policies

However, only a few systems and contexts are covered in the literature in terms of anonymous data sharing policies and related protocols and architectures for data sharing within complex and heterogeneous processing systems [2]. In our previous works, we investigate emerging

technologies and architectural-level developments that drive different ways of data dissemination for data sharing systems emphasizing on autonomous vehicles, smart transportation systems and vehicle data sharing architectures in general. Focus of the presented study is the requirements and their reflection on the design patterns of IoT and Vehicle data sharing system, including privacy preserving data release, by one important aspect in the literature, namely, emerging technologies and processes such as big data, data lakes, Digital Twins and related software and protocols.

Over the years, data sharing for Internet of Things (IoT) applications has transformed from regular file transfers to a real-time data sharing model and a countless number of data is generated through online social life, work and education [14]. Regardless of the initial contribution of data/internet usage, data sharing has become the central stone of our moving lively lives and the primary force for creating real-time solutions. Having an enormous competition on most of the domains, it has been crucial employing data to shift the competition towards a real value proposition. In this respect, artificial intelligence, edge computing, digital twins, robotics and data lakes have been leveraged to deliver real value and enable efficient and smart living [23]. Additionally, the main two reasons why users are not willing to share data have been either incomprehensive circumstances or plain data privacy violation. Still, with the use of abnormal artificial intelligence and machine learning based privacy enabling, data sharing is possible without sacrificing privacy.

8. Conclusion and Recommendations

Such functionalities are important in a plethora of traffic data scenarios where information about vehicles location is released and shared by a non-negligible number r of companies despite the possibility of companies revealing useful information about their internal structure. The data sharing architecture leveraged by VESPA, is a double-edged sword. While creating cooperation potential not spoiling position privacy becomes possible, having many players on the scene might damage view privacy via communication with endorser/other non-local mediators. This paper has two very strong assumptions which are reasonable if alliance is within confined boundaries but not to be relied upon as the only conditions for valid applications. Enhancements exploiting increased awareness of communication cost, redundancy and non-split strategies remain as future work.

Following our high-level architecture, we presented an in-depth analysis of selected key modules including dynamic revocation, precise location privacy through fine-grained spatial grid updates and fair division of the expenses involved in incentivization of data expose for better requested answer fidelity. We perform both a toy example and a proof-of-concept performance evaluation of the general viability and scalability of our approach. Both our results in Section 3 as well as the significantly recent related work underlined that privacy-aware data sharing has high practical relevance in the context of autonomous vehicles and thus that our work is of high practical relevance and contributes fundamental insights for this domain1. Moreover, the complexity and multi-stakeholder nature of data privacy matching the needs of companies, customers and tax/privacy authorities is a non-trivial one.(6) Emp' that legal regulations on privacy that have been in place for a long time still struggle to keep pace with the rapid technical advancements, especially in the domain of transportation.(3)[24] Inspired by current privacy-diminishing practices and infrastructures, we argue that a privacy-preserving ride-sharing alliance system is essential. We then detail an example instantiation of this novel approach: via a privacy-preserving data sharing architecture where different ride-sharing companies participate in a common alliance for situations where no trust or very low initial trust exists between them and for this reason an intermediary mediator has to guarantee alliance consistency. The companies communicate through intermediaries without knowing of each other's' structure. We propose a system that enables each company to easily describe privacy policies and realize data upload tgriprg and update strategies, while allowing mediators to run updates on locally stored data without needing exhaustive knowledge about data held by other mediators. We supply systemyfix for privacy-enabled data sharing policies which control abstract spatial grids through which users spot their locations and viewsets of vehicles moving through a region in some given time intervals along specific trajectories, leaving view cells at arbitrary speeds.

[1] In this paper, we introduced the problem of privacy-aware data sharing policies in autonomous vehicle collaborations in non-cooperative environments. We emphasized that control over the metadata exposed by participants is an essential problem to cater for in the data sharing process. We proposed a multi-vendor framework as an example for such non-cooperative data sharing between participants with potentially conflicting interests. Our framework includes settings such as data access limiting, incentivization through tracking revocation and fine grained queries on privately held data.

References:

1. [1] Y. Asano, S. Hidaka, Z. Hu, Y. Ishihara et al., "A View-based Programmable Architecture for Controlling and Integrating Decentralized Data," 2018. [PDF]
2. [2] C. Xie, Z. Cao, Y. Long, D. Yang et al., "Privacy of Autonomous Vehicles: Risks, Protection Methods, and Future Directions," 2022. [PDF]
3. [3] M. Quinlan, J. Zhao, and A. Simpson, "Connected Vehicles: A Privacy Analysis," 2022. [PDF]
4. [4] A. M. Elbir, G. Gurbilek, B. Soner, A. K. Papazafeiropoulos et al., "Vehicular networks for combating a worldwide pandemic: Preventing the spread of COVID-19," 2022. ncbi.nlm.nih.gov
5. [5] S. Hu, Z. Fang, Y. Deng, X. Chen et al., "Collaborative Perception for Connected and Autonomous Driving: Challenges, Possible Solutions and Opportunities," 2024. [PDF]
6. [6] Y. Duan, J. Liu, W. Jin, and X. Peng, "Characterizing Differentially-Private Techniques in the Era of Internet-of-Vehicles," 2022. [PDF]
7. Tatineni, Sumanth. "Federated Learning for Privacy-Preserving Data Analysis: Applications and Challenges." *International Journal of Computer Engineering and Technology* 9.6 (2018).
8. Vemoori, V. "Towards Secure and Trustworthy Autonomous Vehicles: Leveraging Distributed Ledger Technology for Secure Communication and Exploring Explainable Artificial Intelligence for Robust Decision-Making and Comprehensive Testing". *Journal of Science & Technology*, vol. 1, no. 1, Nov. 2020, pp. 130-7, https://thesciencebrigade.com/jst/article/view/224.
9. Mahammad Shaik, et al. "Envisioning Secure and Scalable Network Access Control: A Framework for Mitigating Device Heterogeneity and Network Complexity in Large-Scale Internet-of-Things (IoT) Deployments". Distributed Learning and Broad Applications in Scientific Research, vol. 3, June 2017, pp. 1-24, https://dlabi.org/index.php/journal/article/view/1.
10. [10] F. Berman, E. Cabrera, A. Jebari, and W. Marrakchi, "The impact universe—a framework for prioritizing the public interest in the Internet of Things," 2022. ncbi.nlm.nih.gov

11. [11] F. Knoefel, B. Wallace, R. Goubran, I. Sabra et al., "Semi-Autonomous Vehicles as a Cognitive Assistive Device for Older Adults," 2019. ncbi.nlm.nih.gov
12. [12] Z. Gao, T. Yu, T. Sun, and H. Zhao, "Data Filtering Method for Intelligent Vehicle Shared Autonomy Based on a Dynamic Time Warping Algorithm," 2022. ncbi.nlm.nih.gov
13. [13] M. Ryan, "The Future of Transportation: Ethical, Legal, Social and Economic Impacts of Self-driving Vehicles in the Year 2025," 2019. ncbi.nlm.nih.gov
14. [14] S. A. Abdel Hakeem, H. H. Hussein, and H. W. Kim, "Security Requirements and Challenges of 6G Technologies and Applications," 2022. ncbi.nlm.nih.gov
15. [15] Y. Guan, H. Liao, Z. Li, G. Zhang et al., "World Models for Autonomous Driving: An Initial Survey," 2024. [PDF]
16. [16] V. Kumar Kukkala, S. Vignesh Thiruloga, and S. Pasricha, "Roadmap for Cybersecurity in Autonomous Vehicles," 2022. [PDF]
17. [17] A. Acharya, "Are We Ready for Driver-less Vehicles? Security vs. Privacy- A Social Perspective," 2014. [PDF]
18. [18] G. Abdelkader, K. Elgazzar, and A. Khamis, "Connected Vehicles: Technology Review, State of the Art, Challenges and Opportunities," 2021. ncbi.nlm.nih.gov
19. [19] M. Ul Hassan, M. Husain Rehmani, and J. Chen, "Differential Privacy Techniques for Cyber Physical Systems: A Survey," 2018. [PDF]
20. [20] S. Kumar Reddy Manne, S. Zhu, S. Ostadabbas, and M. Wan, "Automatic Infant Respiration Estimation from Video: A Deep Flow-based Algorithm and a Novel Public Benchmark," 2023. [PDF]
21. [21] X. Sun, F. Richard Yu, P. Zhang, W. Xie et al., "A Survey on Secure Computation Based on Homomorphic Encryption in Vehicular Ad Hoc Networks," 2020. ncbi.nlm.nih.gov
22. [22] H. Si Min Lim and A. Taeihagh, "Autonomous Vehicles for Smart and Sustainable Cities: An In-Depth Exploration of Privacy and Cybersecurity Implications," 2018. [PDF]
23. [23] N. Jacobs, S. Brewer, P. J. Craigon, J. Frey et al., "Considering the ethical implications of digital collaboration in the Food Sector," 2021. ncbi.nlm.nih.gov
24. [24] R. Kamikubo, K. Lee, and H. Kacorri, "Contributing to Accessibility Datasets: Reflections on Sharing Study Data by Blind People," 2023. ncbi.nlm.nih.gov