Privacy-Preserving Machine Learning Models for Autonomous Vehicle Data Analysis

By Dr. Akiko Yoshikawa

Associate Professor of Mechanical Engineering, Tokyo Institute of Technology, Japan

1. Introduction

The ability to motivate secure communication protocols that maintain both data privacy and training model owner safety has drawn a lot of attention to PPML design [1]. However, this area is relatively new, and most of the work is centered around supervised learning, where the server can easily identify each data point. In cooperative learning, less attention is given to privacy protection, but the cooperation model can potentially exploit the privacy requirements of the various players involved. This fact becomes more important when we combine the standard cooperative learning model with a setup with several possible sources of heterogeneity between the data of the various devices. This has led to research directions that are often considered in isolation from each other. However, due to the fast-paced nature of these technologies, the reality is that these aspects are likely to be influential in combined form during the next-generation technologies.

Autonomous vehicles (AVs) have tremendous potential to change future commuting and transportation [2]. Cars possess the ability to utilize sensor data to anticipate and mitigate traffic accidents, driver errors and poor road conditions. But for these tasks to be carried out effectively, the AVs must be equipped with robust learning algorithms to interpret sensor data. However, these algorithms are also put at risk because of privacy concerns. People are more wary of sharing personal data now than they were a few years ago. Research has shown that people are more accepting of partial data sharing concepts than full data sharing.

1.1. Background and Motivation

Machine learning has been widely used in autonomous vehicles (AVs), both for perception and control, which require a large amount of training data. However, part of the training data used in these robotics tasks are collected during remotely supervised driving or simulations

of the human-controlled driving environment [3]. A lack of diversity in the navigation and control data, combined with inconsistent handling of "low-stakes" decisions in the teleoperators and simulators, often results in poor performance of the machine learning models for AVs. To address this limitation, machine learning models can be trained using data collected from AVs, with data annotated remotely by expert human drivers to increase the diversity and performance of these scaling. Although such a setup has advantages, in that a large volume of vehicle data can be used without bogging down the calibration, it may come with the loss of privacy, given the sensitive nature of the sensor data, as well as the risks associated with the probability of remote access to vehicle systems [2]. In this chapter, we present privacy risks in driver conduct data and the literature on privacy-preserving supervised learning models using differential privacy. In particular, we survey literature on privacy-protecting algorithms for AVs, stress the use of data abstraction in designing privacy-preserving AVs, and present challenges encountered in modern systems that continue to need the development of error and security hub projects.

1.2. Research Objectives

Large datasets of real-world sensor data are essential for the development of data-driven autonomous driving systems [3] which are necessary for the training of machine learning models. However, the collection, storage, and sharing of large datasets have been raised as privacy concerns. Federated learning provides a viable solution for the autonomous vehicle data collection and sharing issues since it allows for decentralized learning on distributed datasets [4]. These systems enable direct access to sensors and computational units on the vehicle and processing data data destroyed by sensors in real time. By using the computational resources in the vehicle, the loss between the onboard network and the base station is significantly reduced. However, the rapid development of communication technologies, the data on the vehicle can be collected to the base station in real time through the data link, and centralized learning can be used to continuously update the data. In addition, in this framework, although data is transferred only asynchronously to the source centers, the target centers synchronize the data transmission to the central server according to the components less than the expected transmission time. In this work, the goal is to combine privacy-based machine learning and the federated architecture for continuous learning of vehicle-based sensory data. In order to be able to create a comprehensive model and not have to rely on individual sensor data, we aggregate different sensor data into a single, neural data

model. In our application, we consider data collected from a single engine as used in the more experimental part, Airlines use this model for basic modeling, and to take into account the specific scenarios and specific privacy requirements of each individual stage, our car model arrives with additional sensor data, including all imaging and GPS [5].

2. Autonomous Vehicles and Data Collection

With the high-speed development of connected vehicles and the wide availability of vehicular datasets, model training is the most crucial step to provide effective navigation results with autonomous vehicles. Economical security, individual privacy, and storage requirements need to be considered simultaneously during data collection, storage, transmission, and management before model training. The study on data privacy in the autonomous vehicle and D2D communication privacy-preserving is still very limited [6]. Moreover, practical challenges for smart cities lie in connecting insights from data to action, with data analysis being a necessary but insufficient step for data-driven decision-making. After all, actionability refers to a range of operational benefits obtained by assigning suitable actions to data analysis results. In addition, for reliable navigation solutions in safety-critical autonomous vehicle scenarios, strong generalizability on the functionality levels of data analytics and model predictions are essential qualities [7].

The digitalization of transportation systems and the evolving technology landscape are creating opportunities for autonomous and connected vehicles. These types of vehicles collect a large amount of sensor data from various sources. This data can be used to gain new insights and improve user experiences. However, it is important to ensure responsible data handling while providing recommendations and solutions based on sensor data. Here, privacy and security threats, along with the ethical concerns that come with gathering and utilizing user data, need to be addressed [8].

2.1. Overview of Autonomous Vehicles

The improvement of deep neural networks implies the processing of huge amounts of sensory data. Among these applications are autonomous vehicles that must perceive complex and uncertain environments [9]. For example, a single autonomous car generates 30 TB of data every day even when it covers relatively few kilometers. To interpret these data, the car systems rely on the data recorded by a variety of sensors (e.g., LIDAR, radar, cameras, GPS

and others) and they combine the information from the sensors using deep learning models (e.g., Convolutional Neural Networks, Recurrent Neural Networks, etc.) to generate an understanding of the environment. The information used as a model also includes information from previous flows (since these models rely on recurrent models), topologically informed maps of the environment (used for self-localization), navigation system, etc. [10]. In the scope of this work, we are mostly interested in ensuring that, when analyzing data from vehicles, we can calculate meaningful quantities that ensure not only that the vehicle is able to understand the world but also that doing so is consistent with the ethical and legal requirements. In this context, the nominal interest of the driver may not always correspond to a public notion of the correct choice: even obeying the law, there is an implicit discourse that involves respecting the intentions and behaviors of the other drivers on the road. This is even more important if the vehicle needs to be able to take appropriate actions when the driver is not in the car and cannot provide direct manual intervention. Ensuring the fairness of the models is a key first step to making sense of this data inflow, in addition to which issues of security, privacy and accountability of the systems must be carefully formulated and algorithmically embedded in each design of each model in the system [8].

2.2. Types of Data Collected

The primary applications for privacy-preserving machine learning models can include safe, adapted real-time operational interventions, personalized recommenders and driver assistance, impact on the environment, environmentally conscious, reducing the number of traffic fatalities, and reducing congestion of road transportation. The encrypted technique is mainly used for data protection in the literature which can be run within the vehicle platform through software or an embedded chipset. In comparison with data encrypting processes, SMCs are better at handling various statistical calculations. Overall, machine learning prediction methods such as support vector machine (SVM), and gradient boosting retract by the privacy preserving methods are: real time intervention, infotainment systems, recommendation services, smart city, autonomous driving, personalized ADAS, connected vehicles, fuel prediction, energy drives, side channel heart, traffic jams, spatio-temporal algorithms extraction, and road traffic congestion [10].

The driving style recognition problem is essential in automated and autonomous vehicles [11]. To recognize the driving style of the driver and model driving patterns, typically, vehicular

data (data related to vehicle attributes and driver behaviors), as well as communications information (e.g., vehicle locations, destinations, and status, communications dialogues, and traffic signals), can be collected by in-vehicle cameras, GPS navigators or mobile business systems. The former data can provide exterior assessments, such as car velocity and real-time acceleration, while, the latter data can exhibit driving behavior characteristics and state intentions of the drivers. Both the data can be fed into machine learning models and analyzed, at the same time, increasing privacy fears in various countries. The volume of data collected can be very substantial and its constituent kind's privacy-sensitive. In order to ensure effective training and testing of driving style recognition models, this difficulty makes it even more severe. For privacy-sensitive data, especially in automated vehicles (AVs) and autonomous vehicles (AUs), the need is to develop privacy preservation and safety protocols. Secure Multiparty Computation (SMC) and Homomorphic Encryption (HE) are two main topics of research in this literature, which are summarized in Figure 2 [3].

3. Privacy Challenges in Autonomous Vehicle Data Analysis

European citizens' concern for privacy is explicitly stated in the European Charter of Fundamental Rights [7]. Heterogeneous data from autonomous vehicles and all related traffic data sources are expected to grant significant benefits in terms of decision making, traffic regulation, and sustainable urban development. The heterogeneity of the data imposes the need for specific methods. Even if realistic geospatial information is transformed and stored in a privacy-preserving manner, an attack might not always be prevented on real-world data. An example describes the application of PLP to autonomous vehicle data management and traffic monitoring to achieve a stronger form of privacy in autonomous vehicles' impact on road safety.

Privacy is a major source of concern in the transportation and automotive industries. In recent years, the increasing use of computer technology and the Internet of Things (IoT) have raised public concerns about how data should be managed and whether these data violate personal privacy originat [12]. Heterogeneous data from autonomous vehicles and all related traffic data sources are expected to greatly enhance decision making, traffic regulation, and urban development. Semi- and fully autonomous vehicles actually produce large amounts of data from many heterogeneous sources, such as cars and infrastructure sensors, electronic control

units, and other autonomous vehicles, as well as communication links and maps. All these data are potentially sensitive and could breach personal and public privacy.

3.1. Sensitive Information in AV Data

Especially, in think mainly of the privacy-sensitive information in AV data such as location/travel information, power consumption information, and airquality consumption information, which could affect the privacy, security, and trust of the travelers and business uses of CAVs. This is a critical issue for the optimal development and deployment of CAVs. In particular, different types of CAVs such as drones, buses, taxis, and logistics systems, have different data collection-heads, and drones carry a lot of IT. Therefore, in the analysis tools, which take into account drone location data and system consumption, also need to ensure their protection of sensitive information by using Privacy Enhancing Technologies (PETs). The analysis tools integrity and confidentiality features are particularly important for drones in industries such as utilities, agriculture, delivery, logistics, and emergency services [13].

Now we discuss the different types of users that can be associated with AV data by means of ML and AI analysis of that data. This is critical for privacy and data sharing. Currently, only the autonomy level of a vehicle is used. However, by analyzing data, more sensitive information can be inferred, which can create privacy breaches [14]. Learning techniques can create models with information that can be used to infer sensitive user behavior, locations, driving patterns, and schedules. This is undesirable in data sharing. In addition, such inference biases AI and ML models, causes representation errors, and can cause significant systemic discrimination against individuals. In addition, body information in CAV analysis that does not generate prejudice or sensitive interests about the traveler or any other business user is also strongly required because any kind of travel data collected by the devices of CAVs could contain sensitive information.

3.2. Regulatory Frameworks

Nearly every modern software stack used to augment in-vehicle functionality includes machine learning libraries. These libraries can be both vulnerable (exploitable) and collect data about user behavior that is nearly impossible to unlink from the user due to the individuating nature of clickstreams and interaction with the vehicle. More and more EDRs (event data recorders) in cars are storing information about driver behavior. Since we

acknowledge that privacy is a social concept, it is difficult to predict how norms for consent management and data collection will change in thirty years, but it is clear that machine learning models and EDRs will allow for data-driven individual privacy attacks that will fundamentally change the "state of the video." [15]. The (in)ability for machine learning models to re-identify data in the distant future due to regularity in the data and the (lack of) inductive biases of the machine learning engineered to learn upon it leads to a finding that drivers represent an erosion of data unlinkability. This not only will affect individual privacy but also could open the floodgates to low-threshold full counterfeiting. This is similar to computer security where the surface area provided by persistent attack vectors decreases the attack cost. With this kind of data, any sophisticated laymen can create "self-forging taxes," where the sophistication of the system is less reflective of vehicle security or privacy capabilities and more directly tied to the defense budget of the hosting company.

The progression and adoption of this technology are directly linked to the ability to properly define and dictate privacy standards and obligations. Currently, a very limited number of regulations exist that regulate connected and autonomous vehicles from the perspective of data privacy protection. Thus, efforts to achieve these objectives still manifest themselves primarily in nonbinding recommendations, documents, and guidelines (e.g., the guidelines recently endorsed by the European Union) [16]. In North America, California introduced new privacy standards, the California Consumer Privacy Act (CCPA). A privacy notice, similar to that we have in the field of the Internet and telecommunication (telemedia), will have to be displayed within the car. In most cases, the starting point of the European Union (which is the leading institution in terms of privacy protection) lacks sufficient protection of users' interests, mainly in the contexts of so-called transparency and proportionality of collected data as well as consent of the interested party [17].

4. Privacy-Preserving Techniques in Machine Learning

With FL, the training model is trained over the data at different users, and finally, a global model is obtained by skillful aggregation. The trained data remains only on the smartphone, where the client trains the model, and the smartphone only shares the gradients over the network, which is much lighter than FL. Since our attack model aims to copy the dataset to track the data with the model train a target client, potentially for misclassification to cause malicious outcomes, we only focused on preserving data privacy through P2CML protocols

when describing how it should work in the context of self-driving cars condition data under training natural automated driving tasks. Hence, we considered the membership fraud attack (MFA) in the P2Falcon scenario in our paper. We used a road-tracking model capable of adapting to different road types and abnormal freezing temperatures as a transferable system, and used this road-tracking model to present a concrete threat to trackable privacy in the federated learning of robot car environmental data obtained in NADS-1.

Training machine learning models often requires large amounts of distributed data, raising privacy concerns. To address this, privacy-preserving machine learning technologies are necessary. Researchers have developed methods such as homomorphic encryption, differential privacy, and secure aggregation. These aim to prevent data exposure and information leakage, ultimately enabling data sharing for improved model building [18]. As autonomous vehicles generate more and more data, adaptive and energy-efficient privacy-preserving machine learning models are a must. In this regard, Norouzzadeh and Song note secure multi-party computation (SMC) as a possible privacy-preserving mechanism to allow authorized parties to jointly analyze their data without leaking the raw data, while FL has been suggested for privacy-preserving collaborative machine learning (P2CML) which is data-centric and privacy-preserving [19].

4.1. Differential Privacy

Although unsupervised and supervised learning have been adopted unceasingly, their primary deterrent is the severe data privacy issue. To illustrate, the datasets generated by an autonomous driven car contain minute information corresponding to all the sensors. Such sensor data were sent to a server, possibly exploiting cloud computing. According to a survey in 2013, the greater consciousness of people about the privacy risks threatens the success of the electric vehicle. Subsequently, for the case of the electric vehicle [20], the users might agree to grant his/her location for safe..ospeak services to a company; however, if as a consequence the loved ones are gone after, the user needs privacy. Further, depending on the content itself, also the Australian government has expressed concerns over critical personal information, such as the access to the data of the vehicle or the battery status of the electric vehicle. Consequently, a compromise is required between the need of private services, such as a demand forecast of the electric vehicle and the maintenance of privacy. Therefore, in some of the applications, a privacy protection of the private information is essential. This permits to

guarantee some efficient techniques, such as those for preventing and controlling fraud, for the reidentification of private services and it shall be destructed in the cases of data mining.

The massive storing and sharing of autonomous driven vehicle data is able to automate several driving-car technologies, such as predictive alerts for minimizing road linking time and strategic plans for scheduling charging processes. To cope with such trend, several companies have designed, manufactured, and installed electric or hybrid vehicles. Moreover, electric vehicle are integrating renewable energies, such as photovoltaic or wind. The environmental and economic success of the electric vehicle technologies is strictly connected with the optimization of the propulsion systems and the effectiveness of the energy management systems [10].

4.2. Homomorphic Encryption

[10] [21] Security in employing machine learning stakeholders, particularly those on the data-provider edge, and hence, multiple privacy mechanisms such as secure multiparty computation (SMPC), homomorphic en-cryption (HE), secret sharing, and differential privacy are gaining attention in many domains. However, among the wide range of privacy preservation methods addressing issues associated with machine learning applications, those that employ the noisy aggregation of model updates based on decentralized learning (copy model or federated learning) have gained wide acceptance due to their support for privacy preservation. Copy model is based on the server-client architecture where clients send their trained model weights to the server, while federated learning allows servers to reach out to the clients and update their model weights to protect a client's data. While decentralized learning methods address the privacy of training data at the data-provider edge, employing centralized methods incurs the risk of privacy breach, lightweight, resource-efficient data processing within the vehicle employing in-vehicle infrastructure, mobile phones, and cloud/virtual private servers (VPS).[22] Encryption tools are the most suited technique for achieving privacy preservation with software applications at vehicle-related infrastructure and machine learning deployment at processing engines at central controllers in vehicles. Homomorphic encryption (HE) methods, which support all possible arithmetic operations on encrypted data, have received increasing interest due to their suitability for achieving secure data inferences in real-time data analysis across connected systems. Unlike secure computation stanzas, where parties involved in computation are trustworthy data processors,

employing a server-client architecture, a client processor mainly comprising vehicle infrastructure logic and software services for managing real-time vehicle data, including data visualization, diagnostic monitoring, and autonomous control of the vehicle, and a server processor primarily comprising service-oriented architecture (SOA) as traffic management virtual machines are involved in the trading of encrypted data in edge-based Privacy-Preserving Triple-Articulated-Edge Traffic Optimization. This technique is employed to secure data at rest, the least required evaluation of security measures, and off-line analysis related to database server storage and machine learning deployment at traffic data centers at off-vehicle computing networks, including cloud, virtual private servers and standalone servers.

5. Case Studies and Applications

The performance of machine learning models and their applications often rely on high-quality data that represents accurate information about the task at hand. The problem of data pollution and data leaks, observed as a result of data collection and its subsequent analysis by machine learning models, has attracted significant research attention. In this study, following the general training, validation, and testing setups, the impact of full training data and privacy-preserving training data on DNN performance were analyzed for various network complexities. The obtained results were explained with respect to data poisoning, fast adaptation, model architecture, input dimensionality, and other possible effects [23].

The primary strength of the proposed privacy-preserving method lies in the new problem setting, where the framework is applied to protect the data collected from real-world autonomous vehicle applications for this solution. However, the application of PPML is not limited to AVs. The proposed approach can be applied to general ML applications to prevent the raw data from being released or analyzed, protecting the privacy of domain users [24].

5.1. Real-World Implementations

As the use of autonomous vehicle (AV) technology among the public continues to increase and the field grows over time, visual saliency prediction (VSP) data in autonomous flying vehicles (AFV) is a new dataset for use in privacy-preserving machine learning (PPML) models especially in flying vehicles. Then, through an analysis of the real-world safety performance of flying vehicles, the relative effectiveness of method is measured, after which

insights into various possible approaches toward both improving accuracy and preserving privacy in AV data usage is derived which can drive future research into this field. Some of them are used to protect the privacy of AVs' environment. While the other models are used to protect the privacy of AVs' status.

[3] [10] Most of the existing works in privacy-preserving machine learning (PPML) lasts for few to several years. Authors can explore recent future directions such as evaluating privacy models' robustness, and the combination of multi-part models to process privacy data. Data protection is recognized as one of the essential requirements for AI.Researchers have developed a list of risks associated with AI from an ethics, legal, and social perspective. In this chapter, we are interested in the possible AI-induced risks in privacy protection and we have decided to study two mini scenarios concerning AI-induced risks in the AV [5] data openly displayed to public safety, private firms (see Section 3.2). Given that efforts on privacy preservation have been growing in recent years, people assume a bright future for PPML in electric vehicles. When the authors do not integrate these three literature perspectives, the authors may not be able to reach a comprehensive research in this paper. "Privacy Preserving Machine Learning for Autonomous Vehicle data" is not significantly investigated in Science and its ethics.

5.2. Use Cases

Privacy concerns and driver behavior provide important challenges to deploy machine-learning models (MLM) optimizing all transportation operations. © This paper introduces a novel approach based on multisensory information ensuring a new vision of individual, moving, and even dynamic driver profiles, to imagine design innovative MLM minimizing privacy risks. Indeed, these new algorithms will be trained exclusively using personalized but already anonymized surrounding data streams. We present three use cases illustrating the potential of this future personalized approach, first to enhance training dataset of MLMs to be less dependent on the driving style and the semantic of each driver's journey data [2], then to support vehicle safety assessment during the experimental phase by permanently comparing real driver and enhanced training behaviour [23], and finally to propose new personal risk factors taking into account additional contextual information transported into the vehicle, making the following of natural environment standardization easier for identifying external anomalies [25].

6. Evaluation Metrics for Privacy-Preserving Models

We then interpret the model's predictions and use SHAPLEY (SHapley Additive exPlanations) analysis to quantify the eventual influence each input signal has on the model's decision. For privacy evaluation, we provide the plain model evaluation metrics (number of independent features), the feature interactions through Clustering Index (CI), and the integrity of the saliency map by designing specific attacks (XOR-SHAPLY). Ideally, the alternate should provide the highest group privacy considering the first two metrics while making sure that the XORSHAPLY values differ significantly between the critical and noncritical groups. It utilizes both classification errors and SHAP values, measures the similarity and difference in feature transformations and model predictions for benign and adversarial attacks, respectively, and can evaluate deep perception and interpretable models [2].

Privacy-preserving model evaluation methods should measure a model's resistance to privacy breach attacks and the role model complexity plays in preserving privacy. Privacy has traditionally been measured with regard to differential privacy [26]. In EL, model privacy can be evaluated in different dimensions: how the feature extraction and aggregation design ensures more balanced privacy protection, how private signals using the root mean square or cosine similarity distance as the distance metric are assessed. Additionally, tracing the statistical and privacy preservation of federated learning aggregation can be a drawback. Taxonomy and detailed survey of the differentially private aggregation methods in multiple rounds required in federated learning are included in related work sections. However, existing approaches generally focus on measuring forward-inference privacy by assuming that adversaries can only access the output of the model. All proofs are provided for the single leader and multiple workers setting under a static worker assumption.

6.1. Accuracy and Utility Preservation

To liberate these privacy-critical environments profoundly from the potential risk, a first step is to group the collision-affected and other special vehicle sections to safety zones that cover a larger geographical area and ground where social violations of integrity can play no role. After the motion data have been grouped to safety zones, the identified driving events have to be recognized for the aim of the vehicle behavior analysis. In particular, a detailed analysis should be executed within the safety zones to support further conclusions of inferring hidden

regularities of data. For many analysis and research questions the concentration on individual vehicle behavior templates and single driving events is insufficient, thus we discuss particular methodologies to analyze drivers' macro-behavior to detect hidden patterns [2].

The analysis of vehicular big data has a growing significance for classical automotive industries, especially from the side of business intelligence and service offers. In particular, the automotive industry becomes more and more capable of gathering data from its vehicles in real time. Properly analyzed, this data can be used for the automatic diagnosis of vehicle situations and accidents [18]. Often, such data are generated in what could be called a "privacy-critical context": We detect the vehicle data as originally generated in areas of privacy concerns, because with them the positions of vehicles can be traced, and potentially the movements of individuals can be reconstructed. Such "tracked vehicles" might not be supposed for company-owned but for privately-owned and -handled, hence personally-associated movements and visits of the driver, together with all side effects implicate something really sensitive. Additionally, as the analysis might concern collisions and other major hazards, the vehicle data can also support conclusions abbout private surroundings, neigborhood and happenings [27].

6.2. Privacy Guarantees

With expressive machine learning workloads, it becomes essential to guarantee the user's privacy within the infrastructure of the cloud. Pseudorandom projections are computed from the training data and then added to the testing data before they are sent encrypted to the cloud for classification by the model [22]. Given the hamming distance between the original and reduced vectors which shows how similar the two are, it is not a constant, i.e. with the same scaled data across more than two cloud layers, the hamming distances are not exactly constant, so we transformed it from 1 of d possible values to a number from 0 to 1. This has the potential problems that the private key is shared among all users so that if the adversary gets one of these private keys, they can fully decrypt data sent from any user to that cloud layer, and the private keys are shared as plaintext.

[24] Users rely on the cloud to store large amounts of data and perform complex processing. As machine learning continues to mature, organizations are increasingly using them to extract more significant value from their data, while also making use of recent models that are continually updated with new data. In one study illustrated by [28], a security comparison

between machine learning as a service (MLaaS) offerings of Google, Microsoft, and Amazon was performed, which concluded that the monitoring mechanisms by the platforms are not enough to detect information leakage from the MLaaS system. Therefore, user privacy could be at risk in the cloud-hosted MLaaS service. To address network detection of privacy leakage, detection methods based on network counters and network APIs are compared, but their performances on encrypted computer vision and natural language models are limited due to the influence of attacked parameters.

7. Future Directions and Emerging Technologies

Furthermore, exploring the role of MINA cybersecurity analytics to secure the communication infrastructure and enable full confidentiality and correctness with ensuring trust in the experience based datasets is also a very significant open research issue. Develop a rigorous testing and evaluation methodology required to ensure the compatibility of privacy-preserving systems with drivers' privacy needs and the data protection standards. In this context, personalised content-adaptive generation of adverse scenarios for diverse autonomy AmSHOW = {SHOW1 ,SHOW2, . . . , SHOWN} against SYNTHMON represents a two-stage learning process, one for understand fair MINA worker pays-in fairness scenario. Non-adversarial synthetic frameworks, for efficient labour cost floor mechanisms scenario, and one for adversarial strategic employee hoarding of synthetic workers and strategic design of adversarial employees in turn requires efficient tactics against all the former strategies with showcase adversarial input set A*. In future, other various unlawful representations such as feasibility, promising easy-insolvent-admissible feasible patterns may be explored.

[29] [8]One of the key future research directions involves the design of privacy-enhanced autonomous vehicle technologies and services that satisfy the needs of all the stakeholders in this space including drivers, on-demand e-hail Taxicab (eTaxi) services, vehicle manufacturers and urban delivery fleets using standardized privacy-preserving technologies with explainable, trustworthy and responsible AI which provide flexible trade-offs between privacy, model quality and actionable information. Quantified Self (QS) has been used in a variety of vehicle related research and product domains, such as driver activity recognition, driving style analysis and energy consumption. However, privacy-friendly analysis of complex time series (CTS) data such as the ones found in vehicles still poses a major challenge. This also provides similar challenges for negative result submission, and reproducibility

evaluation concerns and also on the collaborative efforts where industry and academia can collaborate confidentially and maintain data confidentiality and privacy.

7.1. Advancements in Privacy-Preserving ML

However, these models were not able to get as close to the performance of standard training models. A. Neiswanger et al. proposed to use a Generative Adversary Network (GAN) ... [29]. methodology to create synthetic data from the original dataset with no actual privacy risk. Synthetic data, generated using AI, has various applications, such as improving model explainability and supporting collaboration between companies.

Before the development of adversarial training, Federated Learning ... [30]. did represent the standard framework for privacy-preserving ML in which a global classifier is trained by multiple entities without transferring their data to each other. On the other hand, Secure Multi-Party Computation ... [31]. involves a multiparty encryption and decryption computation that allows nodes to share encrypted data without unmasking them. This technique has gained market attention as it was formalized in the protocol by F.J. Thakur et al. applied to multi-layered perceptron topology.

7.2. Potential Impact on AV Industry

In addition, secure Multi-party Computation and fully Homomorphic Encryption were utilized to train a privately supervised machine learning algorithm. Keeping the learned model private is challenging due to the availability of white-box attack methods. Though, there have been few research works coupling privacy-preserving machine learning approaches in working with autonomous vehicles. It is attractive to secure a collaboration process and protect the design updates on-board from adversaries. Data, that is available to adversaries to train and validate their competitors, leaks information about privacy relevant car owner preferences and behavior. To secure the data transmission, to validate an adversary robustness, the robustness of the corresponding system has to be proven explicitly [10]. It is important to note that it is not a data privacy issue alone but also a question of the behavior safety: Given that for self-driving vehicles models were revealed to be vulnerable to logical fallacies, they could be tricked to misread danger situations. Model summaries make it easier to find safer vehicle architectures. Moreover, advocates of black-box study.

[5]In the automotive industry, it is imperative that machine learning models are kept safe from adversarial inputs, privacy attacks, backdoors, trojan models and are successfully kept trustworthy for other safety-critical applications. Many different data types are collected by autonomous vehicles (AVs) such as camera images, ultrasonic distance measurements, and of course the AV's location and trajectory data, which are crucial data types for safety-critical functions. In addition, personal driver information can also be data that is exposed and needs a level of privacy especially in shared AVs. Moreover, it is essential to monitor the training robustness and control stability of an AV by considering possible variability in the physical model parameters and to keep the performance of an AV robust and predictable during its lifetime. A second level of infection might be due to adversarial inputs which aim to disturb driving assistances and autonomous functions. A third level of compromisability of autonomous functions can occur if adversaries can trick sensors and vehicle-internal systems into believing the car is in a certain environmental state or even acting differently to what the car perceives. Blind spots in the digital perception and decision-making-the machine learning models, are introduced depending on the training database and architecture of the models. Various data perturbing and augmentation techniques are proposed to protect sensitive data such as driver preferences, user habits, and behavior when designing and validating machine learning algorithms [8].

8. Conclusion

A PPML system has four major components: an input schema, a machine learning model, an inference process, and a evaluation system, where the input schema domain data are given to the analysis blocks. The model building stage is usually performed off-line, where the feature vectors and labels are anonymized to minimize threats to user privacy, ensuring the privacy goals of the system, and trained on anonymized data. When suitable model architectures and formulations are available, training of the machine models on anonymized traffic datasets proceeds without compromising driver privacy. After the model construction stage, such models are deployed under a V2X environment, where several vehicles and traffic infrastructures around a city are equipped with communication modules. Pre-trained models are shared with vehicles and traffic infrastructures as per the requirements, and the data analytics occur, like isolation forest algorithm acts as a feature selection process and by implementing the ensemble of such isolation forests, the extension of developed machine learning model - generalized leveraging model is designed as a part of this research. [10]

This paper addresses privacy preservation in autonomous vehicle (AV) data analysis when data analytics is conducted using machine learning (PPML4AV). This survey provides the state-of-the-art in PPML4AV, covering various perspectives including research results and challenges, potential commercial and industrial requirements, legal and ethical issues, the significance of fairness, and potential industry uptake. We kick started the discussion by discussing some of the basic concepts of privacy-preserving machine learning (PPML) and differential privacy (DP). Differential privacy (DP) provides a comprehensive framework for preserving privacy while data analytics is conducted using machine learning, and thus can be used effectively for assessing privacy preservation among autonomous vehicle analytics. We then went into details on how researchers have designed and developed autonomous vehicle analytics models that are DP-preserving.

8.1. Summary of Key Findings

Adversarial inputs: an adversary designs inputs for an ML model to get arbitrary incorrect outputs. In this section, we will explore main threats and defense mechanisms when designing AI Model for autonomous vehicles and uto sharing dataset [32]. Also, we will focus on how differential privacy can be used to handle privacy concerns. Different connected and interconnected vehicles are presented in Figure 2. For the right communication between these incar devices (e.g. human–Machine Interface (HMI), Vehicle-to-Anything (V2X) units) connected via vehicles backbone (e.g. FlexRay, CAN, MOST, or Ethernet), several multi-gateway CAN–Ethernet buses or multi-domain vehicle Specific Gateways.

Privacy is a major concern in today's Big Data World. Building an AI Model using anonymized ride-share data from e-scooters can lead to several attacking scenarios [2]. Hence, it is very crucial to design effective algorithms for not only building models that are useful, but at the same time are privacy-preserving, panduring that no fine-grained personal data is shared with a central entity or with an attacker. In doing so, we have to worry about the following threats: Direct Ascent of Anonymized Data: The attacker is viewed as an adversary who attempts to discover the individual instances of the anonymized data or to learn some trait, such as sensitive properties, about them, which is a challenging task. Model Inference: The attacker actively exploits the outputs of the model through inquiries on their training, to study the model altogether or even revert its outputs.

8.2. Implications and Recommendations for Future Research

To stay precise when privacy scenarios are a concern, federated learning provides a possible solution by effacing the need of sharing data and the trained ML model hosted at an isolated and centralized server. The reason behind isolating vehicle data across clusters is to linearly scale model training server storage spaces. It is possible for an adversary with server access to overturn the data. The less he or she knows, the less likely he or she is to harm privacy. A privacy sensitive model configuration is achieved by adopting low rank separation learning. This ensures that shared data splits are independent with shared model parameters [24]. This separation is utilized at both the cluster level and the federated learning round level with the rank of the model parameters. Shearlet matrix makes the matrix separation low rank. This can provide coordinated information external to the server [2].

Assets sensitive to privacy attacks in machine learning (ML) for autonomous vehicles include the training dataset, model parameters, and architecture. Privacy-related attacks target data owners, model owners, and consumers, with categories such as membership inference and model extraction [32]. Techniques such as differential privacy and homomorphic encryption help to protect the training dataset. In comparison, protection of the model includes sanitization of model parameters and architecture. All these techniques proceed to varying extents by trading off privacy with model efficiency, where performance accretion and privacy erosion over the dataset are adversarial. Transfer learning maintains the model's minimal performance across multiple vehicles.

References:

1. [1] S. Rass, S. König, J. Wachter, M. Egger et al., "Supervised Machine Learning with Plausible Deniability," 2021. [PDF]
2. [2] T. Hagendorff, "Linking Human And Machine Behavior: A New Approach to Evaluate Training Data Quality for Beneficial Machine Learning," 2021. ncbi.nlm.nih.gov
3. [3] C. Xie, Z. Cao, Y. Long, D. Yang et al., "Privacy of Autonomous Vehicles: Risks, Protection Methods, and Future Directions," 2022. [PDF]
4. [4] J. Xu, Y. Zhang, H. Yu, B. Lin et al., "High performance of privacy-preserving acute myocardial infarction auxiliary diagnosis based on federated learning: a multicenter retrospective study," 2022. ncbi.nlm.nih.gov

5. Tatineni, Sumanth. "Ethical Considerations in AI and Data Science: Bias, Fairness, and Accountability." *International Journal of Information Technology and Management Information Systems (IJITMIS)* 10.1 (2019): 11-21.
6. 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.
7. Shaik, Mahammad, et al. "Granular Access Control for the Perpetually Expanding Internet of Things: A Deep Dive into Implementing Role-Based Access Control (RBAC) for Enhanced Device Security and Privacy." *British Journal of Multidisciplinary and Advanced Studies* 2.2 (2018): 136-160.
8. Vemori, Vamsi. "Human-in-the-Loop Moral Decision-Making Frameworks for Situationally Aware Multi-Modal Autonomous Vehicle Networks: An Accessibility-Focused Approach." *Journal of Computational Intelligence and Robotics* 2.1 (2022): 54-87.
9. [8] I. Laña, J. J. Sanchez-Medina, E. I. Vlahogianni, and J. Del Ser, "From Data to Actions in Intelligent Transportation Systems: A Prescription of Functional Requirements for Model Actionability," 2021. ncbi.nlm.nih.gov
10. [9] J. Diego Ortega, P. Natalia Cañas, M. Nieto, O. Otaegui et al., "Challenges of Large-Scale Multi-Camera Datasets for Driver Monitoring Systems," 2022. ncbi.nlm.nih.gov
11. [10] A. Rahman Sani, M. Ul Hassan, and J. Chen, "Privacy Preserving Machine Learning for Electric Vehicles: A Survey," 2022. [PDF]
12. [11] C. Hati, G. Kumar, and N. Mahajan, "$bar{B}rightarrow D^{(ast)}tau bar{nu}$ excesses in ALRSM constrained from B, D decays and $D^{0}-bar{D}^{0}$ mixing," 2015. [PDF]
13. [12] 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
14. [13] 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. [14] M. Ul Hassan, M. Husain Rehmani, and J. Chen, "Differential Privacy Techniques for Cyber Physical Systems: A Survey," 2018. [PDF]
16. [15] B. Carsten Stahl, "Ethical Issues of AI," 2021. ncbi.nlm.nih.gov

17. [16] S. Blake, "A Simple Method for Computing Some Pseudo-Elliptic Integrals in Terms of Elementary Functions," 2020. [PDF]
18. [17] A. Acharya, "Are We Ready for Driver-less Vehicles? Security vs. Privacy- A Social Perspective," 2014. [PDF]
19. [18] F. Zheng, "Efficient Private Machine Learning by Differentiable Random Transformations," 2020. [PDF]
20. [19] E. Novikova, D. Fomichov, I. Kholod, and E. Filippov, "Analysis of Privacy-Enhancing Technologies in Open-Source Federated Learning Frameworks for Driver Activity Recognition," 2022. ncbi.nlm.nih.gov
21. [20] Z. Shen and T. Zhong, "Analysis of Application Examples of Differential Privacy in Deep Learning," 2021. ncbi.nlm.nih.gov
22. [21] A. Vizitiu, C. Ioan Niţă, A. Puiu, C. Suciu et al., "Applying Deep Neural Networks over Homomorphic Encrypted Medical Data," 2020. ncbi.nlm.nih.gov
23. [22] A. Qayyum, A. Ijaz, M. Usama, W. Iqbal et al., "Securing Machine Learning in the Cloud: A Systematic Review of Cloud Machine Learning Security," 2020. ncbi.nlm.nih.gov
24. [23] N. Rizzo, E. Sprissler, Y. Hong, and S. Goel, "Privacy Preserving Driving Style Recognition," 2015. [PDF]
25. [24] C. Zhang, "State-of-the-Art Approaches to Enhancing Privacy Preservation of Machine Learning Datasets: A Survey," 2024. [PDF]
26. [25] F. Lang and Y. Zhong, "Application of Personal Information Privacy Protection Based on Machine Learning Algorithm," 2022. ncbi.nlm.nih.gov
27. [26] F. Ezzeddine, M. Saad, O. Ayoub, D. Andreoletti et al., "Differential Privacy for Anomaly Detection: Analyzing the Trade-off Between Privacy and Explainability," 2024. [PDF]
28. [27] M. Yang, M. Ding, Y. Qu, W. Ni et al., "Privacy at a Price: Exploring its Dual Impact on AI Fairness," 2024. [PDF]
29. [28] E. De Cristofaro, "An Overview of Privacy in Machine Learning," 2020. [PDF]
30. [29] S. Fritz-Morgenthal, B. Hein, and J. Papenbrock, "Financial Risk Management and Explainable, Trustworthy, Responsible AI," 2022. ncbi.nlm.nih.gov
31. [30] E. Angulo, J. Márquez, and R. Villanueva-Polanco, "Training of Classification Models via Federated Learning and Homomorphic Encryption," 2023. ncbi.nlm.nih.gov

32. [31] D. Dhinakaran, S. M. Udhaya Sankar, D. Selvaraj, and S. Edwin Raja, "Privacy-Preserving Data in IoT-based Cloud Systems: A Comprehensive Survey with AI Integration," 2024. [PDF]
33. [32] E. Rodríguez, B. Otero, and R. Canal, "A Survey of Machine and Deep Learning Methods for Privacy Protection in the Internet of Things," 2023. ncbi.nlm.nih.gov