Privacy-Aware Machine Learning Algorithms for Autonomous Vehicle Data Analysis

By Dr. Rajesh Pandey

Professor of Computer Science, Indian Institute of Technology Guwahati (IIT Guwahati)

1. Introduction

In the smart mobility domain, AI-enabled systems are designed to enable machines to make decisions autonomously without the intervention of a human operator. One of the two most important scenarios in which AI solves problems are: (a) in the Inter-Vehicular Communications (IVC) systems, smart vehicles are designed to react directly to the environment in which they operate and (b) in the In-Car systems, smart vehicles are less autonomous than the ones in category (a) but can still perform a wide spectrum of functions. In researches, it is identified that in scenario (a), privacy should be preferentially preserved over other concerns and in scenario (b), privacy is crucial but not is equivocally relevant as in scenario (a) [1]. The aim is to enable vehicles to work in competition and cooperation with humans according to privacy laws while trading off privacy with their performance in functions required such as achieving a compromise to maximize the efficiency of traffic flows.

[2] We are in the middle of a paradigm shift from traditional analytics to data-driven, predictive, and autonomous computing that can be seen in the massive deployment of systems based on Artificial Intelligence (AI) such as smart vehicles, machine learning-based services, and decision systems in the Industry 4.0 scenario. Such a change is an opportunity for human advancement because AI-enabled systems are expected to outperform humans in most tasks. However, the AI paradigm shift creates questions about the social impact, laws, accountability and responsibility of AI-enabled systems and necessitates the need for tools and methodologies to protect the 'welldness' of society. The host of adopted solutions to protect rights, safety, and balance in society ranges from the introduction of logical, ethical elements in programming and AI systems in a formalized way to the design of secure systems with strict boundaries that do not invade the values involved.

1.1. Background and Motivation

It is important to safeguard the privacy of the data that is being collected in order to minimize the risk of data breaches and potential abuse of such data to, for instance, re-identify human drivers, steal trade secrets from commercial vehicles, or serve as adversaries in adversarial settings, where they could insert fake-data measurements as applied for cyber-physical attacks. In this context, combining privacy-sensitive data with machine learning is an important area of research which has witnessed an increased interest in recent years. In this paper, we will cover privacy-preserving data mining techniques and privacy-preserving machine learning (PPML) methods. Recent years, a need for merging privacy with data mining and machine learning is observed in different applications such as healthcare, financial applications, and social networks. Moreover, we observe an increasing application of privacy-preserving data mining techniques and PPML methods in the context of connected and (semi-) autonomous vehicles [3].

The availability of large-scale data has led to a surge of interest and an increasing number of real-world applications that rely on the development of decision-making algorithms. One domain where this is particularly relevant is intelligent transportation systems (ITSes) where autonomous vehicles may be considered as the future intelligent transportation system components. To make proper decisions, the aforementioned algorithms are typically trained upon, and make their decisions based on, large-scale datasets. Thus, the process of data collection, labeling, storage and handling in ITS is crucial for the functioning of ITS. In particular, the process of data labelling and model training can be proemia-vulnerable as it involves human intervention, and hence it is particularly sensitive to socioeconomic and human error biases. With the advent of technologies for fleet sharing, such systems generate detailed data records, e.g., including the vehicle's position and velocity, steering, throttle and braking states, and information related to the current road environment including geometrical and physical data, weather, etc [1].

1.2. Research Objectives

The second main goal of the project, besides the achievement of privacy compliance in the data analysis of autonomous vehicle data in accordance with the GDP Regulation, as established for the previous point, is the development of methodologies and tools to allow the secondary use of sensitive vehicle data for the advancement of ADAS. ADAS are responsible

for a large number of vital responsibilities in a vehicle, such as recognizing and reporting obstacles, signaling and reaction for a potential accident, lane-following, traffic monitoring, collision avoidance, to list a few [4]. Therefore, the need for privacy-aware data analysis solutions in the context of autonomous vehicles is undeniable. As established in the previous point, it is proper to exclusively study policy-aware data analysis algorithms specifically intended for the analysis of information from users of autonomous vehicles.

One of the main objectives of the proposed project involves the achievement of guidelines of the GDP Regulation with respect to user privacy, while performing data analysis of autonomous vehicle data [5]. Data collection and processing performed within a vehicle enable a better understanding of user's behavior in a multitude of real-world driving situations, making it possible to develop algorithms that can improve the next-generation of Advanced Driver Assistance Systems (ADAS). This additional data, however, also has privacy implications, as vehicle sensors record sensitive emissions and the behavior of the users, therefore it is crucial to develop privacy-aware algorithms in the field of autonomous vehicle that treat the information of the users with respect and care. Therefore, the first goal of this project is to address the above shortcomings and develop privacy-aware algorithms specifically designed for the treatment of users' data when performing data analysis on autonomous vehicle records.

1.3. Structure of the Work

Informed Control Setting Performance is evaluated by gathering data Feasibility of a new test track: Ankara which will be uplifting data delight. In the first part of this sub-section, we demonstrate the functioning of the driving action assessment algorithm developed. In total, the study involved 153 language errors in matching symptoms from 68 test subjects and sentences they read. Through the inter- detection of high-level cognitive barriers, modeling and editing will offer methods that improve the performance of reading errors classification algorithms. In the second part of the section, by presenting driving performance ratings between 92 test subjects, stressed that common wire states contain a message. This is the first study where sensors such as camera, gas, brake, wheel angles of a vehicle are used simultaneously to the literature. All the signals received are segmented into 9 different classes using the PID controller and are combined again and a wide measurement is obtained. There it was that, as cannot be ignored, even the slightest changes in the data leads to considerable

differences. When trying to process laboratory data collected at first by using a part of real life data from the annotating data, a struggle was observed, and problems were reached that would not provide sufficient information. After exposing such an analysis, it was finally exposed by the data that a data set that is enough for the continuance of the research was managed and prepared.

Current topology with writing includes; - The first chapter discusses driver-related states and how they affect driving performance. It deals with works done on this subject and points out the research gap. - The next chapter includes research to classify cognitive states of drivers. Dividing the part into two parts, start with methods that solve systems errors, then continuous with methods solving human error problems. - The third section incorporates the research on the problems facing the driver's attention and its intersecting state of decreasing performance, especially drowsiness. Division this part also inter two parts. We start with methods that solve systems errors, then continuous with methods solving human error problems. - The analysis of the results obtained by evaluating the performance of the deep learning algorithm trained to define the above-mentioned subject related to driving performance and describing the strategy to be followed in the future. - Finally, a test drive was carried out for data recording according to the previous section. Also, if the data will be inadequate, new methods will be sought.

Prior efforts in the literature have mainly addressed the problem of detecting and classifying various driving events such as accidents, lane departures, etc. [6]. More recently, the liability issues have emerged, with insurers (or legal professionals) becoming interested in classifying various driving behavior patterns so as to evaluate the liability of a given driving style for various events (e.g., being responsible for an accident). There is a considerable amount of literature focused on the analysis of driving attention or driver fatigue which realizes the afore-mentioned attention (drowsiness and possi- bly also frustration, impatience, etc…) in the quality of driving performance. For the core of the research, the fault of vehicles also required ultimate application to capable of understanding drivers. In, they focus on the introduction to cognitive states by proposing convolutional networks to understand the state of attention in drivers by images. Similarly, by recording the sensor of the vehicle, the approach was proposed to understand in different times and situations by training

algorithms. This research in the same way and with different approaches focuses on the problem that cognitive states affect driving performance and the interest area.

2. Autonomous Vehicles and Data Collection

In general, the ethical risks related to the use of AI in transport can be relevant either for mass analysis of personal data or for the automatic recognition of travelers using a vehicle. AI tools can process huge amounts of multilayered personal data, and in many cases, they can reidentification people from big data and automatically recognize the individuals captured by sensors installed on or outside an AV. Even AI-supported functionalities meant to manage personal data in AV might be exploited to penetrate the privacy of people traveling in the same AV [7]. An extreme example of reuse of AI data is provided by the case in which, following bugging or interception of communications by incorrect sensors (for example, in case of hacking or network failure), third parties could reidentify individuals or obtain private information about them. Indiscriminate gathering and analysis of personal data within AVs might also be used to create mobility profiles and so leverage them for commercial profiling. This is why AI must comply with new data protection norms such as the European Union's General Data Protection Regulation (GDPR).

Privacy is a human right, and the protection of personal data is an objective which requires specific technical precautions to be effectively guaranteed. This is an especially critical issue for artificial intelligence (AI) systems, and for AI in intelligent transport systems (ITS) in particular. Autonomous vehicles (AVs) involve the analysis of different kinds of data, some environmental and others about the infrastructure and relevant for mobility management, sharing, and so on. In addition to them, exceptional and controversial attention is being paid to the analysis of other kinds of data. Data produced by travelers and by monitoring systems (sensors and systems for the recognition, location, and tracking of people and other vehicles) can be managed to govern transfer costs, foster home automation, optimize traffic, support anti-theft systems, and even intervene to protect the health and assist the driving and mobility of users [1].

2.1. Overview of Autonomous Vehicles

The idea of utilizing personal and sensitive information of different people in vehicular data analysis with autonomous vehicles makes analysts more responsible for ensuring the protection of the privacy of people without negative influence on the accuracy or quality of

analysis and performance. The privacy of an individual can be compromised in many different manners. The way in which it can be compromised in the automotive ecosystem is through applications that extract sensitive and private information, stored in the memory of the car, without the consent of the respective vehicle owner. When autonomous vehicles are being used to make decisions in a safety-critical environment, the most popularly used approach in the literature is to collect data from real-world traffic settings, label the collected data, train machine learning (ML) models with it, and employ the model as a decision-making scheme in the AV [8].

The future of the automotive industry is self-driving cars. The fully automated cars are expected to render the current system of driving licenses and requirements obsolete as the vehicles reach the capability of navigating through highly congested roads without the need for any manual vehicle operations. The self-driving cars currently under development require the collection and processing of the vast amount of data. The data collected by these vehicles comes from various sensors installed on the car, which can be broadly categorized into five major types: the perception sensors, which include cameras, radars, and lasers; position sensors such as GPS; control sensors such as the steering angle; and the environment sensors, including light and temperature sensors . There are instances in which the vehicle may need to utilize the data from the smartphone of a passerby. There are also use-cases such as conducting a DUI-check on a person's driving pattern, which again necessitate the transmission of live data to the police.

2.2. Types of Data Collected

The concept of road traffic monitoring and patterns recognition on urban traffic data usually consists of extracting fingerprint-based features from the data and discovering patterns accordingly. A broad range of systems has been used to collect traffic data which mainly includes LIDAR, Global Positioning System (GPS), unmanned aerial vehicles (UAV), etc. As LIDAR plays an important role in semantic mapping and 3D object detection and could get high resolution and precision data in the real road environment, so LIDAR has been widely used in the domain of intelligent vehicle environmental perception object detection and space semantic mapping. Nevertheless, for high price LIDAR, lower velocity and less density data acquisition method on the shelves, LIDAR has not used in proposing comprehensive perception in the perception field. This paper aims to focus on 3D perception of the

autonomous vehicles after the re-search to more reflect the advantages of concurrent rectification of LIDAR and visual spindle information to support sensor fusion after present state of sensor fusion algorithm and visual spindle rectification algorithm for off-line application and different from the current state of the rectification method combining LIDAR and visual data to be used in an application autonomous vehicle that we used real-time and improved SqueezeDetNet and monocular camera image data in order to process this data [9].

The importance of urban traffic is reflected in the fact that it is the most prominent mode of transportation for citizens in a city and is greatly affected by growing economies and increasing vehicle density, employment rates, and environmental problems. Urban traffic is considered as a primary source of harmful gases, including nitrogen oxide (NOx) and carbon oxide (CO), and have become a huge problem for scientists and environmentalists around the globe for their potential hazards [10]. The road traffic monitoring and control systems plays an important role in controlling accidents, feeding the emergency and law enforcement services and controlling the urban traffic flow based on the obtained information. Many of research has focused on road traffic monitoring and intelligent traffic management systems based on data analysis and data warehousing algorithm and methods for changing that data. The main aim of these systems is road traffic and patterns recognition has been to upgrade the public safety for travelers, more and giving accurate and fast information that is for all travelers and vehicles.

2.3. Challenges in Data Collection

"The approach of relying on hidden agebraically saturated models, as employed in both and [11], cannot bypass such issues, as there is still an explicit encoding of design space in the synthesis phase. Therefore, our approach of local measurements in the PaS framework is necessary, yet we show that these are impactful in a whole range of different modalities of verification synthesis. They identify needed behavior, but no weight is given to how unusual it is, due to the lack of a specific target that needs to be approached. On the other hand, when data is aggregated from multiple users, as would be the case for an implicit requirement, some information could be inferred about the transition relation. As discussed in Section 2, such artifacts include removal of implicit features, incorrect hand-crafted partitions or proxy associations, and compromise of submodel formal properties. While the existing methods that work towards protecting privacy in training data, track, or hardware are too relaxed to ensure

worst-case privacy, for some autonomous machine-learning applications valid off-policy training data is also needed. In such settings, simplicity of data dissemination, application-level post processing for preserving privacy or using a distinct instance of automaton systems tailored to every multimodal user may come without significant practical impact. Therefore, our perspective shifts to characterize what threat model is observed in SW verification."

"We present a confidential automaton system [12]. Without loss of generality, this solution uses selectively hidden verification—otherwise, a confidential automaton system can at least reveal information about the model, if not the transition relation. Therefore, a privacy-preserving automaton synthesis (PPAS) involves neighboring models [13]. However, learning that is based on user-provided examples and does not rely on the complete transition relation is useful in a range of scenarios. This is crucial since our verification is based on a subset of reachable states or violated safety properties. Furthermore, there is substantial effort required in experiment design and data collection for ensuring complete coverage of the design space for random verification methods to be effective. While in some contexts such data abundanceseems unlikely, our method couples analysis and synthesis, so that capability is more balanced by the actual requirements of verification."

3. Privacy Concerns in Autonomous Vehicle Data

There is a pressing need to develop privacy-aware machine learning algorithms for large-scale data mining and multi-terminal data sharing in autonomous vehicles. Machine learning has become widely accepted for traffic prediction in smart transportation scenarios. Zhang et al. [14] proposed a privacy-aware distributed machine learning system for managing data onboard autonomous vehicles. A protocol is developed for stream data to be protected with local differential privacy during learning. This privacy-preserving data mining method has been widely proposed to protect passenger shared data for federated learning, criminal-protected data for protecting user privacy and continuous data protection schemes in smart cities. The combination of the above methods can be treated as a privacy protection scheme for the intelligent transportation system.

Critics argue that autonomous vehicles (AVs) are overly fixated on transportation safety and overlook privacy concerns [1]. The characteristics of AVs produce a large amount of inexplicable data, which can not only improve the driving performance of vehicles but also carry out personalized services like travel behavior. In the process of data connection, storage,

and sharing between vehicles, various kinds of data interaction, such as vehicle intelligent control systems, network communication and secondary development of hardware and software, PMs will be generated from different types of ontological data. These security services are applied to AV: Cellular Vehicle To Everything (C-V 2 X) Standard PM, CAN Standard PM, and Secure software based PM. These services secure the corresponding information types, such as geographic location, power consumption, driving habits, etc. Researchers believe that it is feasible to evaluate the security of such vehicles.

3.1. Sensitivity of Vehicle Data

European drivers would consider economy and comfort as the primary reasons for buying a car, while 60% also appreciate the safety it offers. However, they consider safety in terms of the technological functionalities the vehicle offers and privacy vulnerabilities rank among their principal concerns. 37% of the European drivers are concerned about what types of data the vehicle will store and for how long, to whom the information will be disclosed and for what purposes it will be used, while 35% would like to know if they will still be able to enjoy privacy and data protection when fully connected vehicles are in operation. Moreover, 47% fear that connected functions could be monetized through subscription services, while 39% would like to be sure that they could continue driving even without fully accepting any service providing access to their data. Therefore, in order for the uptake of autonomous vehicle (AV) technologies to be successful not only from an innovation and business point of view, but also from the social and consumer point of view, the impact of the privacy robustness of intelligent on-board and remote AI component architectures needs to be considered with high priority, as this impacts the freedom and well-being of people.

Vehicle data can be broadly classified into two categories: the data generated by the vehicle itself and the data exchanged between the vehicle and external entities such as the vehicle manufacturer's cloud and the roadside infrastructure [15]. The hardware and software of connected vehicles collect and internally process, among others, sensitive information, such as the geographic position, speed, acceleration, pressure, temperature, loads, ambient conditions. Cloud and roadside infrastructure platforms usually acquire high-level information like the vehicular geographic position, the vehicle speed and the presence of a smartphone or a credit card belonging to the vehicle user. Additionally, data from multiple vehicles can be processed centrally to provide insightful information to the service providers.

This data exchange should be efficient, as the exchanged information is diverse, large in volume, and fast evolving. While on one hand all this information exchanges enhance the user experience and significantly contribute to the adoption of new applications and technologies, on the other hand they have an enormous impact on driver privacy, especially in the case of semi-autonomous and fully automated vehicles [7].

3.2. Regulatory Frameworks and Standards

Thus, to guarantee the respect of human-privacy rights, the vision of privacy-preserving deployment of AI-DM models must meet numerous requirements that will be transplanted in complex laws and normative acts, as the future legal contexts could be very varied. For sure, at least the following requirements have to be fulfilled at the maximum constraints level by design-based protection approaches: The AI-DM instantiation process must not increase the disclosure risk compared to the deployments of non-privacy-aware models The protection process itself must be inheriting from some concrete guarantee, in order to know if what was applied as privacy aware training was beneficial for the process The protection process itself must not be more complex in terms of inference use compared to the case where no sps-mChalles protection is put in place The training and protection process must not introduce default risks, or their propagation, for instance by making the AI-DM intolerant to small adversarial ones compared to the nonprotected AI-DM deployment. All norms reaching these goals in some particular contexts will impose hard requirements that have to be designed at the model-instantiation level and are the cornerstone of this vision. [16]

Although, when it comes to the development of intelligent and autonomous vehicle technologies, the strong emphasis on software performance and the increasing footprint of AI decision making (AI-DM) systems in the next generation of the intelligent vehicle controllers may introduce not-yet-recognized privacy risks [7]. Indeed, releasing AI-DM models represents releasing information about how the device would react in certain scenarios, thus contributing to an attitude concerning how to overtake autonomous vehicles, how to hit people in crosswalks, etc. A logical approach for protecting this sensitive training data would be to deploy the AI-DM models in production distribution with certain methods that would vary according to the gap between training data distribution and production data distribution. Meanwhile, protection methods and guarantees are also required to conform to legislation such as the Regulation 2016/679 of the European Parliament and of the Council of

27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46, known as the General Data Protection Regulation. In the case of production data distributions being very similar to training data, appropriate solutions should be capable of sustaining privacy preservation against adversarial reidentification attacks. Before going further, we describe the privacy problem as something occurring when sensitive information leaks from a protected distribution.

3.3. Potential Risks and Threats

- E-Calls: It is a new type of wireless distress call or emergency help call. E-Call type 1 is expected to complement the 112 public safety answering point (PSAP) with additional highly accurate incident information, using historical data and data provided by other vehicles in the near area. It could be hard to keep sensitive emergency information about drivers confidential and answer all the e-call on time. An e-Call could remove the driver's anonymity and potentially reveal sensitive geographical places. Additionally, there is high-time pressure to answer these calls [17].

- Individuals/Drivers: The ability of the autonomous system to keep personal data confidential and private is crucial. Autonomous vehicles would collect a large amount of data from their drivers. One type of data is in-vehicle data (sensors, cameras, GPSs), which might reveal a lot about the driver, such as health information, behavior patterns, and secret personal places [5]. Besides in-vehicle data, there is also a large amount of generated or acquired data externally (third-party data). For instance, there are many social networks where user activities could be acquired. Another social network, like Facebook, could be joined to some external identifications (if there is no anonymization), which would leak private information. Therefore, the potential risks considered in this paper are; vehicle-related health and socio-behavioral information, vehicle-related privacy-risk sensitive zones, the third-party data could probably identify the driver and data confidentiality of the third-party data itself. A secure system must be able to keep all these data confidential and private from outsiders and stakeholders (companies, curious employees, or other entities that might have access to the system but should not have access to personal information). A car owner or lessor could be a new entity interested in the privacy of the collected driving data.

TRUST is a critical factor for the successful operation of any system. Potential users of the connected/autonomous vehicle systems must have trust in the underlying technology and be assured by the authorities that their personal and professional information is being protected. We identified the following privacy risks for autonomous systems, and some potential attacks that could occur for different stakeholders involved in this eco-system:

4. Privacy-Preserving Machine Learning Techniques

Machine learning (ML) is the foundation research for intelligent transportation systems (ITS) and autonomous vehicles (AVs) and has been integrated into aspects related to AV design and deployment such as traffic monitoring, mobility prediction, and object detection. This transition to machine learning based AVs results in a need for training data, where gathering real-world data is an important part of evaluating the performance of the learning algorithms (i.e., the more similar to the real world the data used to train the algorithm, the better and safer the decisions made by the algorithm will be). The real-world training implementations have privacy implications, as they usually involve the collection and analysis of personal data, opening the door to various threats such as user tracking, profiling, and discrimination. To adapt the current privacy guidelines of implementing anonymization, consent or encryption to the AV training process, it is important to consider the specific privacy requirements from the well-known Vindija principles, as well as to adopt a comprehensive taxonomy and to develop privacy preserving solutions specific to each layer of the AV.

[18] [19]Machine learning (ML) is the foundation research for intelligent transportation systems (ITS) and autonomous vehicles (AVs) and has been integrated into aspects related to AV design and deployment such as traffic monitoring, mobility prediction, and object detection [5]. This transition to machine learning based AVs results in a need for training data, where gathering real-world data is an important part of evaluating the performance of the learning algorithms (i.e., the more similar to the real world the data used to train the algorithm, the better and safer the decisions made by the algorithm will be). The real-world training implementations have privacy implications, as they usually involve the collection and analysis of personal data, opening the door to various threats such as user tracking, profiling, and discrimination. To adapt the current privacy guidelines of implementing anonymization, consent or encryption to the AV training process, it is important to consider the specific privacy requirements from the well-known Vindija principles, as well as to adopt

a comprehensive taxonomy and to develop privacy preserving solutions specific to each layer of the AV.

4.1. Differential Privacy

Federated learning is a useful learning schema that preserves the privacy of local data. In the first part of this section, the issue of ensuring information privacy of individual driving data is solved considering a federated learning schema. The data analysis algorithm is trained on driving state data collected locally by vehicles, retaining private sensitive data. The second part of this section describes how to train machine learning models that maintain user privacy. To this aim, an automatic mechanism for calibrating and choosing the right hyperparameter value for an ε-differential privacy is provided. We point out that the defense of privacy should limit the action of an adversary able to decorate real data interacting with the system. By providing the present approach, the goal is to remove interactive parts from the implementation of the differential privacy-aware algorithms in the autonomous vehicle. In this way, the concept of virtual DPS code is introduced, which is a set of functions that generate virtual private driving state data. The behavior of the data analysis algorithm trained on this virtual DPS data is indistinguishable from the algorithm trained on the real DPS data."

"Differential privacy [20] is a concept in the field of data privacy that relates to the mathematical definition of the privacy of a specific data analysis query. The goal is to keep the record of an individual secret even from someone with complete knowledge of the rest of the dataset. The concept includes the formal privacy definitions, methods for producing anonymized data that satisfy the definitions, data collection, and database querying procedures, and many area-specific case studies. The definition's usability depends on an evaluation of how well it achieves privacy while maintaining data accuracy. Differential privacy is surely the most well-studied recent definition of privacy in the database setting. The main idea of differential privacy is that the inclusion of one database item does not significantly affect the output distribution, regardless of the actual values in the database. In a vision, future driving data analysis should be preferable to use more complex and robust privacy-aware data analysis algorithms; moreover, privacy-aware algorithms should operate removing interactive parts to ensure that no data leaves the autonomous vehicle. Among the possible privacy-aware algorithms, there is differential privacy, which is the focus of the contributions in this work that are described in the following.

4.2. Homomorphic Encryption

The exponential running time of Generally Hosted Encrypted Data Service is an important reason for the efficiency of current techniques that use HE to search for an applicable model for deploying the encrypted data in a manner $0 \leq \alpha$ 1 thanks to the low practical extra costs that arise in case α is small. HE techniques mentioned above are likely to run slowly and to require higher practical costs when the number of feature variables that make up a single sensor data is quite large [18]. In cloud ML systems that are developed based on HE technologies getting a prediction can be time-wasting and has higher costs if the number of feature variables is quite high. Because the communications between cloud ML gateways and user mobile devices with this scheme are have to be multiplicative operations per each feature variable that corresponds to one sensor, after sending each string of mobile data from these gateways to the server of the host side model in an encrypted manner..

[21] [22]Homomorphic encryption (HE) is a cryptographic encryption scheme whose types are significantly differentiated in terms of how local the operation's scheme is to the server of an HE system. Fully homomorphic encryption schemes are capable of carrying out any complicated operations at the server's side without decrypting sensor's data. However, fully homomorphic encryption has two main disadvantages: (1) Slow to process and (2) the scheme is not yet practical to be used widely. On the other hand, slightly homomorphic encryption is not capable to perform arbitrary operations by the cloud ML algorithms. Nonetheless, paillier scheme with its partially homomorphic property and multiplicative properties would be efficiently used in ML classification tasks such as logistic regression, multilayer perception etc. The encrypted data are sent to the cloud ML model. Then, the cloud performs a series of calculations using its homomorphic decryption key to make a prediction on the encrypted data.

4.3. Federated Learning

Federated Learning (FL) could be a general solution to protect user traffic data with privacy-preserving technology. During FL model training the basic idea is to allow multiple parties, or wireless devices, collaborate and train a shared model, while keeping raw data staying at the edge of the network. Many methods have been designed to adapt typical machine learning algorithms for the federated learning scenario [19].

Several key notes are to be observed for autonomous vehicle data analysis. Specifically, the huge challenges stem from the data availability and addressing privacy concerns of users' transportation data [23]. With the growing concerns of using machine learning technology for various services, challenges and threats must be addressed. One significant challenge is how to provide state-of-the-art services with the use of precise and valuable data while at the same retreating the privacy of the data owner [24].

5. Case Studies and Applications

Anonymization could be used at the discretion of the data collector. In the same way that a manager can decide to store private data from its employees only if needed, a data collector can decide to only keep the anonymous version of the data it collects when this does not affect the utility of the data for his tasks. A Pareto-optimal platform is a trade-off solution allowing the maximization of the performance with respect to privacy, for a given privacy level corresponding to the driver consent, activity, and privacy awareness.

[25] [21]This section describes application scenarios for privacy-preserving autonomous vehicles: Enroot, which is a project aimed at creating a privacy-preserving routing system for electric cars. It is using OPENX-SCRTC to decide secure routes to traverse efficiently while avoiding dangerous zones. The precomputed data and secured-tunnel selection algorithm are evaluated on the YFCC100M and Electric Vehicles charging zone datasets, and their efficacy has been tested in integration with Pedestrian Warning System (PWS) and Autonet as well. An example video of a pedestrian crossing and a road accident next to the car is shown which successfully detects vehicles and pedestrians, while anonymizing the pedestrians. A scenario in which those methods could be applied to facing both privacy and security issues is put forward.

5.1. Privacy-Aware Algorithms in Vehicle Telematics

These systems can impair driver privacy because they transcribe inputs from an external source and compute an output without the involvement of the individuals for whom the output is destined. Pan-European data protection laws are enforced in accordance with telematics in vehicles. The EU General Data Protection Regulation (GDPR) applicable to car driver telematics within Europe provides specific conditions to be fulfilled from when a vehicle starts performing a custom (intelligent transportation systems, smart mobility, autonomous driving, etc.) operation for automatic detection of driving risk to while deciding

on how to provide feedback to the human driver. Moreover, when it comes to driver rating analysis and traffic risk prediction strategies, the usage-based insurance (UBI) policy deploys a rate-tracing protocol that will keep on recalculating a person's insurance costs according to the driving style. Knowing the defined score computed by a UBI protocol is enough to infer all the precise driving moves and behaviors supported by the designed protocol and subsequently, to predict the relationship between the driving parameters and the rewarding decrease in a driver's rate.

Monitoring and analyzing driving styles and behavior is a rising research area in the field of Intelligent Transportation Systems (ITS) as it helps transportation authorities to take corrective actions to reduce traffic incidents, government bodies to optimize transport and urban planning, and car insurance companies to price their coverage according to the driving risks and inaccuracies. During recent years, advanced driver assistance systems have become far more popular and essential not only as useful tools, but also as life-saving technologies. Advanced driver assistance systems (ADAS) are the standard embedded software which is a part of the operating system designed to support a human driver. This includes traffic sign recognition (TSR), advanced navigation systems, and hands-free steering. Some of these systems have become almost ubiquitous, while others are still mere prototypes but becoming accessible. State-of-the-art driving styles [26] are conventionally detected ahead of all within telemetry systems with the implementation of deep neural networks (DNNs). Although these are known to be proficiently accurate in driving style recognition, these models enclose essential privacy and security demands. Storing personal telematics data like car or driver features and transmitting this data to the insurance industry have provoked many publications focusing on the privacy concerns related to collecting and sending private telemetry details.

5.2. Secure Data Sharing in Vehicle-to-Everything (V2X) Communication

To prevent rear-end collisions in V2X communication, sentry cars send their own data to surrounding cars to inform them about previous collisions. Since this collision information may concern ongoing lawsuits, sentry cars may not want surrounding cars to know their identities. To enable V2X communication, various privacy-preserving techniques, using both machine learning and non-machine learning assets, have been proposed. In order to preserve vehicles' privacy, pseudonymity schemes have been designed [21]. This is done by changing

vehicles' unique identities at every message broadcast round. Secure data sharing in V2X communication using a vehicle's radio frequency (RF) signature has also been proposed.Suppressing the vehicle's own identity, without changing it, privacy-preserving communication is also possible. An authentication scheme recently proposed by the authors does not require a vehicle to hide its true identity from other V2X components, as a vehicle can authenticate itself to other components, such as roadside units or sentry cars, without revealing itsidentity.

As vehicles' levels of autonomy and connectivity increase, they generate vast amounts of data, including vehicle sensor data, and traffic condition data [27]. Vehicle-to-everything (V2X) communication, a part of connected and automated vehicle (CAV) technologies, enables data sharing among different components: vehicles, infrastructure, drivers, and backend servers. This interconnected system provides several benefits, including enhancing road safety and urban mobility. However, it also introduces potential privacy risks for participants and their data. To ensure the privacy and security of V2X communication, we need machine-learning-based privacy-preserving model development and deployment techniques. In this section, we introduce ML algorithms for secure data sharing in V2X communication and analyse them in terms of how they can address different machine-learning-based privacy-preserving techniques (fully homomorphic encryption, differential privacy, and secure multi-party computation).

6. Evaluation and Performance Metrics

This study presents a novel privacy-preserving feature selection procedure integrating perturbation-based privacy-preserving measures with a feature selection heuristic. We introduce a privacy-preserving information gain heuristic that ranks the privacy-preserving selected features to propose a near-optimal reduced feature subset. We evaluate the performance of the proposed privacy-preserving optimal feature subset selection technique using four real-world autonomous vehicle datasets. We provide a thorough and deep analysis of the proposed feature selection technique by evaluating 14 statistical classifiers, including six ensembles, four neural networks, and four other popular classifiers. The results show that the proposed technique consistently outperforms existing state-of-the-art privacypreserving feature selection methods in terms of classification accuracy, classification earliness, classification time, synthetic data efficiency, and Pareto efficiency of Distance Reasoning

classifiers. We also conduct an instancelevel evaluation of the presented privacy-preserving feature selection technique showing that it outperforms the state-of-the-art DeepOPM method in identifying privacy-preserving selected feature distribution composed CVs.

In order to build trust in autonomous vehicles, it is important that car companies, data scientists and policy makers take user privacy and data security seriously. Privacy-preserving analytics on autonomous vehicle data has been drawing growing attention as it ensures high-quality data is transformed to support learning. Extant studies report that privacy-preserving data can be exploited and evaluated for different applications [5]. This means, the identified privacy-preserving algorithms can potentially be employed in real-world AV scenarios.

6.1. Accuracy and Utility Preservation

As sophisticated and intricate as they are, privacy-preservation mechanisms should not degrade the accuracy of machine learning algorithms significantly. Using privacy-preserving adversarial model inversion attacks, [3] empirically demonstrate that the effectiveness of various privacy-preserving methods strictly depends on the initial capacity of the DNN. They argue that for sufficient simplicity and low initial capacities, introchraticon times achieve reasonable levels of accuracy when applying a variety of privacy pressure mechanisms. One way to bridge the gap between the enormous design and implementation of low-accuracy utility-preserving learning systems is to employ a second system such as two-stage learning, where a computationally efficient (and hence accurate) doorman is used to quickly eliminate useless signals, before being sent to a dedicated utility-learning system—called a doctor. [25] Based on these observations, Go away, Doctor and Concierge Learning systems have been proposed to address this problem. Go-away and Concierge are human supervision modes which are used in doctor-concierge SVM (DC-SVM) training, a reliable tool for evaluating the quality of data, assessing the quality of training data, and pointing out the patterns which should be removed from the doctor.

6.2. Privacy Guarantees and Compliance

The development of AV services, in particular those fully reliant on data processing, raises ethical and technical concerns. Among others, detectable privacy intrusions might occur. Throughout the data acquisition, storage, and processing stages, potential threats to privacy exist; for example, the following types of data are obtained and stored: driver-related information, vehicle information, external information regarding the surrounding

environment, and traffic information. Since it is difficult to pinpoint the specific scenario in which a possible attacker could strike, it is difficult to ensure that every possible intrusion can be detected and combatted. This difficulty is especially pronounced in machine-learning methods and the privacy-preserving Data Mining methods used to carry them out [5].

Autonomous vehicles (AVs) are becoming increasingly popular, and many major technology firms and car manufacturers have developed, and are continuously improving, their AV technology. Major challenges for the AV include algorithms for trajectory optimization, traffic flow prediction, and improved localization and detection systems, which affect the safety of the vehicles and their passengers. Furthermore, since AVs are designed to be Internet-connected, they continuously aggregate and try to learn from the data they produce [1].

7. Future Research Directions

To mitigate risks connected with compromised maneuverability in harsh weather conditions, an existing architecture or platform for data collection and analysis could be extended. Furthermore, when a sensor in the system starts to fail, it should be easy to evaluate the risk early on. For instance, if the camera stops working, it is important to recognize the potential risk obtained by this failure mode. This requires specific input signals that can be processed into a meaningful interpretation. This hard negative signal will only improve the behaviour when sensor fusion algorithms are able to understand full awareness at every cycle. Moreover, better results in the risk assessment could potentially be achieved if the sensor fusion algorithms could interpret and learn from data obtained by single sensors [28]. Furthermore, for a multitude of sensor types, single sensor deep learning approaches could be used to extract more information from sensor types of which this was not possible before due to the limited sensor fusion capabilities.

The focus of this article was on addressing the privacy challenges associated with the analysis of autonomous vehicle data [24]. Nevertheless, algorithmic decision-making in autonomous vehicles also gives rise to some ethical and technical challenges regarding the data that is being used for those algorithms and the systems that deal with processing the information. At the intersection of these fields, much research is taking place regarding Responsible Data Science (RDS). It concerns the way to create models or analyze existing data in a way that reflects the societal values in the data. Fairness is explicitly evaluated as one of the RDS dimensions. Moreover, privacy from a data analytical perspective is addressed through the growing field

of privacy-preserving data mining techniques [1]. Additionally to address the specific challenges, it is possible to look into some other research directions.

7.1. Advancements in Privacy-Preserving ML

Most existing privacy-preserving federated-learning approaches have two major limitations: First, most of them ignore the issue of plausible deniability, i.e. the ability of the model's owner to deny that a given inference was computed with their global model. This is not a mere technicality; in certain scenarios, for instance following the OpenAI-DALL-E-prompt controversy, manufacturers of machine learning models might want to deny that some particular outputs were ever generated by their models. In this context, we say that "plausible deniability" is the property of an ML model that makes detecting whether a given output was generated through the model technically inconclusive; rather, other factors are expected play a causal role [29]. Even within the current technical and regulatory context, if there persists an "always-on" back-door between inferences and the individual input training samples associated with it, an adversarial agent may invent a novel privacy attack, whose cost-causing backslash might also tarnish the manufacturer's reputation, and deter potential clients from relying on these models. Second, and related to this, federated-formalism-based approaches make the ongoing update process traceable. Consequently, the adversary might also design a privacy attack to dismantle the learning behavior itself; in particular for implementations with a low discontinuity resistance, the adversary might algorithmically interact with the model to reverse-engineer and therefore disclose its architecture, which is set to be a trade secret [5].

Many machine learning algorithms may accidentally violate privacy of the data. Often, they contain vast details of the training data in the trained model, and an adversary may query the model to extract information about some samples of the training data even without direct access to the training data. In addition, sharing sensitive information about their training data is not uncommon for machine learning models. As a concrete example, employment decisions, identified in one study to correlate with changes in regional Google search queries and satellite-image luminosity [30].

7.2. Integration with Edge Computing

In this privacy preserving recommendation technique, part of the user's private data models is trained at the remote server and the vehicle itself. The deployed deep reasoning and privacy-preserving recommendation engine should be performed on the device itself [31].

Outgoing data are kept private as long as possible without severely affecting the recommendation accuracy. The deep reasoning recommendation engine is designed to consist of two modules, which are a secure machine learning model and a Binarized Neural Network, and is annually optimized for lightweight vehicles. Privacy is enhanced using a differential privacy mechanism and binary model characteristics in the first recommendation engine, and the traffic of the second data is designed within split-layered compressed secure architecture.

Communicating real-time data anomalies between smart vehicles in a privacy-preserving way enables a fine-granular data analysis. However, in the existing communication protocols, this functionality decreases the endpoint privacy [21]. The inability of the impaired endpoint to process the anonymized date can decrease the clustering accuracy of the nearby traffic. A solution for fine-granular real-time anomaly detection may consist of two subsequently chained algorithms. The algorithm are: (i) nano-FALE, an algorithm with which vehicle privacy is guaranteed, and (ii) PandeRAiled an algorithm with makes use of a reverse anonymsin service and an attribute distinction algorithm to protect the owner from malfeasance. In the paper by Zhang et all. a fourth approach based on edge computing is presented to mitigate some drawbacks to support friendly communication endpoint protocols.

8. Conclusion and Summary

In summary, a vehicle driving behaviour analysis system requires a considerable amount of data, which generally comes from different in-vehicle IoT sensors and external road infrastructure sensors. Based on the type of sensors used, this data can be classified as in-vehicle and environmental data. Privacy risks are mainly introduced during the handling of in-vehicle data, particularly during data collection/storage and data algorithm model training and testing. This is because an in-vehicle data subset will be utilized in these phases that have multiple in-vehicle and environmental sensor data parameters. To efficiently handle the privacy and data utility issues associated with in-vehicle data processing we have identified that (i) public key cryptography, (ii) user behaviour pseudonymization, and (iii) data poisoning attacks are the main areas. Therefore, we proposed (i) the introduction of public key cryptography algorithms, (ii) the use of the Trusted Execution Environment (TEE), and (iii) the employment of robust and union problem data poisoning attack strategies, to minimize the unfavourable impacts of privacy requirements on the accuracy of a proposed

driving behaviour analysis model during in-vehicle data analysis and robustness validations [21].

Machine learning has almost a few advantages for use in autonomous vehicle environments, like its capability of processing large volumes of heterogeneous data for driving behaviour analysis. However, the privacy concerns of machine learning algorithms employed in this environment might restrict its wider adoption [6]. Considering this, this article focused on the importance of the privacy concerns in machine learning algorithms and assessed the application of privacy-aware machine learning models in the context of autonomous vehicle data analysis.

8.1. Key Findings and Contributions

The figure of taxonomy (III) presented in Section 3 opens new research and development directions in privacy-preserving machine learning enabling algorithms such as low-rank non-convex optimization-based topic modeling, and user personalization strategies integrated into the deep learning models and concepts of differential privacy based privacy-preserved structured topics derived using the variational autoencoders and homomorphic encryption techniques in the standpoint of service quality [32]. In fact, combining algorithms such as differential privacy, homomorphic encryption, and federated learning can serve, not only as possible sources of our future work that can be considered for multiple data analysis in future, but also a practical measure in the light of principle of complete data privacy preserving and AI ethics for the deployment of future AI based systems in practical life such as general practice medicine recommendation system, criminal identification system. Moreover, we consider developing new distribution invariance homomorphic encryption schemes for several settings. The idea is pursued through new cryptographic techniques interplaying in a novel connection together with state-of-the-art functionalities such as ideal lattices, Ring-LWE, Discrete Gaussian Distributions, homomorphic encryption, and other exciting techniques applicable for privacy-aware machine learning models. By showing experimental support with detailed results we also propose to start working on TRL-6 level real form homomorphic encryption deployments [33].

The extensive, comprehensive literature review conducted in this chapter resulted into identifying and analyzing current state-of-the-art techniques for privacy-preserving machine learning algorithms (PPMLA) and privacy-preserving data analysis techniques [5]. It has been

observed from this literature survey that, most of the currently available techniques focus on achieving full privacy protection by using encryption and privacy preserving machine learning techniques that have high computational overheads. As noted in the previous section, virtually all currently identified research efforts focus on either time-domain or frequency domain data. There is a need to work on real data acquired from urban autonomous vehicles. This chapter starts with an extensive literature review on current state-of-the-art techniques for privacy preserving data analysis and machine learning approaches. It presents an extensive survey on privacy preserving machine learning algorithms that have been considered in this chapter.

8.2. Closing Remarks

[2]This book presented new privacy-aware machine learning algorithms and architectures that can be used for data analysis in the domain of autonomous vehicles. Privacy-aware patterns, combined with federated learning strategies, could be adopted to produce localised prediction models shared by vehicles (VItorY methodology), thus achieving a good trade-off between the precision of local prediction algorithms tailored to specific vehicles and the amount of data exchanged. Alternatively, it was demonstrated that privacy threat minimisation strategies could be directly integrated in the learning process in order to create shared models across vehicles that are robust in the presence of adversaries trying to inferences information about specific data samples in the training set. To safeguard from adversarial inference through both knowledge-disentangled representation learning and adversarially-prudent local prediction models, we exploited generative models and prediction models, which monitor the presence of knowledge of a specific ground-truth label to grant confidentiality in the vehicle side.[33]This book presents new privacy-aware machine learning algorithms which can be used to enforce privacy-aware data analysis in the domain of autonomous vehicles. Our Privacy Calculus-based Federated Learning (PCFL) method is suitable for shared (cross-vehicles) and server-based models. To support its widespread adoption of Privacy-aware ML in the ACVs domain, we adopted the concept of Privacy Impact Assessment (PIA), extended to ATIS for privacy-aware risk prevention throughout the entire lifecycle of the model. A technical solution is then deploying federated learning (FL) and homomorphic machine learning (HML) to ensure the privacy and confidentiality of the AV data are maintained during the data processing in the data center. Furthermore, the Move-Regress architecture will allow future autonomous vehicles (AVs) to integrate privacy-aware

learning models for an automatic protection by default of the cyber-physical records, ensuring the perpetual re-examination of their capabilities and operational suitability in light of the variable cultural needs and expectations of society through accountable traceability.

Reference:

1. Perumalsamy, Jegatheeswari, Bhargav Kumar Konidena, and Bhavani Krothapalli. "AI-Driven Risk Modeling in Life Insurance: Advanced Techniques for Mortality and Longevity Prediction." *Journal of Artificial Intelligence Research and Applications* 3.2 (2023): 392-422.
2. Karamthulla, Musarath Jahan, et al. "From Theory to Practice: Implementing AI Technologies in Project Management." *International Journal for Multidisciplinary Research* 6.2 (2024): 1-11.
3. Jeyaraman, J., Krishnamoorthy, G., Konidena, B. K., & Sistla, S. M. K. (2024). Machine Learning for Demand Forecasting in Manufacturing. *International Journal for Multidisciplinary Research*, *6*(1), 1-115.
4. Karamthulla, Musarath Jahan, et al. "Navigating the Future: AI-Driven Project Management in the Digital Era." *International Journal for Multidisciplinary Research* 6.2 (2024): 1-11.
5. Karamthulla, M. J., Prakash, S., Tadimarri, A., & Tomar, M. (2024). Efficiency Unleashed: Harnessing AI for Agile Project Management. *International Journal For Multidisciplinary Research*, *6*(2), 1-13.
6. Jeyaraman, Jawaharbabu, Jesu Narkarunai Arasu Malaiyappan, and Sai Mani Krishna Sistla. "Advancements in Reinforcement Learning Algorithms for Autonomous Systems." *International Journal of Innovative Science and Research Technology (IJISRT)* 9.3 (2024): 1941-1946.
7. Jangoan, Suhas, Gowrisankar Krishnamoorthy, and Jesu Narkarunai Arasu Malaiyappan. "Predictive Maintenance using Machine Learning in Industrial

IoT." *International Journal of Innovative Science and Research Technology (IJISRT)* 9.3 (2024): 1909-1915.

8. Jangoan, Suhas, et al. "Demystifying Explainable AI: Understanding, Transparency, and Trust." *International Journal For Multidisciplinary Research* 6.2 (2024): 1-13.
9. Krishnamoorthy, Gowrisankar, et al. "Enhancing Worker Safety in Manufacturing with IoT and ML." *International Journal For Multidisciplinary Research* 6.1 (2024): 1-11.
10. Perumalsamy, Jegatheeswari, Muthukrishnan Muthusubramanian, and Lavanya Shanmugam. "Machine Learning Applications in Actuarial Product Development: Enhancing Pricing and Risk Assessment." *Journal of Science & Technology* 4.4 (2023): 34-65.