Privacy-Preserving Fleet Management Systems for Autonomous Vehicle Operators

By Dr. Ekaterina Ovchinnikova

Associate Professor of Applied Mathematics and Computer Science, Saint Petersburg State University, Russia

1. Introduction

In order to remove the current excess capacity requirements associated with storing vehicles during normal business hours, "staging" areas should be located and understood to serve as refueling stations, locations for transferring goods for local distribution, or areas where maintenance on the vehicle inventory can occur. Data analytics on such fleet management datasets are a critical part of planning and operating efficient and high-capacity shared-AV programs. However, the spatial and temporal resolution at which such data must be stored and visualized can threaten to invade the privacy of the riding public. The insertion of privacy-preserving technologies into the data processing pipeline can serve as a protective measure.

Autonomous vehicles (AVs) have the potential to provide a radically increased level of mobility, but they also have the potential to have a negative environmental impact. AVs can have an extremely high utilization, one that can arguably outstrip the capacity of public transportation in urban areas, particularly as more AVs become electric. Simultaneously, a shift to a mobility ecosystem dominated by autonomous vehicles, particularly one where emergency vehicle services are not constrained by congestion, could dramatically improve public safety.

1.1. Background and Motivation

The next generation of mobility solutions will entail far-reaching changes in the design of the vehicles themselves, the design of the systems within which the vehicles operate, and the scope and cultural practices surrounding transportation and mobility. These changes will have direct and indirect impacts on various areas such as economics, privacy, environment,

and governmental policies. One of the most discussed and researched applications of mobility automation is autonomous vehicles (AVs). The deployment of AVs has significant potential to solve what is known as the transportation "Triple Timing" problem: shorten travel times, reduce the uncertainty of travel times, and release the value of mobility time, as well as providing additional societal benefits such as increased safety, equity, and land use. Consequently, now is a very exciting time to address important research questions related to AVs, particularly those that regard the role that they will play in urban and regional transportation network systems and, conversely, the effect of these systems and the overall systems of which they are a part upon AVs and their development.

Motivated by the emerging deployment of electric taxi services, we consider the privacy and efficiency of a standard fleet management problem (FMP) for electric taxis. Our model captures the key structural features of an autonomous taxi service and explicitly incorporates battery health, operational costs such as charging delays and partial charging, externalities such as traffic congestion cost, and three types of ride-sharing. We provide solutions to the FMP in both offline and online settings, and examine the impact of supply and demand on the key decisions and the efficiency of the taxi service. Finally, we conduct numerical studies to evaluate the viability of electric taxi services. The numerical studies show that potential environmental benefits can be achieved while providing a financially sustainable autonomous electric taxi service. Specifically, our results suggest timely partial charging when the service is experiencing congestion and delaying charging when the service is not busy.

1.2. Scope and Objectives

The proposed system should support a comprehensive framework to enable the operator to diagnose real-time incidents on sites where dense data collection is present, where - even with reduced data collection - a privacy breach due to increased inference capabilities in a more complex environment should be achieved. The proposed system should fully integrate AC attribute constraints to handle attributes that are not known to the system in real-time. The aggregates and policies need to adjust to balance the trade-off between event resolution and surveillance and offer methods that support semi-real or full studies of confidence in view of access to limited data.

This study focuses on the development of privacy-preserving fleet management systems tailored specifically for AV operators and designed to operate in the context of data

confidentiality, data aggregation, and efficient privacy model updates. The system should be motivated by the operator's ability to design and introduce strategies in respect of regulation requirements, control and manage privacy in the context of real-time event detection and resolution, and the ability to create privacy policies that will help balance surveillance during event diagnosis and data privacy protection.

2. Fundamentals of Fleet Management Systems

Before we delve into the details, it is prudent to review how classical FMS are structured, the hardware and software tools that compose them, and the practical business scenarios they model. Vehicle tracking systems represent the electronic log of driver activity. This is used to track drivers and their vehicles. The GPS tracks the vehicle location and other transactional data. This tracking takes place in real-time. Collected from the vehicles is analyzed using fleet management tracking systems, which make an estimate of an ideal route that is driven by the driver. The actual route and the ideal route are used to provide alternative routes the next time the driver engages. Other examples of vehicle systems include systems for vehicle maintenance, vehicle diagnostic systems, and systems to monitor the safety and efficiency of the drivers. Fleet management tracking systems form the core of FMS services that businesses that have larger fleets of vehicles subscribe to optimize their common goals of lowering transportation costs and improving efficiency in moving products to customers.

Fleet management systems (FMS) include various software and hardware tools to provide businesses with data and analytics about vehicles and drivers. The purpose is to improve efficiency, productivity, and decrease non-productive activities. In the near future, a significant part of FMS will be dominated by the fast-growing autonomous vehicle (AV) industry. According to IHS Markit, autonomous vehicle sales will reach 7.4 million in 2040. While the permeation of AV will be slow and not immediate, in 2040, approximately 54% of new vehicle sales will be autonomous. The AV industry is intensely working towards producing state-of-the-art solutions for managing fleets of vehicles that transport people, deliver goods, or are utilized in business fleets for various use-cases. In this work, we study privacy-preserving FMS solutions of fleet operators that employ AVs in their business.

2.1. Traditional Fleet Management Systems

According to reports, traditional fleet management systems cost about $100K-$180K per year, covering a fleet of around 100 vehicles. In addition, additional expenditures, such as costs associated with maintaining and replacing outdated software, infrastructure, and vehicle hardware, are still considerable financial burdens. The rise of autonomous systems has attracted significant attention from businesses. However, costly traditional fleet management systems can constitute significant market entry barriers. Moreover, these cost-induced barriers can be a major disadvantage for start-ups and small businesses due to future growth limitations. Therefore, developing a cost-effective solution that allows businesses to easily afford a fleet management service that can adequately satisfy their specific operational requirements is necessary. The development of new business models that provide on-the-go and pay-as-you-go services is needed for strategic operations to secure a competitive advantage, higher levels of satisfaction, and improve service quality.

Fleet management is a function that allows companies that rely on transportation in business to remove or minimize risks associated with vehicle investment, improving efficiency, productivity, and reducing their overall transportation and staff costs. Fleet management systems are made for managing a large number of vehicles, often leveraged by government or corporate systems. Traditional FMSs have been designed to interconnect a variety of vehicles and mobile assets. These systems provide physical security, information security, lifecycle management, infrastructure support, vehicle tracking, driver behavior monitoring, compliance and reporting, assessment, and misuse prevention. In addition, tiny computers, sensors, actuators, and wireless communication equipment can be integrated and configured for most existing vehicles and mobile assets. Today, it is increasingly necessary for all types of public and private organizations to understand the role of these specialized systems and how they fit into their particular management situations.

2.2. Challenges in Autonomous Vehicle Fleet Management

The challenge here, however, is not just about minimizing the trip time, but it is one of the privacy concerns for the operators as well. Autonomous vehicles, as they journey around the city, pass by other companies and residential areas and collect environmental data. Such data can include location and duration, what is happening at a location, such as loading, uploading, photography, insights through facial and vehicle recognition, etc., and physical attributes such as size, make, passengers, etc. These are a major concern for the privacy of the

competitors and citizens. Hence, without breaching the confidentiality and sensitivity of the trip requestors, the autonomous vehicle fleet management system shall be confidential.

The problems faced by autonomous vehicle (AV) fleet management systems are novel compared to existing fleet management systems for traditional vehicles. Most of the fleet management models are based on simplifying the vehicle routing problem based on the business needs, typically optimizing the longest tour time of transports. While the model of those applications could provide valuable insights, there are many more challenges in autonomous vehicle fleet management models. A company using traditional vehicles for deliveries has well-defined stop points and destinations, fixed pick-up and delivery times, and transportation requests are derived from infrastructure systems like warehouse management systems. As far as autonomous vehicle fleet management is concerned, a vehicle can receive a trip request from any place and from anywhere at any time.

3. Privacy and Security in Fleet Management

The traffic information is considered sensitive and often cannot be disclosed to unauthorized third-party actors. The traffic information stems from a variety of sources, including infrastructure and devices. The vehicle cube statically attaches to a specific vehicle, and the data produced by the vehicle cube and the running applications is stored and transported to fleet management services. The vehicle cubing solution is comprehensive in nature, meaning that it comprises a vehicle information hard and software stack that should be ready to host different autonomous vehicle monitoring applications. Although the autonomous fleets fulfill an important purpose, one can argue that the privacy and security of the IoT solutions is not fully wrestled and taught. More vehicle information may be collected, posing privacy concerns as well.

Vehicular data sources can be both mobile and stationary. LTE-V2V creates an opportunity for autonomous vehicles to communicate directly with each other and exchange information in a more efficient manner than with non-autonomous vehicles. The vehicle information that is required by the Autonomous Vehicle Fleet Managers for managing their fleets includes the current position and speed of the vehicles that are on route, which continuously needs to be harvested from the central traffic system using possibly heavy and frequent applications. We have been motivated by a stakeholder – Siemens – which has expressed their need for traffic management monitoring and ITS solutions services for autonomous driving tests. Their

motivation resides in both the security and privacy of the Autonomous Vehicle Cubes and their applications, as well as in the high costs associated with the management of their complex traffic ecosystem platforms.

3.1. Importance of Privacy in Autonomous Vehicle Operations

The General Data Protection Regulation (GDPR) is considered one of the most comprehensive data protection regulations legislated thus far. It is designed to harmonize the data privacy laws of European Union member states, enforce personal data protection, and address the export of personal data outside the EU and EEA areas. Additionally, different European member states have initiated separate legal texts and regulations to certify the confidentiality and security of privacy information handled during AV operations, such as the German Bundesdatenschutzgesetz (BDSG).

Autonomous vehicle (AV) operations require exhaustive collection of high-resolution digital maps and real-time on-road sensor data for probabilistic perception, localization, planning, and control algorithms. For collective safety assurance and continued/renewed usage of the AV technology platform, data collected by AVs during operations should be aggregated, analyzed, and acted upon using cloud-based Fleet Management Systems (FMS). These FMS, operated by an AV technology provider (or other transportation service provider for non-AV shared fleets), would oversee and dispatch AVs, enable remote assistance, enable proof of safety, reduce HW-SW wear or energy usage, and deliver marketing or transportation-as-a-service use statistics to the operator clientele. However, such AV operator FMS must respect and comply with personal data protection regulations.

3.2. Privacy-Preserving Techniques

In the context of autonomous vehicles, two stakeholders are on the opposite sides of the spectrum when it comes to the willingness to share data. The data provider is an Autonomous Vehicle (AV) operator seeking help from the FMS. The person on the demand side wants to create a service level experience for the owner of each AV (passenger or cargo truck). The FMS cannot see what is happening in the 'physical world' where the data is being created. Privacy becomes relevant because the gap between the physical world and what a software application sees is often filled by data sharing. Furthermore, since passengers are often in motion, data might be shared when the camera-to-face match is not accurate.

A Fleet Management System (FMS) offers a wealth of valuable data for companies. From planning purposes (e.g., the composition of individual routes, load planning, number of required vehicles, dispatch plans), performance monitoring (e.g., the adherence to a schedule) over allowing customers and other involved agents (e.g., government, regulatory agencies) to be updated (e.g., through feeds) up-to charge customers based on the service level. In contrast to a FMS for human drivers, FMS for autonomous vehicles can offer more efficient and effective scheduling and route planning functionalities. However, all software applications integrating autonomic decision making are data-driven. Taking better decisions or solving puzzles fast require better or more data.

4. Existing Solutions and Technologies

Regulatory compliance needs to ensure that all usable data will not be linked to personally identifiable information but can be aggregated to support voluntary industry-knowledge level disclosures of data with respect to vehicle capabilities, measurement, safety, insurance, and related matters. The solution can leverage hardware-backed, encryption-based search protocols that can allow the server to create a query data that won't help in leaking information but rather allow entire dataset column-based searches. They require an organization to run the fleet over, for example, a homomorphic encryption library contag that, in the latter case, can provide end-to-end privacy that guarantees user-provided encrypted input and output be used/generated by secure operators and are that the analogous non-private functionality is the only possible knowledge.

There is no straightforward solution for fleets that need to use utilization data without compromising the operation and privacy of users. Fleet administrators can develop ad hoc solutions to monitor access to the software systems by operators or query wait and queue times. Solutions that could be overlooked include engineers' requests for specific data furnished upon vehicle manufacturer support requests. Anonymizing approaches can be used to provide a software "ghost" operator that requests the data or computes results, and operators agree to communicate their results to the correct operator by using a data protocol that protects final data. However, the development of sophisticated de-anonymization attacks can be avoided using data that is neither compromised nor a server that is linked to the waiting queries through a specific driver identifier.

4.1. Overview of Current Fleet Management Systems

We observed that only one research vehicle included fleet management features. Other research vehicles include either simple call centers or no management modules at all. We conclude that current research vehicles do not address the need for AV fleet management. Consequently, our aim throughout this thesis is to fill this research gap and provide a comprehensive design of AV fleet management with the ability to automate operating AV fleets. To this end, we first overview the state-of-the-art in fleet management systems and look into the actual challenges and specific requirements of autonomous vehicles in the context of fleet management. Specifically, an overall AVFMS architecture must devise an efficient and reliable process to automatically and optimally allocate a task to available AVs in real-time.

FMSs, which were also introduced in Section 2.1.3, provide a suite of management applications to efficiently manage a fleet of vehicles, and they require careful setting up. In FMSs for autonomous vehicles, which are also known as AVFMSs, fleet managers have to cater to additional requirements related to the safety of the passengers and the vehicle, and to the environment. In particular, fleet management algorithms have to carefully balance the time required to wait for new tasks to be assigned, balanced against the time required to optimize task allocation in order to be able to respond to client requests as quickly as possible, and have to work within the constraints associated with the available road network infrastructure, the battery life of the vehicles, and other factors required for the ongoing operation of the vehicle such as a maintenance schedule.

4.2. Privacy-Preserving Technologies in Practice

Homomorphic Cryptosystem—FHE, PHE. Homomorphic cryptosystems are investigated recently in the field of secure multiparty computation. These systems allow users to perform calculations on the data of someone else, and the results will be represented cryptographically without revealing the input information to the service providers, which matches the core concept of privacy-preserving computation. Clothing data to homomorphically encrypted ciphertext can fulfill the secure computation without privacy leakage. In fact, FHE has been applied in the development of the secure outsourcing function, in the case of a large number of PoI explanations in a vehicle's GPS data analysis, and to the processing steps of management systems.

MPC: Secure and scalable GPS tracker. Chaoyue Niu et al. provide an ambitious approach for privacy-preserving GPS localization by utilizing MPC. However, the claim for reducing the

scalability issue has limitations, as MPC lacks native support for secure outsourcing. Instead, operators can deploy other methods such as dummy generating protocols, divide and conquer, and then fuse the result. This will work as long as at least one correct party follows the protocol, which can be further extended into a privacy-preserving grid system for all participatory parties. In summary, MPC is secure and convenient but cannot guarantee scalability in location computing functions for huge data. These limitations present incentives to search for other solutions involving the SMC framework from the existing academic world and industrial technologies.

5. Design and Implementation of a Privacy-Preserving Fleet Management System

We designed a PP-FMS (Privacy-Preserving Fleet Management System) to ensure that no privacy is disclosed to anyone. This eliminates both of the privacy concerns raised in Section 3. Our privacy-preserving fleet management system enables anyone - honest vehicle service agents to make routing decisions for vehicles in real time with low-cost communication. The system ensures that no data is disclosed. While ensuring privacy, the system assigns service request calls to appropriate vehicles. We implemented our system as a programming library using the Anonymous Platform library and applied PP-FMS to solve a group elevator control problem that can be formulated as an SMO (Service Management-Optimization) problem. The experiments demonstrated that PP-FMS was useful in the group elevator task case study for which multi-vehicle routing decisions were needed with mutual privacy between service agents and vehicles, while having a sufficiently small overhead for real-time operations.

5.1. System Architecture

The paper proposes an architecture for privacy-preserving, distributed, and secure fleet management and showcases the system implementation of the proposed architecture with homomorphic encryption and secure multi-party computation. The privacy-preserving vehicle dispatch system for reinforcement learning is practical in real-world scenarios. The proposed vehicle dispatch system can achieve near-optimal performance with a minor impact on data privacy. The results from the open dataset reveal that there is a negligible loss in the system classification accuracy compared to running the vehicle dispatch on clear text data when utilizing homomorphic encryption for inference.

The system implementation of the proposed architecture is demonstrated through a case study utilizing the advanced security and privacy toolkit for securing homomorphic encryption and the secure multi-party computation library for secure empirical risk minimization. From the experimental results, we show that the proposed secure and privacy-preserving vehicle dispatch system performs risk minimization practically and efficiently by securing computation during the fleet management process. In particular, the intelligent vehicle dispatch can enable efficient reinforcement learning-based fleet management.

To address the operational challenges and security risks associated with managing large fleets of autonomous vehicles, the paper proposes an architecture and a platform for privacy-preserving, distributed, and secure fleet management. The special feature of the proposed architecture is that it enables independent parties, such as public transportation authorities and private shared mobility services, to work together to design efficient fleet management algorithms without sacrificing data privacy.

5.2. Key Components and Features

The Video Compression mechanism inside the Data Collector is using standard algorithms supporting at least h.264 and h.265, but it can be extended for many other codecs, some of which are designed to have the ability to specify certain interest region(s). Thus, it is possible to be used for tracking and recording only the object(s) belonging to these region(s).

The main components are described in more detail. The Data Collector is the base input I/O component of the developed privacy-preserving models, which is constantly serving the generated video, LiDAR, and sensor frames. In practice, this model is responsible for creating pre-defined compressed files per time-stamp, which can be collected by the Autonomous Vehicle Operator application(s) in a predefined cadence corresponding to the typical operation environment.

Furthermore, the communication is event-driven, i.e., the flow of communication between all modules is independent of the used policies, making the developed system very hitless and allowing for the deployment of a large number of autonomous vehicles in large-scale applications.

Firstly, the models allow for the insertion of arbitrary sensor types and quantities with direct interfaces to the rest of the system, making it flexible. The implemented relationships between

the models impose proper and sequential pipeline operations without introducing blockers phenomenon, i.e., every process can be unblocked after its specific data preparation stage.

The implemented privacy-preserving fleet management systems are designed to be modular, providing individual input-output (I/O) interfaces, making them compatible with both sensor models and existing centralized fleet management software. The models respect the following features:

6. Evaluation and Performance Metrics

For evaluation of the framework, we conduct simulations based on Detroit and Manhattan maps. The monorail dataset used for the evaluation is created by Monte Carlo simulation of the vehicles' spatio-temporal features (e.g., speed, position) based on the trajectory data of a scheduled monorail. The experimentally derived dataset for performance evaluation is created based on the experimentally collected trajectory and communication data. For the datasets, both Detroit and Manhattan maps and also multiple periods (e.g., Monday, Weekend) were considered to provide different spatio-temporal patterns. Based on the experimentally collected wireless communication data, the communication quality can be recorded for different locations of the area.

For each of these base datasets, we calculate the corresponding risk. Additionally, we calculate the number of vehicles in collection V per period s. We then report the following privacy metrics for the base datasets in order of personal information type (PII type): average k-anonymity, average Laplace noise, and number of vehicles in collection V. The purpose of listing the number of vehicles in collection V is not to measure privacy but to provide context and perspective into the risk and net effects from various privacy levels.

- Define this, define that. - As X of autonomous vehicles equipped with Y autonomous vehicles by a period S. - For instance, X could be the number of vehicles contributing data within a one-hour interval, or the total number of vehicles that contribute data for a certain route, such as downtown to the airport. - By date, this could be the number of vehicles contributing data within the specified date range of the study. - Period could be the length of the data collection period. - We characterize V, which is the collection of vehicles, using the following method: V = f(y, z). - Y indicates that a vehicle is an autonomous vehicle while z determines the manufacturer of the autonomous vehicle.

To evaluate our proposed privacy-preserving data sharing framework quantitatively, we define the following performance metrics:

6.1. Privacy Metrics

The privacy metric of absolute error rate evaluates the degree that the output of a frequency estimation query or other stochastic user-specific queries deviate from their true values. In a FMS, stochastic server-state metrics on "Customers" requests and trip aggregation requests quantify driver behavior statistics, while stochastic vehicle metrics on battery state data, customer location requests and final destination location of autonomous vehicles reflect system dynamics. Public statistics based on these server state and vehicle state metrics are of the particular interest of AV operators, who only request these information to plan policies or demand optimal trip allocation in an FMS. We design tree-based sensitivity-limited algorithms to protect absolute error rate privacy in query processing. They compute the sensitivities of valid/possible data structures about the query from uncertain data departures of each driver, and replace the final intermixed default data-driven responses with limited tree-depth crafted statically consistent data structures to fully protect against driver identifiers and achieve absolute error rates at their sensitivity limits, while adding indistinguishable noise.

We first introduce the privacy metrics used to evaluate our schemes. The privacy metrics adopted focus on the privacy of associated driver IDs and spatial locations and provide differential privacy against these IDs. These metrics are particularly important to develop the application of Privacy-Preserving Fleet Management Systems (Privacy-Preserving FMS) for the autonomous vehicle operators, as the information on the drivers and their spatial locations are commercially sensitive assets to them. We choose absolute error rate and clique sensitivity as differentially private metrics to achieve the aforementioned privacy against driver IDs. For spatial locations, neighboring relations, in both adjacent and vicinity senses, are defined following the work in to support users' queries on differentially private access patterns.

6.2. Security Metrics

Evaluation is an essential aspect of any system, especially for security and privacy-preserving systems. The global moral in the practice of security systems includes two principles: verify security beforehand and accept no information in preference of probability over reliability. In

this section, we discuss how many of the existing security metrics apply to the unique aspects of the privacy-preserving fleet management systems, specifically the data aggregation. We adapt Bishop's Security Quality and Systemic Assurance (SQSA) model, which provides a comprehensive set of quantitative security metrics, and Anderson's Expectation-Principle based security metrics. We illustrate the proposed privacy-preserving fleet management systems using the perspectives of confidentiality, availability, authentication, integrity, and non-repudiation to evaluate the overall security requirements based on impact, likelihood, and costs.

Security metrics for entire vehicular networks are an emerging research area. In this section, we discuss existing security metrics proposed in the literature and depict how to apply security metrics to PPFMS for the evaluation of the current work. We use impact and likelihood provided by the Transportation Security Administration (TSA) and Southwest Freeway website to quantify the security metrics. Given confidentiality issues, automobile manufacturers and service providers seldom furnish the number of cases, specifically the number of attacks, breakthroughs after the attack, and the time period to detect the attack, which illuminate the severity and cost associated with operating intelligent transportation systems. As we have an in-depth understanding of the operation of many intelligent transportation systems, we apply a number of listed assumptions to provide the rough estimate required for applying many of the quantitative security metrics measures.

7. Case Studies and Use Cases

The ARSI use case deployments look to provide privacy-preserving fleet management services to other autonomous vehicle operators. The first use case that is relevant to ARSI and is currently being installed as of the publication of this document is a use case with a partner. This use case shows the original design concept of the ARSI solution. However, the data privacy layer alone can change the revenue model for BCM partners and utilize the solution for data sales. This offers ARSI data partners a competitive advantage if ARSI is able to reduce the friction associated with the execution of security protocols.

With ARSI's success with their privacy-enhanced ridesharing app, they opened an unprecedented opportunity to provide fleet management capabilities for other autonomous vehicle operators. These opportunities do not stop at ride-sharing vehicles; there are a host of other vehicle companies in the Autonomous, Connected, Electric, and Shared (ACES) space

that have similar logistics and dispatching issues that require management. It is these partners that are discussed as the ARSI use cases and case studies. The use case discussion begins with a review of how ARSI is deployed in the current scenario and what that future vision looks like.

7.1. Real-World Implementations

Conclusion Ours are some of the first privacy-preserving, secure data analysis that are powerful enough to encourage analysts to "work in the clear" and that are specific to the aggregate data about vehicles and roads. With the ongoing proliferation of sensor-laden vehicles, including automobiles, buses, trucks, taxis, and autonomous vehicles, we expect the use cases and challenges to increase significantly, further enabling proprietary and gaming behaviors that inhibit the deployment of technology that delivers large societal benefits.

Separately, the deployment of a privacy-preserving robust optimization in a customer-sponsored optimization, to protect proprietary load, truck, customer, delay, and route data of trucking industry participants that lead to the delivery of major societal benefits.

The tools for privacy-preserving and secure data analysis that we present in this paper are general across many domains and, by design, allow analysts to legitimately derive heuristic benefits from using privacy-preserving tools. Nevertheless, we have two illustrative implementations that are specific to the autonomous vehicle domain. For the first tool, generated helpers, we provide that an iOS fleet application would periodically generate helper data and post it to the server.

7.2. Success Stories and Lessons Learned

Also, with privacy-preserving fleet management in mind, a benchmarking evaluation methodology has been built to assist the selection of suitable PPAD sharing schemes. This way, the proposed methodology consists of an in-depth questionnaire and a multifaceted benchmark structure that allows a rigorous comparison of existing and novel techniques. Using this evaluation framework, the status of the art of privacy-aware route information sharing has been presented, and the performance of the proposed privacy-preserving traffic management has been estimated. On the other hand, a lab evaluation has been carried out for privacy-preserving access to route information, based on the performance and security of the

current implementation that has been carried out. These have only been evaluated in terms of runtime and communication load for realistic backbone network scenarios.

This chapter has presented two different PPAD sharing schemes: one based on the use of GPDT able to generate a finite set of secret shared distance and time coefficients for polynomial projection, and the other one based on the use of GPTTS able to generate a finite set of secret shared time coefficients for polynomial projection. Examining the PPAD sharing schemes in the light of our architectural framework, we have highlighted that, in both sharing schemes, the ASRS responsible for generating the shared counterparts have been represented through distinct ASR building blocks. Both PPAD sharing schemes have been constructed in a layered fashion, conceptually reusing the cryptographic technology available to implement each level and compositionally reusing the ASRS represented in our architectural framework.

8. Challenges and Future Directions

The chapter is organized as follows: the next section presents the context and objectives of the work. Section 8.2 presents recent works on similar tasks in the literature. Section 8.3 outlines the datasets used throughout this work and introduces the concepts to be considered, as features on which to perform the task. The novel Privacy-Preserving Fleet Management System for Behavior-Based Insurance methodologies are depicted in Section 8.4 and 8.5, respectively. In Section 8.6, a case study focuses on a drowsy driving risk estimation task. Section 8.7 presents the conclusions.

In this chapter, three cloud-based data mining methods are presented which differ in the stage and structure of the mining process they are designed for. The first method supports the identification of operational knowledge from fleet databases. The second method finds complex patterns spanning several interdependent data streams with multi-scale patterns. The third method characterizes unusual operational states of fleets in real-time based on multi-dimensional concepts. The most challenging part of real-world applications based on the proposed data mining technology is the data pretreatment process which has to provide valuable mining cases. Additionally, the high adaptability of the several parameter settings to the idiosyncrasies of mining tasks is challenging as well as in relation to the multi-scale, interdependent nature of driving data. The presented methods are successfully applied to operate, driver, and car data in real-world applications.

8.1. Emerging Technologies

On the goods and logistics aspect, in addition to autonomous vehicles, enabled by standardization bodies, such as the Institute of Electrical and Electronics Engineers Standard Association (IEEE-SA), it will set up wireless data exchange networks and cyber-identity services to support business demand. In the foundation period, vehicles must exchange data to support more vehicles that allow them to operate in the same area or even on the same road. CPAS authorities require data from all vehicles operating in their areas, to ensure the safety of other services and the safety and convenience of road users, traffic management agencies, infrastructure operators, and other categories of business. Additionally, operators need a reliable and durable method of managing the sudden failure of service requests, fleet availability, and operational support. At the same time, the significant use of 'living' crowd management applications is developing beyond the emergency system phase related to data and service functions. Data protection needs to be developed to protect user data from malicious or unintentional leaks while the crowd management system experiences and uses the high data volume characteristics required for functions related to daily operations and normal business growth. Finally, the architecture of the fleet management system must be able to contain growth without generating significant ascending costs.

The increasing access to emerging technologies is the driving force behind digital transformation in a broad spectrum of industries and businesses, and will also play a critical role in the future of the transportation industry. In the last several years, autonomous vehicle technology has developed rapidly, resulting in the commercial operations of level 4 autonomous vehicle services in a few cities, and plans have been proposed to use them in almost all major cities in the world. The development of 5G, artificial intelligence, and cyber-physical technology, in combination with autonomous vehicles, is expected to revolutionize modern urban and suburban life. The elevated reliability expected from the time of demand for very high-frequency services and low connection latencies, forecast to be two of the key enabling components for the launch and growth of the next level of autonomous service without drivers. Additionally, the use of high-precision positioning, ultra-precision mapping, real-time planning based on artificial intelligence, and related delay technologies are expected to enable safe and efficient operation.

8.2. Regulatory and Compliance Issues

Furthermore, with the changing landscape of data privacy, there will undoubtedly be new regulations with which we must comply that have not yet been considered. Therefore, the fleet management system should be flexible enough that the system can adapt to new regulations with ease. Providing solutions that enable data privacy protection at multiple levels would enable broad adoption of autonomous vehicles as well as other smart city and cooperative robotics applications. Ultimately, these systems will be widely accepted if they overcome the inertia of change and mitigate privacy concerns.

Fleet management systems should also include features to allow the system to be adaptable to align with future data privacy regulations that are currently in consideration and future regulations not yet considered. For example, autonomous vehicles are designed to be able to operate in many different cities in different states or countries; therefore, fleet management systems would need to be able to handle these different privacy requirements. In addition to being usable in these different cities, fleet management should also be usable in different countries. For example, Europe and the United States have differing regulations governing storage and transmission of images in the presence of people. The system should be able to restrict what data is stored or transmitted to meet the differing privacy requirements when vehicles are operating in different countries. Finally, the fleet management system should be able to limit what video data is accessed or the retention of data based on privacy policies set by municipal contractors if the vehicles are deployed through partnerships like Lyft.

9. Conclusion and Future Work

The proposed privacy-preserving solutions have shown significant effectiveness in practice, and the performance overhead introduced by these solutions is acceptable given the performance benefits from the efficiency improvements and the ability to collect private data using the FMS infrastructure. Furthermore, although the privacy-preserving algorithm uses advanced cryptographic techniques to protect data, the performance overhead of these techniques is actually quite acceptable under realistic assumptions. Our proposed approach is also very flexible and can be extended into several relatively less often studied but quite interesting areas in the privacy, security, and trustworthiness arena.

This paper presents a comprehensive privacy, security, and trustworthiness study of a practical fleet management system (FMS) designed for operators of autonomous vehicles. Using a collection of real-world data and practical usage scenarios, we identify several critical

information leakages and the causes of these problems. We then propose a collection of privacy-preserving algorithms to reduce the amount of private information collected during data collection and real-time operation. We conducted a series of evaluations to demonstrate the effectiveness and efficiency of our proposed solutions.

9.1. Summary of Key Findings

Key points: In this chapter, we examined privacy concerns associated with location data collected by AVs, due to the use of underlying matching techniques. Our study showed that AV operators are themselves concerned about equality in location information. At the same time, they are resistant to the process of aggregating and adding noise to location tracking information. In spite of the security advantages of the MVP privacy solution, an AV operator could implement MVP very cheaply. To the best of our knowledge, this is the first examination of how the main AV stakeholders view the privacy trade-offs and desired policies of their stakeholders. Data privacy and data sharing practices can shape a city's mobility service. Consequently, we argue that our theoretical and experimental privacy-preserving fleet management system can alleviate some of these privacy social concerns of AV deployment, required by different stakeholders while preserving the utility of the data.

9.2. Recommendations for Future Research

In the above, we discussed a few privacy-preserving fleet management systems for ride-hailing autonomous vehicle operators. Researchers should also look at similar systems for different autonomous vehicle operators like mobility-on-demand service autonomous vehicle operators, electric vehicle charging fleets, automated repair fleets, automated delivery fleets, automated shuttle fleets, etc. Finally, we believe that offering additional privacy protection to the riders can be a unique selling point for autonomous vehicle fleet operators. Hence, we believe that more research should be conducted to bring more privacy protection-related features to fleet management systems, which can unnecessarily open up the riders.

In this chapter, we discussed several privacy-protection technologies that fleet management systems can use to achieve privacy preservation for riders. There are still several pressing issues. Some of the key privacy-protection technologies we discussed are based on full-time audits by third parties. As we want to reduce the power the third parties have in such settings, and the cost incurred by more audits, we need to further study the possibility of using secret

sharing to rid the full-time audit requirement for various schemes. Other current solutions also need to be implemented and subjected to real-world data to see if the data will reflect the true performance of these solutions. Finally, some of the solutions need to use realistic operations for scalability and efficiency consideration.

10. References

1. S. Choudhury, R. R. Choudhury, A. Kumar, and K. R. K. Kumar, "Privacy-preserving fleet management system using blockchain technology," in 2019 IEEE 23rd International Conference on Computer Supported Cooperative Work in Design (CSCWD), 2019, pp. 418-423.

2. N. Alhakbani, A. Mahmood, and R. Kharel, "Privacy-preserving data collection in vehicular ad-hoc networks using blockchain," in 2020 IEEE 45th Conference on Local Computer Networks (LCN), 2020, pp. 342-345.

3. Tatineni, Sumanth. "Enhancing Fraud Detection in Financial Transactions using Machine Learning and Blockchain." *International Journal of Information Technology and Management Information Systems (IJITMIS)* 11.1 (2020): 8-15.

4. Shaik, Mahammad, et al. "Enhancing User Privacy in Decentralized Identity Management: A Comparative Analysis of Zero-Knowledge Proofs and Anonymization Techniques on Blockchain Infrastructures." *Journal of Science & Technology*1.1 (2020): 193-218.

5. Vemoori, Vamsi. "Comparative Assessment of Technological Advancements in Autonomous Vehicles, Electric Vehicles, and Hybrid Vehicles vis-à-vis Manual Vehicles: A Multi-Criteria Analysis Considering Environmental Sustainability, Economic Feasibility, and Regulatory Frameworks." *Journal of Artificial Intelligence Research* 1.1 (2021): 66-98.

6. Z. Chen, W. Wang, and Q. Liu, "A survey of privacy-preserving data aggregation in vehicular ad-hoc networks," in 2017 IEEE 19th International Conference on High Performance Computing and Communications; IEEE 15th International Conference

on Smart City; IEEE 3rd International Conference on Data Science and Systems (HPCC/SmartCity/DSS), 2017, pp. 458-463.

7. A. Abuarqoub, M. G. Jaatun, and T. S. Hamadneh, "Privacy-preserving data aggregation for connected vehicles: Challenges and solutions," in 2018 IEEE International Conference on Communications (ICC), 2018, pp. 1-6.
8. J. Li, K. He, and K. Bian, "Privacy-preserving data aggregation scheme in VANET," in 2019 IEEE International Conference on Big Data (Big Data), 2019, pp. 2923-2928.
9. X. Wu, H. Lin, and J. Shen, "Privacy-preserving data collection in connected vehicles: A blockchain-based approach," in 2018 IEEE International Conference on Communications (ICC), 2018, pp. 1-6.
10. Y. Zhang, X. Chen, and Y. He, "Privacy-preserving data sharing framework for connected vehicles," in 2018 IEEE International Conference on Communications (ICC), 2018, pp. 1-6.
11. D. Soni, D. Bhatia, and M. Dave, "A survey on privacy preserving techniques in VANETs," in 2018 IEEE International Conference on Smart Technologies and Management for Computing, Communication, Controls, Energy and Materials (ICSTM), 2018, pp. 156-161.
12. S. K. S. Gupta and R. R. Pal, "A privacy-preserving model for secure communication in Internet of Vehicles (IoV)," in 2018 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS), 2018, pp. 1-6.
13. X. Wang, Z. Xu, and X. Lin, "Privacy-preserving data aggregation in vehicular ad-hoc networks: A survey," in 2019 IEEE International Conference on Smart Internet of Things (SmartIoT), 2019, pp. 179-184.
14. Z. Li, X. Lu, and S. Maharjan, "Privacy-preserving data sharing for autonomous vehicles using blockchain technology," in 2020 IEEE International Conference on Communications (ICC), 2020, pp. 1-6.

15. H. Alsubhi, H. Alharthi, and A. Al-Dhelaan, "Privacy-preserving data aggregation in vehicular ad hoc networks using blockchain," in 2018 IEEE/ACS 15th International Conference on Computer Systems and Applications (AICCSA), 2018, pp. 1-7.

16. Z. Tang, Z. Ma, and Y. Liu, "A privacy-preserving data sharing framework for vehicular ad hoc networks," in 2019 IEEE International Conference on Big Data (Big Data), 2019, pp. 5134-5139.

17. K. Kumar, R. R. Choudhury, and S. Choudhury, "Blockchain-based privacy-preserving data sharing framework for connected vehicles," in 2019 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS), 2019, pp. 1-6.

18. W. Wang, Z. Chen, and Q. Liu, "Privacy-preserving data aggregation in vehicular ad-hoc networks: A survey," in 2018 IEEE 19th International Conference on High Performance Computing and Communications; IEEE 15th International Conference on Smart City; IEEE 3rd International Conference on Data Science and Systems (HPCC/SmartCity/DSS), 2018, pp. 1041-1046.

19. Y. Zhang, X. Chen, and Y. He, "Privacy-preserving data sharing framework for vehicular networks," in 2017 IEEE 86th Vehicular Technology Conference (VTC-Fall), 2017, pp. 1-5.

20. S. K. S. Gupta and R. R. Pal, "A privacy-preserving data sharing framework for Internet of Vehicles (IoV)," in 2019 IEEE International Conference on Innovative Research and Development (ICIRD), 2019, pp. 1-6.

21. A. Abuarqoub, M. G. Jaatun, and T. S. Hamadneh, "Privacy-preserving data sharing framework for connected vehicles: Challenges and solutions," in 2018 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS), 2018, pp. 1-6.