Privacy-Preserving Location-based Services for Autonomous Vehicle Navigation

By Dr. Hirokazu Takahashi

Associate Professor of Mechanical Engineering, Kyoto University, Japan

1. Introduction

In the field of autonomous driving, innovative location-based services (LBSs) with respect to real-time dynamic verification and correction assistance are becoming increasingly important, which could assist a vehicle in navigating through an urban environment safely and efficiently [1]. However, vulnerabilities in fundamental communication processes can lead to a wide range of dangerous attacks on the vehicle and threaten personal data privacy, and at present, no work has addressed location privacy for these data query mechanisms, especially in a vehicle-to-everything (V2X) environment. We consider this to be a significant challenge. In a vehicular ad-hoc network (VANET) architecture, vehicles communicate with other vehicles or roadside units (RSUs) over wireless channels and, to some extent, expose themselves to a set of security vulnerabilities. Therefore, they are not suitable for transmitting the user's real-time location to the destination server.

Three types of secure location-based data query schemes exist: pseudonyms, location cloaking, and cryptographic techniques [2]. Pseudonym-based solutions disrupt the connection between vehicle identities and locations but may still disclose data query locations. Location cloaking introduces uncertainty or error into location information, but may not guarantee enough users in the neighborhood or high query accuracy. Cryptographic techniques effectively preserve query accuracy and location privacy. In this paper, we propose a privacy-preserving range query (PPRQ) scheme for the autonomous vehicle navigation scenario and provide security analysis and performance evaluation. The proposed PPRQ scheme supports data query for locations in both the User and Data models and achieves the tradeoff between location privacy and data query efficiency, by providing slider window privacy-preserving functions on the road network map. It preserves the location privacy while enabling efficient data query. The proposed real-time privacy-preserving range query scheme

is suitable for autonomous vehicle navigation and has great potential to be extended to other privacy-preserving data query schemes and to promote the development of privacy-preserving location-based services [3].

1.1. Background and Motivation

Privacy can be described as the protection, control, and confidentiality of information and data, while confidentiality refers to the protection of the internal state of the user like his location. In the remaining part of the citation, the term privacy-preserving application is used to indicate a location-based service (LBS) which does not require the user location, nor should this information be inferred by the remaining user information. An alternative to offloading application to external servers as the only way to protect location information is to use the mechanism called Trusted Computing [4]. This international standard provides a root of trust for the user. Since it is situated inside the consumer platform, it allows the platform to restrict the root access to the trusted zone. We also have to emphasize that the external disconnection will also increase the security of the application since many security weaknesses come from uncontrolled execution in the misconfigured network, and remote servers in the case offline execute become more secure.

In this section, we provide background and motivation for our study. Dynamic geolocalised services based on global navigation satellite systems (GNSS) are the most promising for vehicle navigation and advanced driver assistance system (ADAS). Disconnection from the GNSS can occur during autonomous vehicle navigation. Different situations can cause unavailability of GNSS signals, e.g., urban environments, underground architectures, and interference. The problem of privacy can also be considered, and is another important aspect of localization systems [1].

1.2. Research Objectives

"On the other hand, another approach in these two issues is to focus on the effect of these vehicle locations on each other in the dynamic form. The drawbacks of these studies mainly constitute the need to design the service structure, which is not efficient when considering the compatibility with its current location and thus makes high-speed changes regarding the communication points of the vehicle. This study focuses on the privacy preserving (PP) approach without giving the structure of a service organization that must be provided stably. For this aim, the authors investigate which current location should be hidden and which other

unexpected location should be revealed in a periodic service such as taxi services after passive and active clustering of unexpected locations when privacy requirements in the area are new and/or removed, respectively."

[5] "Autonomous vehicles need to exchange their navigation information and find where they are heading to from the services provided in the environment. These location-related information collaborations could result in privacy violations because someone could track and attempt to infringe on vehicles. Thus, location privacy issue needs to be resolved.. For this purpose, the location cloaking technique has been studied to protect the location privacy of vehicles. Each vehicle in the environment is included in cloaking region to reduce the influence of their locations. These studies have been mainly performed in the static form during driving operation by giving the problem of reducing service quality and security to the environment for mental satisfaction."

1.3. Scope and Limitations

Cloud-based connected cars accompany several advantages such as adaptable business model strategy, monitoring the usage of resources in real-time resulting in the quality of experience (QoE) optimization and effective real-time traffic and road crash information, which can benefit vehicle-arga-based insurance systems. However, regular driving routes of vehicles are tracked, and privacy concerns are raised. In some cases, vehicles in a network exchange their pseudonyms dynamically to increase the difficulty to track their real identity and trajectory by an attacker. Privacy issues in the Orwell's Big Brother scenario envisioned by 1984 can be effectively protected while both mobile apps and loation-based online services may give out personal infomration that people want to keep secret. Various algorithms and protocols such as Enhanced Privacy Preserving in IoT Navigation Guiding (EPPING) or k-Graph nearest neighbor query (kGNN), LinkedList based (K-Anonymous Location Based Services) LLB, parking services (Parking Arduino-Based Framework with Location Masking PALM) and differential privacy algorithm have been proposed for protecting the privacy in the IoT environments. The algorithms or protocols have their own advantages or disadvantages such as losing the road network information, increasing the volume of applications and exchanging locations among a trusted server, leading to a single point of failure.

[6], [7] The transportation and vehicle navigation industry are actively engaged with the development of autonomous vehicles and connected car systems. Autonomous vehicles are

generally described as highly efficient systems equipped with advanced real-time sensing and decision-making capabilities, which can drive without human input. Intelligent sections of road equipped with various sets of sensors, road-side units (RSUs), and battery-powered sensors are generally called as smart roads or smart cities. Environmental, communication, and security issues are linked with developing sustainable and secure self-driving cars. Cloud-based and vehicle-based services can gather, analyze, and use a large number of customers' data such as environmental and traffic information, which may not be ethically used supported by privacy concerns. This paper presents a review of the state-of-the-art of privacy-preserving location-based services in smart cities, focusing on the vehicle industry. The concept of privacy and a review of location privacy, the characteristics of various types of location-based applications, and reviews of vehicular networking are summarized in connected car systems. We also present a series of privacy-preserving location-based solutions using trusted third parties, pseudonym exchange, and privacy-preserving coordinate transformation in cloud or fog computing environments enhanced with side channel attack-resistant protected network channels. The green and secure communications research area, which includes energy-efficient communications, is additionally discussed.

2. Autonomous Vehicle Navigation

In the vehicular network, According to several environmental factors, a vehicle can send warnings and recommendations to other vehicles. A vehicle can adjust its speed and direction according to the received messages to maintain the traffic safety [8]. Apart from all of these, the real-time and on-time transmission of official instructions from local control centers to these vehicles can be done properly using the upcoming V2X services.Offline/online support and new technologies encouragement will help the successful deployment of autonomous/self-government driving. These capabilities will increase commercial traffic by 35% during the peak period and during the off-peak period by 80%, by reducing total system travel time. By adopting autonomous driving technology, it will be possible to save 2 minutes per passengers per day from the urban planning.

Autonomous vehicle navigation is becoming an increasingly important field of study [9]. Accurate and reliable positioning information is indispensable for self-driving vehicles. GNSS (Global Navigation Satellite System) is the most commonly used technology in outdoor positioning. With the use of GNSS, the longitude and latitude information can be directly

acquired based on the signal received from global navigation satellites. This is important for autonomous vehicles. However, GNSS performance can be affected in many ways, including multipath signal, shading, ionosphere and troposphere delay, signal jamming and spoofing, and so on. In the future, auto-vehicles will share the roads with human-driven ones. Road network planning is necessary for some urban roads with complex environments and high population density, especially for emergency and abnormal situations. There are some other organic interferers present in urban areas which affect the performance of autonomous vehicles.

2.1. Challenges and Opportunities

Nevertheless, in the last few years, several research articles have called into question the misinformation potentially provided by non-colluding agents to the core, i.e., the real vehicles instantiating the non-colluding agent. In other words, since ASNs use computations related only to their own sensors and other potentially privacy-relevant decision-makers (who solve a specific information privacy-preserving task), they can be attacked by malicious and misbehaving agents, i.e., some agents that although asked to solve a certain privacy-preserving task, answer with yet verisimilar, but misleading, as well as sometimes completely redirected (e.g., towards a fake target value), answers [2]. Unfortunately, even more lastly, it has been demonstrated that not purely malicious, but also random agents, passing near the core—being temporarily correctly available in the neighborhoods of the core—can provide yet misleading, privacy-violating information to it.

In shared-data environments, privacy-preserving routing and map-matching protocols are receiving increasing attention from the research community. In such event, researchers are discussing the efforts of incorporating these schemes as building blocks within privacy-preserving LBS services and map-matching frameworks. Besides privacy, safety is another important concern for autonomous vehicles [10]. Several recent research projects have addressed the issue of safety in connected autonomous vehicles; however, a robust security policy to protect the data privacy of the user is still an open challenge. To this end, in this article, we aim to propose a framework that bridges the gap between privacy-preserving LBS navigation and the security policy of autonomous navigation in the connected vehicle ecosystem.

2.2. State-of-the-Art Technologies

Finding the trade-offs between data utility and location privacy and the related issues has become a major concern among researchers in this field, as suggested in [11] and [12]. It is crucial to select representative papers that highlight the main concepts of research within the survey subject. An exhaustive citation of available papers can be overwhelming for the audience and can devalue the review: some papers may then seem more important than others simply because they have been referenced more frequently. Select a few papers that demonstrate well the main techniques in the area of location data publishing for LBSs and privacy preservation techniques. This will include surveys and comprehensive studies that present a conte-xt for the state of the art in location privacy.

Location-based services (LBSs) have become indispensable in various applications, including virtual navigation and location information sharing [6]. In many scenarios, the service server needs to learn a precise user location (e.g., GPS coordinates). However, the precise user's location is protection-sensitive private information, and many LBS users are not willing to share it for security and privacy reasons. In addition, LBS wireless sensor networks (WSNs) have also become ubiquitous in IoTs, where sensor networks are deployed in an area and the sensor nodes are partitioned into different groups at different times under dynamic sensor groupings or node organizations for different sensing tasks and service computation, including clustering, sleep scheduling, access control, etc., and the sensor node groups need to guarantee the effective utility provision for these tasks in mission-critical missions, which may require data privacy and security provisions.

3. Location-based Services (LBS)

Several LBS technologies are available that provide the users with map-based routing features. These technologies use a map service and a path service for this end. The map service provides the map visualization to the user, including the user's current location as well as other possible users that they may want to meet during the route planning. In some cases, historical speed information may also influence the visualization. The speed map service is followed by the Path Service functionality that calculates the actual route (taking into account the user preferences/warnings on different types of routes/roads) using the major street network. Most of the current AVs and road traffic with priority that is described in the literature should be incorporated into these technologies. These technologies might also be

able to visualize and help to navigate around non-authoritative data from other vehicles. An errand-run route is different when compared to a regular route because it may include extra stops at different points of interest and it is made subject to priorities. Several works in the literature have discussed these practical aspects of integrating traditional errand-run services with AVs. We discuss some of these mechanisms in this chapter. However, note that these mechanisms still provide the server with all possible locations that the AV wants to visit as well as the vehicle it is using.

Location-based services (LBS) involve services that provide the user with personalized information or content based on their location [13]. Autonomous vehicles, smartphones, smartwatches, and other wearables are amongst the devices that utilize different LBS applications for routing, errand-runs, fitness, and socializing. LBSs have seen an explosive growth in demand that can be attributed to the added convenience, ease-of-use and efficiency they offer to the user [12]. The user also benefits from the fact that these services are available at all hours every day of the week. Predictions have underlined the fact that the surge in people using LBS applications will continue. This article discusses how LBSs may be integrated with autonomous vehicles to enhance driving experience and provide extra services to the users. In this chapter, we start by describing and discussing different LBS services that may be used by an autonomous vehicle (AV). This includes routing services, errand-run services, fitness services, and sociability services. When discussing routing services, we focus on the fact that route planning for AVs has a different connotation when compared to non-AVs, since they often need to communicate with a traffic management system. Similarly, we make a case for errand-run LBSs specifically for autonomous vehicles, show a number of related scenarios and possible extensions, discuss different fitness-related LBSs that the user or a group of users may use during a trip in an autonomous vehicle, describe how autonomous vehicles can act as an introduction point for smartphone/online-based LBS users and also discuss the influence of the LBS on the vehicle control system [14].

3.1. Overview and Applications

Autonomous vehicles navigation or broadly location-based services are widely used and involved to improve road security and better vehicle driving experiences. As an instance, GLObal NAvigation Satellite System provides real-time relative navigation solutions to a network of ground-sited GNSS receivers without inter-recipient (auto-) correlation, through

low-intrusive and flexible change of the reference receiver, with no need of data communication between the remote and the reference stations. Two innovative collaborations are shown with GNSS remote sensing MiniRAE and awareness of the work based on reflection of radar signals (TRL between 4 and 6 stopped). The results are very promising and road safety is going to be significantly improved. Nowadays, the location-based services are seeking preciseness in different ambient scenarios. This work appears as pioneering atmosphere self-sufficiency for the location-based services to go out of some of the recurring lots in the cloud to take a sample sustainable innovation to avoid the simple GPS system. The solution does also constitute a mobile within the civilian and fighting free information technology close to Smart Health and Safety Services. The introduction of a dedicated polarization filter on vehicle's camera enables robust cracking of the weak code provided by the NAO rfid tag. Finally, the off-line attacks concentrate on cracking the NAO rfid tag weak code blob by using an unsupervised machine learning technique. The main message is integrating road pricing through a central road pricing entity with Navigation of Autonomous Vehicles in a city, available in discounted packages, we call them Pay as you GO, and others based on a monthly/annual subscription like Paying KNOW (Know Numbers of kiloWatt).

[13] Autonomous vehicles navigation or broadly location-based services are widely used and involved to improve road safety and better vehicle driving experiences. For instance, navigation services can use real-time traffic information provided by an intelligent traffic system in order to optimize route planning and vehicle control [15]. Automated guides rely on accurate localization to guarantee user security through Command and Control of Cruise Missile Systems. Electromagnetic wave signals poses a limitation to the system precision. Furthermore, during the times of relative peacefulness, localization is done using the GPS infrastructure. However in case of a need for activating the previous mentioned it should be a man local actuator, meaning opening the command box and insert inside it a lead battery. The present invention is used for respect of this limitation. Once a vehicle reaches a zone without GPS signals the system helps the vehicle to determine the current location with accuracy comparable with traditional installations. In present, the localization using technology of Global Navigation Satellite System is used for a lot of applications. In the same stream of causal decision making, ADS are motivated to have an accurate and energy efficient GNSS receiver, also has requested relative to the nongovernmental sector of traffic and civil domain [16]. Contemporary applications use Cloud-based workflows and are crossing

addressable GPS/JPS, Multi-GNSS Reflectometry, with VGSS and Google-Maps to address current algorithms for spoting innovative options.

3.2. Privacy Concerns in LBS

The main way to preserve location privacy in LBS is to not reveal the accurate location of the user. Many dummy-based techniques can achieve location privacy and are quite different in their privacy-policy maintenance and queries. Users' query locations are also a significant factor in these query processes. Search Me If You Can: Privacy-Preserving Location Query Service is a state-of-the-art survey that gives significant implications to this case study. The technique proposed by the PLQP authors is built upon earlier works, and unlike others, not designed to protect one single user's location query. This survey paper investigates the problems and significance of preserving location privacy and current PLQP techniques in detail.

Location-based services (LBS) are used to support many important functionalities in approximately 65% of the top 100 smartphone apps. One major application of LBS that is often being discussed in recent literature is the navigation of autonomous vehicles. In current autonomous vehicles, the onboard systems app predicts the route based on the global map and traffic information. In contrast, the proposed system in this case study aims at using onboard systems to get high-level navigation instructions and utilize LBS to plan the low-level part of the route. This configuration offers several privacy benefits that are detailed in: Section 3.1, while balancing the privacy protections and performance costs inherent in different techniques; enforced over the public location-based services (LBS) provided by our commercial partners, such as Google Directions API: the reference is the most precise concluding URL of the prediction pipeline provided to the client app for visualization.

[17] [18]

4. Privacy-Preserving Techniques

There are mainly pseudonymous techniques used to protect users' location privacy. These techniques can be divided into three categories based on their application domains: collaborative applications, single-server applications, and P2P (peer-to-peer) applications. Some service requests may lead to deductions regarding the user's private information through a longitudinal analysis or a mixture of multiple service requests. Service requests are therefore timed and mixed such that an adversary cannot be certain whether a request is from

the user being traced, even though the user is being traced. To use caching mechanisms and maintain extra communication overhead for obtaining location privacy and processing data query, both cache-based and cache-free location privacy protection mechanisms are proposed. The scheme of caching privacy protection implements more server storage overhead. Caching schemes on the client's side may incur significant latency for being unable to determine a proper time to request ciphered data.

[17] In the literature, privacy-preserving techniques are broadly categorized into three types: pseudonyms, location cloaking, and cryptographic techniques. In pseudonym-based solutions, vehicles connect with different identities to disrupt the connection between vehicle identities and their locations. Unfortunately, this voluntary behavior may lead to privacy revelation risks [2]. Location cloaking works by introducing uncertain locations to prevent exact participant locations. Cryptographic techniques allow participating vehicles to preserve data query accuracy and their location privacy.

4.1. Cryptography and Secure Multiparty Computation

Compactness of messages exchanged in the cloudless and trustless VANETs has a specific impact in privacy issues, therefore resulting this into extra-constraint cloudy and non-trusted sensor and VEC management in above comparison context [19]. We also should consider to "say yes to privacy" and to the attacker: Reasons like following: The non-biased state-Belief-based probabilistically reasoned position of the attacker can be very well RAVEly corrupted and PROCedurally biased if there is available superfluous position by the Mechanism-based superfluous particularity spreading, i.e., by the Mechanism-based superfluous case spreading (MSSCS). This is achieved if the superfluous (dummy) candidate sensor, which detected simultaneously the real entity-really departing Victim-Will-Chain (vertically re-arranged unit of the vert) and the Query about its last difference-non-equally aesthetically common underground sectional tenderlove automorph's private decision-transformed Participants-Dray (Preshared Key based truth transformer service of the poods-(the solution of WP-Transform (TrPM's), uses at minimum double par Them's) based POW), in the doer's position, where the bound DT (dummy Sensor) lies.

Solutions for location privacy preservation in VANETs can be sorted into three types: pseudonyms, location cloaking, and cryptographic techniques [2]. One layer of privacy-preserving solutions is to issue the vehicles anonyms (or pseudonyms), which frequently are

changed. This way the connection of the vehicle with its sensor can be physically disrupted through breaking the long-term connection with pseudonym-changing events. The location-based broadcasting of the pseudonym may be organized so, that around each single vehicle, at least k active vehicle-pseudonym pairs exist (k-anonymous), so that an observer predictions about the actual vehicle location becomes difficult. Another approach to achieve confidentiality is the location cloaking. If a sensor will be able to mask its correct location with a set of appropriate positions, then an adversary would never be able to physically decide on the exact sensor location. Cryptographic techniques offer the trade-off to preserve data query accuracy together with the actual location privacy of the vehicles. A drawback for purely cryptographic solutions can be the costly operations and communication resources (e.g., the well-known anonymizing network "Tor" has a rather bad peer-to-peer relation for linear time cryptosystems, which can be excellent leadership, redundancy and speed within k-anonymity or location cloaking.

4.2. Differential Privacy

For example, pseudonyms, location cloaking, and cryptographic techniques are used to protect the privacy of location-based services. These methods regard the users as attackers and seek to protect the servers from these attackers. However, they do not provide strong privacy guarantees against the server, which can access a lot of users' information [2]. Recently, Geo-Indistinguishability has been proposed. This model can only protect data against noiseless and nongroup privacy attacks. Tian et al. have introduced differential privacy technology into location-based services and proved that differential-privacy location-based services can be provided by utilizing Geo-Indistinguishability. However, their core algorithm is based on R-algorithm, which is efficient for high query accuracy, but it can be nonrobust. It is a risk to adopt differential privacy technology to location privacy for locations data on road networks. In this paper, we provide a differential privacy model especially for the setting of location-based services. Our model, called Geo-Graph- indistinguishability, incorporates location information, road-network information and differential privacy. The concept of kinematic perturbations of root and tree graphs for location privacy of momentum-based location-based services and kinematic-based location-based services, respectively, are proposed. Privacy guarantees in differential privacy of spatially correlated random variables are discussed, which is the first interpreter among community. In the end, we design two DP-LBS on road networks based on our differential privacy mechanism.

A formal connection between differential privacy and location privacy for query results. A flexible and scalable approach to route construction, based on stochastic movements, suitable for handling the non-uniform spatial distribution of queries. An in-depth analysis of g-anonymity, formally introducing it into the world of differential privacy and demonstrating its potential. The privacy of range queries on location-based services is an important issue.

Differential privacy was first introduced by Dwork [ref: 0f94014d-6177-4b8b-805e-d6132f2429c4; 0f94014d-f89e-44fa-a9d0-27e8c07690be], and recently it has become a well-established privacy model, which is proved by its certifications for robust privacy claims, and half-decade standardization progress. Theorem 1 shows how common differential privacy notions can be exploited in a specific location privacy scenario, following a systematic process inspired by formal model transformations between spatial concept transitions. To this end, we bridge the gap between the usage of differential privacy in typical data mining setups and the more challenging, mobility inherent spatio-temporal sub-sampling.

5. Integration of Privacy-Preserving Techniques in LBS for Autonomous Vehicles

As the use of autonomous vehicles (AVs) starts to become mainstream, the privacy issues that come with the deployment of these systems are starting to gain increasing attention. In, the authors reviewed the leading edge of location privacy–preserving methods for AVs. The privacy issues and requirements peculiar to an automotive environment were identified. Most importantly, the authors carried out reviews of available cryptographic primitives and building-blocks and provided an outlook on how they can be employed for enabling privacy-aware intelligent transport systems. The authors assessed where future research and development activities should concentrate in order to deliver AVs, keeping location data private. Based on these findings, the following work has evaluated five implemented case studies—each centered around autonomous navigation—to measure their privacy preservation performance.

There have been a number of research efforts that focus on the development of practical location privacy schemes, in particular, within the domain of distributed, next-generation mobile ad hoc networks (MANETs). In the context where supplemental infrastructure may be unavailable or unreliable, re-visioning the expectations for providing trusted services—such as location in particular—must, at the very least, still contemplate how the availability and deployment of traditional location services influence the plausibility, feasibility, efficiency,

and resultant privacy of upcoming location privacy realizations. Hence, it becomes essential to understand and anticipate the possible psychological and even legal implications of putting current designs into practice.

5.1. Architecture and Design Considerations

MDP solves this majority of the layout of the location-based information system with the help of minimal transparency data disclosure [15]. In point of fact, to provide anonymity in location-based systems, location cloaking or group recommendation techniques are outlined for noting with mutual consensus. Network outlink properties also leverage optimal placement and distance to an analysis point with the help of appropriate heuristic scoring.#+#+Nevertheless, the algorithm includes an attribute key in LBS and provides security algorithms and satisfy the properties of minimal minimal transparency pinpoint with tags. Cybersecurity solutions and privacy preserving techniques are the core constitutions of the Vehicle-to-Vehicle (V2V) Communications. On the contrary, this model suites a V2V category of configurations shown in Fig. Similarly, we consider the legitimacy points as the logical incorporation of the VNFS into EVI services.

To satisfy the numerous applications and a sudden increment of users in the cyber-physical platform Cyber-Physical System (CPS), a considerable measure of infrastructure is working for dealing with the again acquired data [6]. To enable the functionalities of CPS, ongoing research has the inclination to connect different devices to the cloud-presence networks out of which the vehicle-based positioning systems and location-based services (LBS) are considered profoundly. The adversary traffic analyses and behaviors toward the V2X networks consistently block legitimate data transfer inside communications [12]. The feasible solution is to model an effective architecture using various available tackling algorithms. This solution will result in consensus routing services. Leveraging this architecture, an effective model is proposed with the help of the e-commerce shopping system and the destination with the aid of the WINS Infrastructure. Pursuant to successful implementation of this model, the consent server-user communication on the consequence of the traffic response is acyclic decomposable.

5.2. Case Studies

Witness receipt tokens enhance the KDT, as well as see CDT for off-path attackers. Without witness receipt tokens, the CDT of all nodes in the witness and non-witness paths are not

enhanced. Therefore, they can attack and compromise the map of the witness. W wit ka h n witness receipt tokens, the CDT between the client and the new witness can achieve hamming (or burst) to be less than "GreaterThanOrEqualTo" Z Z. This may imply that they can locate their adversary by sending a number of fixed witness queries to the new witness. [12]In this section, we present three case studies of the use of LPPMs in AV navigation at the edge. Their audience is the right for which the case study is aimed. The first case study) developing a so ed “big city “ AV navigation assistance in IIT, Hyderabad, and the next two to transport fleets including non-profit service organizations (NPOs) in the SAMI Navigator in Spain and “last mile” navigation for AVss in an urban transport system with EVs in the Netherlands and Belgium-route plus charging-stations in SCHUNK (Extended study 1). [3] The Agent Oriented Lab/The Robot Lab, Department of Computer Science and Engineering, The Robotics Institute, The Vision Institute, IIT Hyderabad, India, is currently developing an autonomous vehicle (AV) navigation assistance, an AI based BigCity Technology for AV navigation with privacy preservation. [20]

The most prevalent method for providing privacy-preserving navigation to AVs is without using witness receipt tokens, which is sometimes referred as map download or replica-based schemes in the literature. Here, the AV is equipped with a client and a witness client in order to request a target address, receive an encrypted route along with the witness keys from the SP/rapper, and decrypt the route with the witnesses. In more detail, during the initial setup phase, the client requests Z-time-based indexes of the routing table, obtains 1 2 3, and then sends a broadcast message to the set of all vehicles. Some vehicles in their neighborhood (denoted as witnesses), respond with witnesses, which are key-value pairs. The stored key-value pairs can help the witness token to query the addresses.

6. Evaluation and Performance Analysis

With the well-informed degree of tolerance, asymptotic stasis, and h Mom Perot, a tracked obstruction strategy is faced with a conflict concerning anonymous split positioning determination . In Governor 6, we support the privacy-saving and fortification style of the Booster Valley over, via Olle vulnerable-backbone message order, operator dermal jaw reflexes, and user wrap feedback close to anonymous grifted. The Gymroenso unobserved reveres (`*RegwrofO' is forced to trick IvO with trusted cool to adorn the Healer ring by solar flares.

A maker, an enemy of self-governing vehicles will feedback no wayfinding goals to help successive programmed GPS, and consequently block it from auto-driving . As USV goes through the no-man's land, the tracker's objective is to firearm significant false data into the VFSs to lead them to swerve the state of the beaten path without being identified by the Power Real-time Inference Machine (PRIM) . In screen 5, the trust improvement proportional error analysis for the simple anonymous MVP related to VFS sequence is enlarged by the coordinating tick ace forgetting (MWP-SMCF) boost.

6.1. Metrics and Benchmarks

For metrics, we employ two spatial privacy metrics—probability of k-anonmity, accuracy, and normalized discrimination error (NDE), to evaluate privacy protection. Accuaracy is used to estimate how close to the original request the result of the location query is. NDE is used to estimate how much the result of the location query can reflect the real distribution of the underlying data. In addition, we measure the route completion rate as a utility metric, which is used to evaluate to what extent we can help the vehicles to achieve their final destinations. Furthermore, the energy consumption rate and completion time are used for network overhead (i.e., HK-SSF) which is also a utility metric to evaluate the overhead of KVFS. The first four utility metrics can be measured based on the original query-response pairs and privacy breaches. We define the route completion rate as the proportion of routes that can be completed according to the original query-response pairs. With all these metrics, In our experiments, we use three types of vehicles with various moving speeds i.e., 30, 60 and 90 [km/h] and the number of vehicles varies from 60 to 150. In addition, several (entropy based fine-grained) privacy metrics are also employed to evaluate security in our experiments including average entropy of vehicles, average entropy of the attacker and sum of entropty. The average entropy for ıt+1 can reflect average privacy budget for a vehicle at epoch t+1. In addition, we evaluate the information gain in each one epoch of the h attacker, i.e., the monetary cost that the h attacker pays. Specificly, we use the above four metrics to evaluate the performance of the two KVFS and the corresponding baselines. We evaluate the proposed method in terms of privacy and utility. The privacy of the WDSA is evaluated using two methods: (1) reidentification scenario and (2) adversary's success rate. Given a scenario after processing, we consider whether an adversary can reidentify the vehicle based on location-based query logs. Note that in the reidentification scenario, we assume that each vehicle performs a large number of queries in the 24 hour horizon to form the location-based query.

For each estimation, we consider 60 realistic moving scenarios, and for each vehicle, we randomly pick one query-location that is meaningful (i.e., the location is complex enough). We consider this particular location-based query log as the estimation. Moreover, we also evaluate the privacy in terms of adversary's success rate. For both privacy metrics, a smaller value suggests higher utility level as well as higher privacy quality. The utility of the WDSA is evaluated using route data, i.e., trip completion rate of WDSA and the relative values resulting from WDSA were used to depict how similar the trip sequences performed by the WDSA vehicles are to the real ones. Note that GPS UE data are provided to the data collector for all vehicles and random samples in the GPS UE data are considered the real query-log sets of vehicles. For each scenario, 2000 random sequences of realistic query logs are obtained by randomly combining query logs of multiple vehicles. The aggregate real-world trip sequence is used to depict the route participants use. Then, we compute the average normalised dynamic time-warping (NDTW) error to indicate the accuracy of trip completion, where a smaller NDTW error suggests better accuracy.

6.2. Simulation and Real-world Testing

These localization schemes, however still demonstrate notable limitations, unsatisfactory responses to user application demands or challenges in supporting some particular smart city important applications. For example, on the question of green, environmental mobility, the localization scheme of users envisions that a query information dataset does not impact the consideration of the CO2 emissions and pollutions by cars of any type . Furthermore and more interestingly in our context, the question of privacy and security of users on database query requests does not exist and will not be taken into account. Last but not least, for the context of fraud prevention on smart city applications, the localization scheme of users should alert on data injections, data perturbations and similar detected attacks. Even if any malware attacks on smart vehicles named Mirai, Brickerbot, WannaCry, Adylkuzz, Hajime, Stuxnet and others often targeting vehicles when these drivers do not take digital security into consideration.')}}

Three types of secure location-based data query schemes exist that protect against location privacy leakage to some extent: pseudonyms, location cloaking, and cryptographic techniques. Pseudonym-based methods can effectively achieve location privacy protection, however, the maximum privacy level with these methods is medium and they do not guarantee the query completeness. Location cloaking-based techniques, such as k-anonymity

and its various extensions, will also greatly reduce the positioning accuracy of the query area thus significantly reducing the query accuracy. The current infancy of cryptographic techniques ranges from secure session initiation to secure data transfer and secure data query. They are high efficient and can provide strict computational guarantee and even statistical guarantee .

7. Regulatory and Ethical Considerations

Moreover, in recent years, following the widespread use of the Internet, privacy issues have closely followed technological advances. This is an extension of the concept such as geoprivacy, which is the protection of privacy concerning geographical location information, and location-based services (LBSs) that have rapidly transited into more efficient and powerful forms, making them more widespread and available. LBSs are now expected to deliver ultrafine location information and provide services both indoors and outdoors. In the past, LBS applications such as find nearby restaurants, navigate, and map were first provided in the original developer's environment, such as the app environment. Signal transmission, processing, and storage times are hallenging for communicating LBS information between locations due to the existence of a centralized server. Also, the computer work done using geoprivacy protection technology emits quite a large amount of radio wave energy.

There are significant societal consequences to the widespread adoption of privacy-preserving technologies in autonomous vehicle navigation systems. The US Department of Transportation (USDOT) is focused on removing regulatory barriers that may prevent automated vehicle deployment. In the safety spectrum of interest to this study, and raising policy and ethical considerations for the automated vehicle industry, would be the privacy perspective. Privacy concerns in automated vehicles have been broadly discussed in the literature [21]. [22]. The privacy of automated vehicle passengers is a major concern since fully automated vehicles make traditional privacy protection measures difficult or impossible. In existing transportation systems, identity information generally does not need to be considered, because people use physical money to pay for public transportation, use fuel cards to refuel their vehicles, and use a non-unique number plate to get away with vehicle taxation. However, with the advent of automated vehicles, these issues have become issues to be considered. To solve this issue, we propose an automated vehicle autonomy policy. The thing is, an autonomy policy can help to jointly solve the problems of preventing secondary

threats to safety and unintentional disclosure of personal information through automated vehicle sensors. Moreover, developing the necessary technologies is essential, but first, it is important to discuss the social requirements that we should fulfill as a protection object, even if we do not act, in order to clarify what we should do.

7.1. Data Protection Regulations

To the European Union's General Data Privacy Regulation (GDPR), the European Telecommunications Standards Institute (ETSI) Methodology for Provision of Service Requirements (ETSI GS PMR 004) and the equired scenario will not require the use of personal user data, while preserving the accuracy of the final service data and operation of connected car locations is proposed. While preserving the accuracy of service data, this solution only applies to local and nearby data, and thus, far-distributed data is difficult to handle. This solution is further reported, as being not applicable under the scenario where there are various proprietary and incompatible systems in the vehicle ecosystem, as different manufacturers provide different connected car location services. This paper describes (1) the occurrence of the privacy risks caused by LBS, especially in autonomous vehicles; (2) the consequences arising from the unauthorized access to personal data in the health-care sector by the approximately 70 % of medical facilities which have suffered from such unauthorized access in the last 1.5 years; (3) gives the insights into building the desired defensive mechanisms to manage privacy rather than simply protecting data or identifying cyber-threats.

[8] In the automotive industry, users are used to giving control of services a certain amount of personal vehicle data. Manufacturers of connected vehicles and service providers use user data to improve various aspects of the vehicle and to offer advanced vehicle-related services. In terms of autonomous vehicles, location-based services (LBS) play an important role in autonomous vehicle navigation, as well as in the implementation of advanced driving and safety systems [23]. In autonomous navigation, location data are considered to be sensitive personal data, as user location information is collected, transmitted, and processed in order to provide users with location-based services. In response, distributed and privacy-preserving techniques have recently been proposed, which limit the disclosure of user personal location information by transforming the data into a form that does not compromise privacy, such as shared measurement and collaborative and location masking.

7.2. Ethical Implications

Second, as disclosed in the summary of GDPR and CNIL guidelines in [24], which are two of the most referenced regulations by the present paper, we also notice that it is difficult to satisfy the general requirements of location privacy whenever we use the conventional GNSS for a variety of architectural reasons. Some isolated researches connecting intelligent transportation systems and GNSS with LBS consumption have appeared in the recent years, but they are not plentiful. One way of taking benefit from the AI can lead to the changes in ethical concerns about the individual user for the sake of increasing the business gains for the big data corporations. A specific regulatory effort show that the privacy trap could be bridged for the emergence of sustainable AI powered ITS downside of transitional EU regulation as compared with previous ones because of some challenging privacy issues concerning the protection of cyber-physical spaces have to be solved for autonomous vehicular navigation, securing the independence of the GPS-like systems to which the autonomous vehicles shall recur, and removing the legacy vulnerabilities inherent in the AI training datasets. Our discussion suggests that more efforts need to be put to the surface at the technical graduate counters and are greatly welcome to the context of data unified civilizational era respectively.

As we continue with our analysis, many questions arise as to the data we are working with. First and foremost, we should solve the problem of setting a acceptable balance between privacy preservation and usability. In this sense, the authors in [3] have studied decision-making session for users of a simulated ridesharing application. They revealed that about 15% of users wouldn't adopt the app unless their friend's real-time status are also available to them. This imposes on us the social seeking patterns of passengers in chilling group, and it can also justify the necessity of developing the dynamic privacy control schemes for passengers in the car. In addition, clear consensus between location informa-tion privacy and cybersecurity should be reached before we conducting linkage between the informativity and the adversarialness in position data.

8. Future Directions and Research Challenges

Three of the research challenges are centred around the robustness of the location privacy solution to be used in the context of an AV. The significant reduction of output uncertainty observed in related privacy-preserving knowledge extraction procedures when specialized AV sensor and typical human sensor details are neglected. Enabling privacy-preserving

navigation effectively and efficiently for practical-scale safety-critical applications in response to disruptions in the context of rogue vehicle trajectory attacks. And acting within the constraints of the direct vehicle-to-vehicle channel range or average channel power settings to build a class of adversarial preference-aware navigation strategies.

Three of the research challenges identified are specific to AVN. The problem of improving the effectiveness of the solution to protect against an adversary trying to link individual location updates to construct trajectory histories. The problem of securely outsourcing location-based service functionalities to untrusted computation resources while preserving various users' privacy [9]. And the problem of achieving coordinated route planning algorithms that are resilient to declared but incomplete traffic conditions which malicious vehicles aim to exploit [2].

8.1. Emerging Technologies

However, the edge technology that is currently able to satisfy the necessity is Big Data. This chapter aims at providing an ensemble of tools to translate the WoT principles (made available through VANET and IoV) into a set of Web-based services by enabling and validating the concept of IntelligentTransportation Systems IoTs (ITS-IoTs). We will also try to highlight all possible points of difficulty and their logical solution and describe Web of Underground Things and an integration with pedestrian traffic and IoT technology, and also new solutions for Include of ML and CM, anonymous or blind signature and steganography to modify and (de)face the localization risks [25]. The Chapter also aims at popularizing FastWeb as a Google Chrome and Firefox extension, presenting standard libraries that facilitate setting the correct strategies for the evaluation of travel time and provide e-consultation or e-transaction into a chain signed by the traveller and/or by the possible provider per various locations, that are indispensable in order to form the PRP-ISCS (that is the payment or non payment signed anonymous e-decisive, subscription, ride sharing e-dict on new Ms & R & Q) paradigm. All e-consultations and e-transactions are concluded using the FastWeb status-variable for the validating MS or RS session.

The transportation field has been revolutionized with advances in new technologies, including monitors and sensors; various techniques for collecting data; and smart transportation systems. More recently, intelligent vehicles with path planning or traffic prediction applications, or autonomous vehicles that control themselves, have received

attention and investment. These vehicles utilize a variety of sensors to collect data s and achieve objectives such as reaching destinations, avoiding collisions, and controlling speed and motion [26]. Technology for path direction and parking, digital control systems, remote sensing data processing, and state-of-the-art simulations in urban and regional traffic have also been popular. Nonetheless, these systems still require a means of communication between the vehicle or drone and cloud infrastructure; methods to manage data collection, processing, and privacy are often ignored. With the continuous growth in the use of V2X communication to provide cooperative information, security and privacy issues, such as privacy protection from adversaries, secure data storage, and privacy-secure EV public charging from adversaries are characteristic of the underlying Web technologies [27]. The intelligent vehicle system has a lot to offer in this context, and the current focus on the evolution of this technology is markedly noticeable. In this context, the set of articles aims for translating the Web-of--Things principles into Intelligent Transportation Systems, using algorithms and new technologies based on the meta-language known in the computer science, as variants of L(evemon)TL and new neural DPI or DPSSE to protect the localization data and public key enciphering the big data and data mining data (that represent the various data that are indispensable).

8.2. Unsolved Problems

B) Finally, it must be taken with into account that progress in functional layers (e.g. sensors and others) require an adaptive cooperation preserving privacy between different manufacturers: their systems must do behind each other the “mutual veracity certification” federated for periodically guarantees to their connected vehicles privacy compliance and safety with high probability. The geographical position of participants might induce additional privacy issues [28].

A) Additionally, robust location privacy provision must be dispensable under different regulations requiring privacy. Such protection mechanisms in a car must, for example, be safely deactivatable for high precision parking aids like parking aids or protection against collision detection with moving vehicles and other objects on-site [24].

Issues still remain unsolved to provide the best possible Defense-in-Depth security architecture, fulfilling different levels of reliability (e.g. worst, average, and best cases). A better protection against various attackers, reliability for a wide range of clients, and

versatility would need addressing more uniquely integrated privacy protection frameworks throughout the entire system, liberating applications from responsibilities in controlling datasets and configurations only in very specific functional layers [29].

9. Conclusion and Recommendations

[7] Location-based services (LBS) have gained importance and demand with the wider use of global positioning systems (GPSs) in smart devices. LBS find applications in multiple domains, such as e-commerce, Internet things (IoT), mobile marketing, mobile payments, and autonomous vehicle (AV). Sharing precise location information in LBS may lead to significant safety and privacy implications. In the meantime, AV could leverage accurate location information over the infrastructure basis as well as among cars within vehicle-to-anything (V2X) communication. However, a vehicle that shares its current location or route may reveal its planned path to LBS applications and adversaries. This paper develops location privacy in LBS for AV and sincerely considers consent of vehicle owners. The potential impacts are evaluated over AV, including the reliability of vehicle navigation and routing that obscures the planned route from AV; attacks on LBS that could alter vehicle paths; and the fake analysis of data that contains unexpected locations [3].[5] The global pose of the vehicle is revealed to the attacks that exploit the inherent vulnerabilities in LBS for AV. Instead of iteratively altering the planned route using accurate and available navigation (AlterRoute), a number of random paths would be generated for analysis to alter the next location of AV when considering differential privacy. LBS-based AV shall analyze the altered paths for off-road locations, and would alter the navigation to the least expected location. In general, differential privacy is not suitable for AV navigation because the navigation scheme may choose the worst expected routes to evade location reads. In this paper, it is shown that if the differential privacy costs are higher than the utility of vehicle flows regarding the gathered path information, AV networking fails. When planning differential privacy from the start, instead of making a smart transportation system (ITS) more secure, one eventually restores the very fundamental challenges of producing aggregate system models or refuses the system's analytics expected utility. The analytical solutions for an instance of LBS security for ITS services are provided as theoretical expressions based on modified convolution properties. Shows that if differential privacy in LBS turns out to have been pursued initially as a misaligned policy, privacy policies for AV are also prone to attacks.

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.