Privacy-Preserving Data Sharing Mechanisms for Autonomous Vehicle Collaboration

By Dr. Jorge Castro

Associate Professor of Computer Science, University of Costa Rica

1. Introduction to Autonomous Vehicle Collaboration

When a vehicle perceives its surroundings under different driving scenarios (e.g., poor weather and occlusion) with multiple sensors, it obtains diverse observation data. Different sensors focus on different objects and situations. For example, LiDAR works well in both day and night conditions, but its performance degrades for bad weather. In contrast, radar maintains stable performance under adverse weather and light conditions and remains a reliable choice for vehicles. Camera perception has been very much challenged under various circumstances, such as severe weather conditions, or light and shadow interference. Sensory homogeneity provides little help here, because it will also be impacted by inadaptable adverse impact factors [1]. Independently perceiving the environment or only considering the multi-sensor difference in AV coordination creates a new "central perception" approach, in which decision-making and action output are based solely on local observations. This approach preventively circumvents multi-sensor redundancy observation issues and still produces safety decision making when individual sensors fail under certain adversities.

[2] [3]Autonomous vehicles (AVs) rely on a variety of sensors, such as vision cameras and LiDAR, to perceive the environment and make safe driving decisions. However, incomplete perception of AV sensors and their limited range can lead to decision-making performance degradation under some adverse conditions (e.g., occlusion, bad weather, and obstacles). V2V collaboration technology helps vehicles perceive their surroundings over long distances, thereby greatly broadening their perception range and improving their safety level. In a V2V-enabled driving scenario, participating vehicles collaborate and collectively form the foundation for remote observation of their respective environments. This sharing of observation data is the first essential for cooperative AV perception and enables a better understanding of the environment around an AV.

1.1. Overview of Autonomous Vehicles

[4] Autonomous vehicles (AVs) have come to fruition after decades of effort and research. With the rapidly advancing sensor, processor, communication, and actuator technologies, AV technology has advanced from level 2 to the level of conditional and high-level automation, with the clearly identified roadmap towards full automation available. Planning, control, decision making, and reinforcement learning form the backbone of AV advancements. Sensing and perception are also critical to AV technology. Enough sensors have been installed on the vehicle to ensure the reliability of environment perception. However, many shortcomings still exist. AV equipment has limited by the Line of sight, leaving the rear area of the vehicle liable to occlusion. Three-dimensional point cloud information of large vehicles, pedestrians, traffic signs, and other objects are difficult to perceive from the vehicle. In this scenario, exploring more efficient environmental perception becomes the study hotspot of scholarly circles. It is also the most important research area of traffic and car enterprises innovative solutions for environmental perception deficiencies [5]. In recent years, the idea put forward for collaborative perception has made remarkable achievements in addressing wear limitations of the vehicle and has risen to prominence as a feeling hotspot of the auto trade. In the early stages, the perception surroundings of each vehicle were shared and aware, realized by each vehicle's raw sensor data sharing. It improved the effect of environment perception by overcoming perception limitations of size and range of sight through synchronous integration of diverse vehicle perceiver data. The kind of solution depended on mode cars because synchronous information exchange operated on the vehicle. However, without communication capability, real-time cooperative perception effects were difficult to get. Collaborative perception was implemented under our feasibility and practical prototype conditions around the wireless capability known as V2X systems. As vehicle-to-everything (V2X) communication technology, low-latency, high-reliability and wide -range dynamic acquisition of environmental information ambiently and in advance achieved environmental perception among single vehicles. It is reported that, under certain traffic conditions, the results of relevant purely cooperative perception are that extreme long-beam vehicles and short-beam vehicle-individual perceptions are, respectively, 20% and 10% lower than that of cooperative perception [6].

1.2. Importance of Collaboration in Autonomous Vehicle Networks

[7] Although the various sensors equipped in autonomous vehicles (AVs) today make them opulent in terms of functionalities, there are still some critical shortcomings affecting their full autonomy. The biggest barrier is that the data captured by the sensors is limited to the specified boundaries of the physical vehicle, which restricts AVs from seeing the full picture. To alleviate this setback, in the last few years, the autonomous driving community has turned its attention to the idea of autonomous vehicles collaborating using vehicle-to-vehicle (V2V) communication. Through collaboration, the movement and perception of one vehicle can be shared with others in the neighborhood to generate a comprehensive view of the doings of the whole environment known as perception sharing [4]. With such a system, every participating AV will have enhanced situational awareness coming from multiple perspectives, or essentially a complete spatial encapsulation of the traffic scene where each AV can individually measure any position as far as data from at least one of the participating vehicles' sensors is available. Additionally, every survey on the drivers' perception of AVs has concluded that 90% of road accident responsi- bilities arise because of driver errors [5]. These include driving under influence, speeding, reckless driving, and engaging in activities while on the move like texting and eating. It is believed that replacing human drivers with AVs can significantly reduce the number of road accidents. The seminal work for this end is being accomplished these days. The end-state aim is to eject human presence from the vehicle cabin and thus saving their lives from the hazards of road accidents, which is the cause of the highest number of accidental deaths in the world.

2. Cybersecurity Challenges in Autonomous Vehicle Networks

1) Privacy-preserving vehicle network architecture evolution of corresponding access to autonomous vehicle data sharing : autonomous vehicles, on their own initiative, collect data and query data from other vehicles or RSU tasks to access solutions, and define different architectures according to their respective trust levels and user requirements; 2) The privacy-preserving vehicle network mechanism of the corresponding deployment (a) Respectively, synthesize and summarize the data service settings provider, data query requesters and different participants in autonomous vehicle networks; 3) The corresponding technology evolution for protecting privacy, and thus the property rights of the user's data.

The privacy collection and its authenticity manner have been deeply studied from different angles. However, a new challenge has being introduced, that of protecting user's data despite

the large-scale sharing for primary autonomous vehicle manufacturers [8]. The data privacy-preserving vehicle networks are further divided into:

Developing secure vehicle network architecture for autonomous vehicles is crucial [9]. Autonomous vehicles share data through the cloud and road-side units to provide safety and convenience services between vehicular networks. Although exchanging resources and data via the network creates added convenience for all participants and services, it also brings the risk of cyber-attacks [10]. Once an actual vehicle is invaded, not only the individual user's privacy or asset is being violated, it may also affect the safety of all vehicles and even violate the lives of pedestrians in the nearby vicinity. Therefore, it is essential to support resources of data and query searches of autonomous vehicles among the collaborative vehicular network, and meanwhile, guarantee that the individual vehicle's privacy is being protected.

2.1. Threat Landscape in Autonomous Vehicles

Users already face threat impacts in terms of their privacy or personal information in vehicular communications enabled by connected vehicle technology, which can compromise their perception about revenue generation from their personal driving, vehicle itinerary, or crash history data. Autonomous vehicles would also never be accepted if they cannot guarantee their occupants freedom from privacy loss, i.e., users of a connected vehicle need to feel comfortable and confident that the vehicle is secure enough to guarantee their own and their passengers' privacy – a fundamental human right [11].

[10] [12]The threat landscape faced by autonomous vehicles is broad, existing as a set of protocols, technologies, and data that must interact securely across complex ecosystems of manufacturers, providers, and third-party stakeholders. Layered security threats against the systems that control vehicle dynamics and automation pose a safety risk to drivers as well as pedestrians and other objects sharing the road. Compromising the data integrity of systems that depend on ground and traffic infrastructure requires security across wireless and sometimes physical links between the center, edge, and external data networks. Security threats can affect systems, equipment, or telematics solutions for directly or indirectly managing data from driving tasks and infrastructure. Threats may be launched using multiple transmission types for vehicular communications within the vehicular network, ranging from vehicular ad hoc networks (VANETs) to device-to-device (D2D) systems and other sets of trusted models in the network of networks. Such model support should also provide comfort

for on-board devices in relation to their own security when they are deployed to be applied as intelligent assistants to passengers.

2.2. Security Vulnerabilities in Autonomous Vehicle Networks

Security of cyber–physical systems (CPS) is crucial for the development of sustainable autonomous transportation systems [13]. The safety of these systems, in turn, largely depends on their ability to protect the system units from unauthorized access and malicious activities. Recent studies have addressed the implementation and verification of security mechanisms for autonomous vehicles in switched-based architectures. The integration of tens of different applications with different security requirements on the same platform fabric remains a limitation. Key vulnerabilities of integrated systems include spoofing attacks on sensors, false data injection, and the lack of a vehicle security framework ensemble. Vector intrusion detection and response architectures are presented to identify threats and store and maintain real-time environmental conditions using several sensors. Given the fact that the unorganized and unordered emergency parameters can cause catastrophic situations, a spatiotemporally stored intelligence-based emergency algorithm is used to identifiy unknown threatening factors and take the necessary protective action. Therefore, a complete architecture consists of secure communication channels and secured automotive ethernet, safe execution platforms with security engine switches, and real-time intelligent security agents that can identify all cyber physical vulnerabilities.

Trust and collaboration are essential for successful multi-stakeholder collaboration in a Mobility as a Service (MaaS) platform [10]. Security threats in autonomous vehicle networks pose serious concerns. Data theft, identity theft, device hijacking, denial of service (DoS), and privacy infringement are some of the factors affecting stakeholders, thereby hampering successful collaboration. These threats can target the network, device, and software levels, making it crucial to address vulnerabilities in data, network, vehicle, and financial security. At the data level, attacks can disrupt the reading or writing of data, inject false data, and compromise confidentiality. Network attacks can create black holes or access points, redesign the network, hog the network's resources, and disrupt communications. Vehicle security can suffer from spoofing attacks, reserved attacks, injection of false data, and degraded localization [11]. Threats to data and network secure communication include both internal and external risks including key management, eavesdropping, data manipulation, and DoS.

Finally, financial security can face threats of toll fraud, black-market trading of user IDs, and false advertising. The authors concluded that successful collaboration in MaaS should address concerns for hostile multi-stakeholder collaborations, including mobile and edge collaboration security, and complex multi-stakeholder collaborations in the emerging spectrum framework, thereby requiring new trust and security mechanisms to achieve successful economically viable operations.

3. Privacy-Preserving Techniques in Data Sharing

Homomorphic encryption (HE) is an encryption technique that allows computations to be performed on encrypted data, without decrypting it. HE is highly suitable for scenarios in which data is transmitted to multiple entities, but its accuracy and privacy remain paramount. This allows tasks to be jointly executed on encrypted data, resulting in encrypted output with the same information content as the desired plaintext. In autonomous vehicle collaboration, HE can be used to encrypt sensory data stored by autonomous vehicles, allowing for collaboration on a collective learning platform. Masking techniques, including secure multi-party computation and private information retrieval, essentially reduce the probability of sensitive data being leaked during data sharing. Multiple parties can share sensitive data without revealing the data to others, and their collective conclusions are computed privately. One way of achieving privacy at the data sharing level is to integrate advanced steered parameter estimation methods with HE techniques in autonomous vehicles. A well-observed method for data manipulation is to use perturbation at the data sharing level. Gaussian perturbation-based mechanisms add independent Gaussian noise to factual data to generate privacy-preserving data to successfully extract the global gradients of the factual data in a cloud-based IoT service. Conversely, Laplace mechanisms are suitable for environments with bounded data. Homomorphic-based encryption mechanism is generally of two types: additively homomorphic and multiplicatively homomorphic. When more than two participants interact in sharing data, a horizontally federated learning network is formulated that neither transfers their trained models nor shares any data with the centralized aggregation platform. Data masking is achieved through shared perturbations across different iterations, buffers are independently populated, and models begin at the same convergence point.

Differential privacy (dp) is a promising approach for privacy-preserving data collection and data sharing. According to the concept of dp, a mechanism for data processing is called differentially private if it only reveals results that are virtually the same without one of the individual's data. Differential privacy, denoted as (ε, δ) -dp, is an essential attribute as it quantifies the gain in privacy protection. To illustrate, even if the adversary can learn the information of an individual from the released data and the one without the individual's data, the gain in knowledge should be minor. When δ = 0, differential privacy is called pure differential privacy; when δ > 0, it is called approximate differential privacy. The value of ε and δ determines the privacy?loss randomness added by the mechanism. The small value of ε and δ indicate enhanced privacy protection. In the above definition, the smaller the value of (ε, δ), the lower the degree of attack and snooping activities carried out by an adversary. The requirement for this property is satisfied when the global distribution of the data and the local distribution of the individual data is exactly the same. In the case of differentially preserving mechanism, the global distribution and the individual distribution will be different due to random noise and privacy loss. As a result, differentially preservation analysis is performed to estimate the privacy disclosure and infer hidden information from noisy data.

3.1. Homomorphic Encryption

[14] Homomorphic encryption (HE) is another cryptographic technique that has gained increasing popularity recently. It is a powerful cryptographic approach developed for secure data processing and has found several applications, including autonomous driving, and smart charging systems in the transportation domain. In general, HE is a form of encryption that supports homomorphic operations that can be performed on the ciphertext, and then gives the same result as if the operations were performed on the plaintext. Based on heir generality, HE is cla4ssified into two categories: Partially Homomorphic Encryption (PHE), and Fully Homomorphic Encryption (FHE). Partially homomorphic encryption is the type of encryption that allows one type of operation to be j^erformed on the ciphertext, and then it will gives the same result as if that operation were performed on the plaintext. Two types of operations are considered for PHE: addition and multiplication. A PHE is called additively homomorphic if and only if it supports addition operations, and it is called multiplicatively homomorphic if Bnd only if it supports multiplication operations. On the other hand, FHE is a more advanced version, where it allows both addition and multiplication to be j§rformed, as well as other operations.[15] Despite the investment in homomorphic encryption, PHE in particular, it has

serious limitations. First, the supporting target space of a PHE is limited. Second, the size of ciphertext increases drastically as the complexity of plaintext decreases. Third, comparison tasks are obviously not supported, that is, it can not determine which is larger or smaller among two encrypted data. Fourth, the running time of encryption and decryption algorithms must be considerably high in this way. Thus, designing an encryption scheme which supports more operations in a possibly limited target space, has smaller plaintext/ciphertext blow-up and works with frequent requirement of comparison is still an open challenging question. Note that these concerns are even more serious in the vehicles' collaboration context where privacy is essential. Therefore, adopting such techniques for preserving data privacy in the context of accident warning is a challenging task.

3.2. Differential Privacy

Due to the fact that the centralized algorithms might suffer various network-related issues and losing privacy rather than the bargaining capabilities of participants, it is still insusceptible in a review of the collaborative autonomous driving scenarios [16]. Caruccio and Grassi addressed the problem of automating autonomous negotiation for establishing pairwise contracts between vehicles in the context of a vehicular information sharing network. To reach a decision, every vehicle has to collaboratively check the autenticity of the message received from another vehicle by using a sophisticated and configurable reputation system that can be tuned with respect to many parameters.

Differential privacy (DP) is an anonymous method that injects pixel-wise noise into an image to execute the traditional deep learning task using the private datasets [17]. The generative adversarial private nets (GAPNs) form a differentially private generative adversarial network (GAN) architecture whose generator aims to transmute the original image data distribution into an approximate differentially private distribution so the discriminator is in charge of discrimination between private and original datasets. Differential privacy (DP) has attracted significant attention in today's deep learning era, providing guarantees of privacy-preserving methodologies in which the private information can be extracted and the accurate models are also trained using the noisy gradients [18].

4. Fusion of Threat Intelligence in Autonomous Vehicle Networks

In practical training environments, the Uber vehicle was the most effective regularly updating vehicle and the Volkswagen the least. The Honda and Toyota vehicles contrast the different updates providing more information at lower and upper bounds, respectively. Generally, it should be anticipated that the proposed vehicle update data fusion will exhibit the worst cybersecurity – however, vehicle achieved an unprecedented material discovery of threats in real-time. With the intention of safeguarding the cybersecurity vigilance, the publicly released data was transformed into Microsoft BELTA-compatible databases containing T-cells for all the vehicles as the primary threat indicator data to provide a simplified interface for the cybersecurity research community. The T-cells have a 50% chance of avoiding bystander exposed security flaws and the remaining H-cells represent real threats for the future sensitive operation.

[19] There exists a distinct difference between periodically monitoring traditional notification updates and regularly updating in-vehicle cybersecurity threat intelligence data at an enterprise level, the latter generally requiring extra attention because it is essentially like acquiring analytics in that updates contain important information on potential vulnerabilities. The existence of several vehicle control units also raises a risk, whereby the use of a single, centralized cloud network results in strain caused by heavy reception and transmission traffic, suggesting that bloom filters should indeed be computationally efficient [20], and alert updates should involve cryptography. The vehicle cybersecurity monitoring and warning system involves an important data aggregation phase from which legitimate and physically associated Alert Updates collate into a sizeable "with_domain _and _without_domain" datasets that can be used for training Alert and Update encapsulated defense models. Without useful Alert Updates to learn, these datasets could be abandoned in favor of legitimate bigdata. In cases of a scan with every warning vibration issued to the driver and acted upon using WLAN, a formal encapsulated defense model developed using the two datasets complies with typical detected miscon- figured elements without compromising any cybersecurity research.

4.1. Importance of Threat Intelligence Fusion

Regulation demands aside, rampant autonomous systems research is accelerating us towards an exciting future characterized by highly-integrated autonomous systems that will process large volumes of mission-critical data from an array of onboard sensors and from a myriad of

interacting teams or platforms requiring specification of what safety-critical events need to be monitored for. In terms monitoring for cyber-threats, just like in the commercial software market, techniques for detecting intrusions and malware differ dramatically. Firewalls and network proxies, for example, detect malicious file transfers by examining the content valid state space, seeking a comprehensive protection strategy in an evolving automotive threat landscape. Moreover, lightweight intrusion detection methods designed for autonomous system environments must be introduced, whereas traditional methods for host-based or network-based intrusion detection are ill-suited to vehicle retrospecting since vehicle users often deploy single-purpose, non-modular, and guest-friendly security functions [21].

Although the cybersecurity challenges for autonomous vehicles are already significant, with the increased enforcement of 'opt-in' regulations such as the SPY Car Act [7], the traditional intrusion detection method relying on the direct observation of the network security events and host security events will suffer challenges under new regulations. First, the transparent and real-time operation is imperative for the system in every machine learning-based method, which must operate in a transparent mode and must be online / real time without any abort. In contrast, the E15 nullifies the ability for the vehicle control unit to opt for online and transparent detection of unknown attacks, since if a service relies on the collection of logs for the profiling stage, the vehicle user shall delete the logs [11]. Second, the vehicle cannot guarantee continuous power consumption without thresholding the number of services running on board computers. SparkPlus delegates long-term warranty to automotive manufacturers without any punishment, unlike to new regulations' warranty period.

4.2. Techniques for Threat Intelligence Aggregation

If the updated threat intelligence is not shared among different AVs used by different agents, then that could create dangerous threats to the AV's agent and other vehicles present nearby their functional range. So, to avoid these dangerous threats, the prediction information learned by one agent must be shared along with salient and irrelevant information among the other agents so that we could perform safe manoeuvring and actions [22]. The Autonomous Vehicles agent can share their data and models using a differentially private method such as homomorphic encryption, federated learning, and multi-party computation. The weight-vector corresponding to the input feature vector can be generated in the form of obfuscated ciphertext using a homomorphic encryption method.

The finest way to aggregate threat intelligence information shared among different collaborating AIs using autonomous vehicles is to construct several types of threat prediction models. However, sharing AV's data and trained model itself with the central authority could make the AVs privacy vulnerable [7]. In order to preserve the privacy, the Central Authority could propose the incentivised sharing strategy to the AVs. This could activate trustful interactions between different AVs and the Central Authority. Also, the Central Authority could perform prediction without sharing full information by training threat classifier model at each of AVs, and central aggregator mixes these partial results [20].

5. Case Studies and Applications

Many companies are investigating the relative distance and angle of two vehicles for collaborative mobile application development. For example, Toyota released a self-driving car technology road tested around its headquarters in Plano, TX, USA, that could exchange construction data and metadata within four vehicle-to-vehicle (V2V) control stations, according to their online dispatch. Google introduced the Mobile V2X solution, R1, designed for remote control functions. R1 supports both camera-to-UI and camera-to-cloud exchanges and represents vehicle data in collaborative applications like Smart Transportation virtual machine images. However, in the aforementioned studies, secured visualization and secure transfer of V2V data is not discussed [23]. Kleyko et al. mentioned the voice message can be used to create a short gradient descent algorithm, which adjusts fuel-efficient planned paths for large multi-point vehicles. In addition, deep learning-based two-level dispatch for the rapid planning of one-time augmentations in optimized driving directions in intelligent connected vehicles was proposed. The authors recommend further studies on advanced attacks in CAV, as the wireless medium between vehicles could have interference with the driving directions. When future V2V interferences are formulated accurately, it will be possible to develop an updated architecture for enabling secure forensic arbitration. FFA-CF Authors group showed an alternative approach for the consumer self-reporting of health data in the CAV domain using a secure privacy-preserving protocol, called Consumer HEalth Acquiring Protocol. This approach suggested hiding sensitive data inside an anonymous request in a transposition request and forming health data with the information reclaimed in Fan Fangping AES key-based anonymization [24].

Kiyani et al. presented the idea of an interconnected vehicle (V2V) and road surface (V2X)-based network equipped with a reliable systemic architecture of 5G-aided Large UAVA (Unmanned Autonomous Vehicle Area). They claimed that efficient data sharing among vehicles and providing a user-friendly interface for decision making among V2V, V2R, and V2I links would allow autonomous systems acquiring and using information to reach smarter decisions more efficiently. However, their work did not address the security and energy efficiency issues in a timely manner and supposed that 5G technology is available to resolve any challenge of the considered system in V2V technology. Challita et al. proposed a secure encryption and decryption framework for data sharing in a collaborative environment to secure the communication between UAS and the remote-control center. Their proposed method consists of encrypting exchanging real-time data using a secure and efficient C crypto library named libe3crypto for the native Linux environment. Xu et al. introduced Efficient and Privacy-Preservation Truth Discovery (EPTD) technique for multicast-enabled ICN. The authors observed the joint considerations for multicasting and privacy-preserving truth-ing techniques in ICN, and the optimization and adaptation problems based on EPTD with heuristic algorithms in ICN were not well addressed yet. It is also pointed out that the heuristics could be further adapted for specific application scenarios to achieve better performance and higher effectiveness, but it is still computationally complex in ICN-based Intelligent Connected Vehicles (ICV) [25].

5.1. Real-world Implementations of Privacy-Preserving Data Sharing

After being instructed by this foreword, the reader is awaited to keep this summarized distinction in view and look into ?2 to 4 for details. The subsequent organization of this paper is as follows. Some classic, well-known, and state-of-the-art privacy-preserving global and local mechanisms in DP and EP will be introduced and analyzed in Section 2 [7]. It can be clearly seen that existing privacy-preserving mechanisms are generally designed and tested upon text-based data, such as data produced by commercial search engines, though they can be applied to autonomous drive data sharing. As we demonstrate here, such mechanisms exhibit significant deviations from their original efficiencies and is able to unserve the AI tasks.

At the same time, there would be less demand for training data from real historical data as training data generation should be less sensitive to the vehicle_dis_labeling_feature [20]. The

changes in the skewness and the majority feature of this dataset may be caused by other unobservable attributes mystery-related. For certain automakers, the vehicle_dis_labeling_feature may be already controlled when their data are exploited for data training due to technical or economical considerations. This problem will not be discussed further in this paper.

5.2. Success Stories in Autonomous Vehicle Collaboration

Even very recently developed autonomous vehicles have cloud computing features that are already providing drivers with communication and experience enhancement [10]. Further development of autonomous vehicles suggests that the requirements of cloud computing have evolved toward autonomy. For example, autonomous vehicles that interact with each other could generate driving data (e.g., typical driving speed of a given route) and store these data on servers for future applications, including improvement of current daily experiences [26]. Then, future autonomous vehicles might start dealing with driving operations without being directly asked by the driver. A major reason for this is that vehicles are an essential means of transportation, especially in regions without good public transportation. One could easily wonder what we need to be able to make good and efficient use of these autonomous vehicle cloud computing features. There would be many prerequisites before autonomous vehicles can be integral parts of cloud computing, some of which might only be technical, while others would be both technical and non-technical. Privacy-preserving mechanisms will be the key to achieving integration of cloud computing and autonomous vehicles. The main function of privacy-preserving mechanisms is to extract core features from inputs, which minimize the possibility of revealing private inputs [27]. The features extracted by privacy-preserving mechanisms must have good utility, which is a common quality requirement for features used in traditional machine learning systems.

6. Future Trends and Research Directions

[28] [29]The future trends and research directions regarding private data sharing within vehicular network systems, including autonomous and connected vehicles, are multifaceted. As a first observation, it is noted that in the asdcurrently discussed mechanism the production, gathering, and usage of AVL events relying on a privacy-preserving architecture guaranteeing that an attacker (another vehicle or an entity outside the vehicular system) cannot reveal individual data information. However, the mutual exchange and fusion of the produced data

provide us with a possibility for improved cooperative management of individual vehicle trajectories based on cooperative perception and decision architectures. This perspective can be approached by defining different levels of sharing responsibilities and talking about the contribution and conclusions from different independent data sources. In this context, the concept has already been explained. The optimization and selection of which data to combine and when to combine vehicles are currently open research questions. A detailed discussion of what type of applications and algorithms for autonomous vehicles could favor such autonomy data is also an opportunity for exploiting cooperation securely.[30] Moreover, efficient algorithms allowing vehicles to perform some privacy-preserving queries over their private DB or controllers are another research challenge. The potentiality of XYZ exchanges for AV-based applications and the performances of the data as a side information of vehicles within a platoons as been demonstrated initially. However, a user-level features evaluation for improving user-perceived quality of these kind of queries remains an open question. Alternative methods to share prediction results previously discussed have to be investigated from the user-level point of view relatively to our global contribution. Moreover, various possibilities of employing the proposed mechanisms as a private path and origin-destination matching mechanism to improve routing algorithms have to be studied. Moreover, our contributions are mainly analyzed at the application level, and a full cross-layer study from the MAC level to the application level still lacks. Therefore, a joint study is needed to know how our contributions relate to the physical components of the vehicular network and how security at the MAC level may affect our mechanisms. Therefore, it is of utmost importance to understand, develop, and secure the complete set of interactions of a vehicle with other components, such as a road side unit, within a smart city.

6.1. Emerging Technologies in Privacy-Preserving Data Sharing

Under autonomous transportation of goods and stuff, only a system-level co-operative path data sharing mechanism would be struggling to meet real-time optimal path swapping amid vehicles with minimal data privacy threats. Wrapping all forms of collaborative transportation together mentioned above, we categorize those all as vehicle collaborative systems here. For the sake of confidentiality, a few studies on Assisted Vehicle Collaboration (AVC) loosely assemble a group of Autonomous Vehicles which collaborate in a real-time and modern-day with active usage in today's world, and a little summary on those has shown in the subsequent two sub-sub-section [27].

Modern autonomous vehicles contain a lot of sensors and data. Two vehicles independently collecting their own data need to properly process and share this data to avoid accidents and congestion in a traffic network. Thus, numerous issues ranging from data processing, like data reduction and filtering, to data collection from surroundings need to be addressed to facilitate the internal data sharing among and between the vehicles, called vehicle-to-vehicle (V2V) as well as vehicles-to-infrastructure (V2R) data sharing [31]. Recent advancements in networking protocols and technologies have extensively enhanced vehicular communication by introducing 5G wireless systems, intelligent and secure medium access control strategies, and cooperative intelligent transportation systems (C-ITSs). This has turned traditional vehicular communication into Vehicle-2-Everything (V2X) communication, where traditional dataset collections are further expanding to the edge, fog and cloud infrastructure as well. All such specialized expansions have witnessed the advent of an era called interconnected vehicle informatics (IVI). However, in interconnected vehicle informatics, privacy concerns such as the threat of node location obfuscation, ability to vote for unfair outcomes and the threat of nonreal-time data processing cannot be ignored [19].

6.2. Potential Research Areas for Autonomous Vehicle Cybersecurity

In that context, recent stepping to deeper domain systematic investigations by mimicking cyber status behaviors with respect to numerous use-case situations is recent scientific insight. Furthermore, these study propositions place privacy-preserving solutions in scopes of other privacy preventive mechanisms on cyber-risk in connected vehicles. Additionally, within both the vehicular discipline and D2D, it is essential that the outputs of PPDSC in the vast majority of cases will be communicated in the following research stages, but to realize them, a specific one-hop 5G facility for direct data onboarding is required. Such a message embedding system might create an even safer cyber-surrounding; by fostering a sufficiently safe method of communication, the correlations between users' behaviors on physical levels can be maintained.

Protective and effective adjustment approaches could be accomplished by integrating recent ML and AI strategies with vehicle security procedures [21]. Leveraging the Internet of Things paradigm, as well as new cloud as well as edge and fog computing systems, could help create effective research outcomes and suggest future suggestions that might cover vehicular and intelligent transportation system architectures and published/subscribe data sharing

situations [32]. A complementary research ambition may be verification testing, since privacy-preserving data sharing is clearly a potential cybersecurity concern for intelligent transport systems (vehicles, pedestrians, and infrastructure) [33]. PPDSC outcomes might serve as a modality for more immediate conclusions attached to the secrecy designs, so further PPDSC analysis should be merged with proper verifiable investigations mimicking multisource data correlations and vulnerabilities.

7. Conclusion

In the present study, in order to design an appropriate mechanism that enables the entity to only share communications, it is not only necessary to analyze the performance of the systems with respect to sharing communications, but also to examine sharing vehicular and complementary relevant threat and bottleneck for implementing such a mechanism. It is for this reason, that in this study, we investigated all the relevant issues with respect to sharing vehicular- and , some of the important complementary issues regarding this mechanism have also been touched on (e.g., autonomous driving, etc.). Accordingly, this study can be used as an effective starting point for formulating related policies and decision-making-support systems. In addition to the identification of important considerations regarding the implementation of a mechanism for minimizing the costs of participation individuals in an IoT network, the network technologies that require new policies and economic models to increase or to develop a new market for these products have also been discussed.

[7] Non-cooperation and conflicting interests can quickly escalate into serious road traffic crashes caused by driv- ers due to the lack of cooperation; and this is when the limitations in the individual vehicle perception and other sensor-based pre- dictive algorithms in autonomous driving technology expose their disadvantages .As the main and most mature IS aim of IoV is to provide road users with real-time and accurate road traffic information for the purposes of driving safety, identifying road conditions, and traffic efficiency improvement, the perception sensor extended to the external environment is the most intuitive and significant application for the cooperative perception of autonomous car in IoV environments.[24]We provide a comprehensive overview of the design and attributes of blog-ging vehicular networks with respect to pandemic-free data collection and aggregation in and present efficient solutions to pandemic data sharing and alerting in,,. Simpler cooperation data sharing between neighboring vehicles and a base stations can definitely improve the

detection of abnormal human driving behavior, but it can also produce a large amount of spu- 5rious data or hinder the judgment of the real abnormal human driving behavior due to the influence of realistic vast amount of car data. our work proposes and investigates a hybrid online monitoring and assessment of the safety of CAV. In offline phase, the authors explore various abnormal human driving behaviors from enormous surveil- lance data based on low-rank factorization to model essential vehi- cle information that can be considered as independent student.

8. References

1. [1] M. Yazgan, M. Varun Akkanapragada, and J. Marius Zoellner, "Collaborative Perception Datasets in Autonomous Driving: A Survey," 2024. [PDF]
2. [2] A. Plebe, G. Pietro Rosati Papini, A. Cherubini, and M. Da Lio, "Distributed cognition for collaboration between human drivers and self-driving cars," 2022. ncbi.nlm.nih.gov
3. [3] G. Cui, W. Zhang, Y. Xiao, L. Yao et al., "Cooperative Perception Technology of Autonomous Driving in the Internet of Vehicles Environment: A Review," 2022. ncbi.nlm.nih.gov
4. [4] S. Ren, S. Chen, and W. Zhang, "Collaborative Perception for Autonomous Driving: Current Status and Future Trend," 2022. [PDF]
5. Tatineni, Sumanth. "Cloud-Based Business Continuity and Disaster Recovery Strategies." *International Research Journal of Modernization in Engineering, Technology, and Science*5.11 (2023): 1389-1397.
6. Vemori, Vamsi. "Harnessing Natural Language Processing for Context-Aware, Emotionally Intelligent Human-Vehicle Interaction: Towards Personalized User Experiences in Autonomous Vehicles." *Journal of Artificial Intelligence Research and Applications* 3.2 (2023): 53-86.
7. Tatineni, Sumanth. "Security and Compliance in Parallel Computing Cloud Services." *International Journal of Science and Research (IJSR)* 12.10 (2023): 972-1977.
8. Gudala, Leeladhar, and Mahammad Shaik. "Leveraging Artificial Intelligence for Enhanced Verification: A Multi-Faceted Case Study Analysis of Best Practices and

Challenges in Implementing AI-driven Zero Trust Security Models." *Journal of AI-Assisted Scientific Discovery* 3.2 (2023): 62-84.

9. [9] K. Fida Hasan, T. Kaur, M. Mhedi Hasan, and Y. Feng, "Cognitive Internet of Vehicles: Motivation, Layered Architecture and Security Issues," 2019. [PDF]
10. [10] S. Paiva, M. Abdul Ahad, G. Tripathi, N. Feroz et al., "Enabling Technologies for Urban Smart Mobility: Recent Trends, Opportunities and Challenges," 2021. ncbi.nlm.nih.gov
11. [11] V. Kumar Kukkala, S. Vignesh Thiruloga, and S. Pasricha, "Roadmap for Cybersecurity in Autonomous Vehicles," 2022. [PDF]
12. [12] S. M Mostaq Hossain, S. Banik, T. Banik, and A. Md Shibli, "Survey on Security Attacks in Connected and Autonomous Vehicular Systems," 2023. [PDF]
13. [13] S. Lee, Y. Cho, and B. C. Min, "Attack-Aware Multi-Sensor Integration Algorithm for Autonomous Vehicle Navigation Systems," 2017. [PDF]
14. [14] B. Ma, X. Wang, X. Lin, Y. Jiang et al., "Location Privacy Threats and Protections in Future Vehicular Networks: A Comprehensive Review," 2023. [PDF]
15. [15] E. Jafarigol, T. Trafalis, T. Razzaghi, and M. Zamankhani, "Exploring Machine Learning Models for Federated Learning: A Review of Approaches, Performance, and Limitations," 2023. [PDF]
16. [16] J. Wang, R. Zhu, S. Liu, and Z. Cai, "Node Location Privacy Protection Based on Differentially Private Grids in Industrial Wireless Sensor Networks," 2018. ncbi.nlm.nih.gov
17. [17] F. Lang and Y. Zhong, "Application of Personal Information Privacy Protection Based on Machine Learning Algorithm," 2022. ncbi.nlm.nih.gov
18. [18] B. Lepri, N. Oliver, and A. Pentland, "Ethical machines: The human-centric use of artificial intelligence," 2021. ncbi.nlm.nih.gov
19. [19] S. Sultana, J. Hossain, M. Billah, H. Hossain Shajeeb et al., "Blockchain-Enabled Federated Learning Approach for Vehicular Networks," 2023. [PDF]
20. [20] Y. Duan, J. Liu, W. Jin, and X. Peng, "Characterizing Differentially-Private Techniques in the Era of Internet-of-Vehicles," 2022. [PDF]
21. [21] D. Haileselassie Hagos and D. B. Rawat, "Recent Advances in Artificial Intelligence and Tactical Autonomy: Current Status, Challenges, and Perspectives," 2022. ncbi.nlm.nih.gov

22. [22] C. Xie, Z. Cao, Y. Long, D. Yang et al., "Privacy of Autonomous Vehicles: Risks, Protection Methods, and Future Directions," 2022. [PDF]
23. [23] A. María Quintero-Ossa, J. Solano, H. Jarcía, D. Zarruk et al., "Privacy-Preserving Machine Learning for Collaborative Data Sharing via Auto-encoder Latent Space Embeddings," 2022. [PDF]
24. [24] A. M. Elbir, G. Gurbilek, B. Soner, A. K. Papazafeiropoulos et al., "Vehicular networks for combating a worldwide pandemic: Preventing the spread of COVID-19," 2022. ncbi.nlm.nih.gov
25. [25] S. A. Abdel Hakeem, H. H. Hussein, and H. W. Kim, "Security Requirements and Challenges of 6G Technologies and Applications," 2022. ncbi.nlm.nih.gov
26. [26] S. Malik, M. Ahmed Khan, and H. El-Sayed, "Collaborative Autonomous Driving—A Survey of Solution Approaches and Future Challenges," 2021. ncbi.nlm.nih.gov
27. [27] C. Hati, G. Kumar, and N. Mahajan, "$bar{B}rightarrow D^{(ast)}tau bar{nu}$ excesses in ALRSM constrained from B, D decays and $D^{0}-bar{D}^{0}$ mixing," 2015. [PDF]
28. [28] G. Abdelkader, K. Elgazzar, and A. Khamis, "Connected Vehicles: Technology Review, State of the Art, Challenges and Opportunities," 2021. ncbi.nlm.nih.gov
29. [29] Y. AlSaqabi and B. Krishnamachari, "Incentivizing Private Data Sharing in Vehicular Networks: A Game-Theoretic Approach," 2023. [PDF]
30. [30] J. Joy, D. Gray, C. McGoldrick, and M. Gerla, "XYZ Privacy," 2017. [PDF]
31. [31] M. Ul Hassan, M. Husain Rehmani, and J. Chen, "Differential Privacy Techniques for Cyber Physical Systems: A Survey," 2018. [PDF]
32. [32] Y. Wang, Z. Su, Q. Xu, T. H. Luan et al., "Secured and Cooperative Publish/Subscribe Scheme in Autonomous Vehicular Networks," 2023. [PDF]
33. [33] F. Berman, E. Cabrera, A. Jebari, and W. Marrakchi, "The impact universe—a framework for prioritizing the public interest in the Internet of Things," 2022. ncbi.nlm.nih.gov