Emerging Privacy and Trust Issues for Autonomous Vehicle Systems

Thai-Hung Nguyen*, Truong Giang Vu†, Huong-Lan Tran‡ and Kok-Seng Wong§
College of Engineering and Computer Science, VinUniversity
Hanoi, Vietnam
Email: *20hung.nt@vinuni.edu.vn, †20giang.vt@vinuni.edu.vn, ‡20lan.th@vinuni.edu.vn, §wong.ks@vinuni.edu.vn

2022 International Conference on Information Networking (ICOIN) | 978-1-6654-1332-9/22/$31.00 ©2022 IEEE | DOI: 10.1109/ICOIN53446.2022.9687196

***Abstract*—In the awakening of cutting-edge technology, companies such as Apple, Waymo, and Tesla are racing to launch the industry's first fully autonomous car. Besides the technical challenges such as safety and infrastructure, privacy and data protection have attracted the autonomous vehicle industry and researchers' attention. In particular, it is hard for autonomous vehicle manufacturers to impose substantive privacy and security protections when different vendors and suppliers are involved in vehicle production. Although we know how much data autonomous vehicles will generate per day, there is a lack of knowledge of how the collected data will be used (e.g., real-time broadcasting and offline analytic). The privacy risks associated with data collection raise individual concerns in autonomous vehicle systems. For instance, when location information is combined with personal information, a person's details such as wealth status, profession, sexual association, and religion can be deduced. The misuse of present and historical travel patterns also puts someone susceptible to physical harm or stalking. Driven by mutual benefits or regulations, specific data must be shared in real-time or published for analysis or research purposes. This paper discusses the emerging privacy and trust issues that are essential to motivate the acceptance of autonomous vehicles operating on public roads.**

***Index Terms*—autonomous vehicles, self-driving car, privacy concerns, trust issues**

I. Introduction

Autonomous vehicles (AVs) such as self-driving cars contain smart devices that connect and exchange data with services, software, and networks inside the vehicle, other vehicles, and road infrastructure via the Internet. It is an emerging technology that has drawn significant attention from automotive and tech companies due to its potential to offer a wide range of benefits, including reduced driver stress, improved productivity, enhanced traffic safety, and increased mobility [1]. In addition, the technology further improves environmental impacts where it helps traffic planning reduce road congestion and hence, reduce fuel consumption and CO_2 emissions [2]. As a result, the autonomous vehicle market was projected to be US$219.21 billion in 2025 [3].

As the development and testing of self-driving car technology have progressed, AVs are becoming massive data hubs that collect a wide variety of data from multiple resources (e.g., vehicle, sensors, and smart devices). Data such as speed, energy consumption, engine performance, location, driving habits, and objects detected in its surroundings will be processed, stored, and shared with different parties for various purposes, including driver profiling, traffic planning, and safety improvement. The automotive companies face significant challenges in balancing the extensive collected data and the safety on the roads [4]. Although sharing and publishing these data have enormous benefits, several privacy concerns arise as there is a lack of knowledge of how these data will be protected.

The privacy risks associated with data collection in AVs raise individual concerns. For instance, location information availability provides a precise and comprehensive record of a person's movements. Such location-tracking information can reflect someone's wealth of details, profession, sexual association, and religion. Also, misuse of present and historical travel patterns can put someone susceptible to physical harm or stalking. Driven by mutual benefits or regulations, some data must be published for analysis or research purposes. For example, in Usage-Based Insurance (UBI), insurance companies require data related to miles driven, driving behaviors, and location to determine the premium rates for different users [5]. Similarly, Tesla releases its vehicle safety data to provide critical safety information to the public. Therefore, it is inevitable to release a microdata dataset, which allows valuable analysis (data utility) to be performed while guaranteeing that sensitive information is appropriately protected (data privacy). To resolve the tension between data privacy and utility needs, the scientific community has been devoting significant efforts to investigating privacy-enhancing technologies for this purpose.

Issues of privacy and trust remain understudied in the design and implementation of autonomous vehicles. These issues are becoming more crucial when today's vehicles are subjected to cyber-attacks that target vehicular communications [6]. As reported in [7], security researchers managed to control a Chrysler Jeep Cherokee by exploiting vulnerabilities within the vehicle's entertainment and navigation system. The car was forced to stop in the middle of traffic. In another incident [8], the members of the Keen Security Lab (a division of the Chinese firm Tencent) reported that attackers could access to Controller Area Network (CAN) bus of the BMW cars. The recent attacks raise safety concerns and affect the public trust and confidence in the AV system. As reported in a survey result [9], only around 15% of the respondents trust or would trust an autonomous car. However, the majority has a certain level of initial trust and tends to try out and utilize a semi-autonomous vehicle.

In this paper, we focus on discussion related to the emerging

privacy and trust issues essential to motivate the acceptance of AVs operating on public roads. Furthermore, we identify types of sensitive data and privacy threats in AVs.

A. Paper Organization

The remainder of this paper is structured as follows: In Section II, we discuss the development of the self-driving car, its architecture design, and an overview of the autonomous vehicle systems. Section III discusses the emerging privacy and trust issues for autonomous vehicle systems, and possible technological solutions are presented in Section IV. The conclusion and future directions are in Section V

II. Background

A. Typical Architecture of Self-Driving Cars

For navigation and making decision purposes, autonomous cars are equipped with various sensors: Camera, LiDAR (Lighting and ranging), radar (long-range and short-range), and other supporting devices (hardware and software). The architecture of the autonomy system of self-driving cars is typically organized into two main parts: the perception system and the decision-making system [10].

The perception system is responsible for estimating the car's state and creating an internal (to the self-driving system) representation of the environment by using data captured by onboard sensors such as Light Detection and Ranging (LIDAR), Radio Detection, and Ranging (RADAR), camera, Global Positioning System (GPS), and Inertial Measurement Unit (IMU). The perception system requires precise information of sensors to return accurate estimation [11].

The decision-making system is responsible for navigating the car from its initial position to the final goal defined by the users, considering the current car's state and the internal representation of the environment, traffic rules, and passengers' safety comfort. The system is commonly partitioned into many subsystems responsible for route and path planning, behavior selection, motion planning, obstacle avoidance, and control. However, this partitioning is somewhat blurred, and there are several different variations in the literature [11].

B. Autonomous Vehicle Systems

In general, autonomous vehicle systems consist of the following main components:

- **Users**, a party who drives the vehicle (driver) or inside the vehicle (passenger).
- **Vehicle**, a connected car capable of communicating with smart devices, other vehicles, and road infrastructure via various communication channels.
- **Smart things**, wearable devices by the users, embedded devices, sensors, cameras, LIDAR, etc. installed on the vehicle.
- **Communication channels**, telecommunication networks such as vehicle-to-everything (V2X), vehicle-to-infrastructure (V2I), vehicle-to-grid (V2G), and vehicle-to-vehicle (V2V) used to support the data exchange, sharing, and storing.
- **Cloud and edge**, computing resources for offline analytics, data storage, and real-time processing.
- **Infrastructure**, road infrastructures such as traffic lights, land markings, road signs, etc.

The interaction of autonomous vehicle systems' components is shown in Fig. 1.

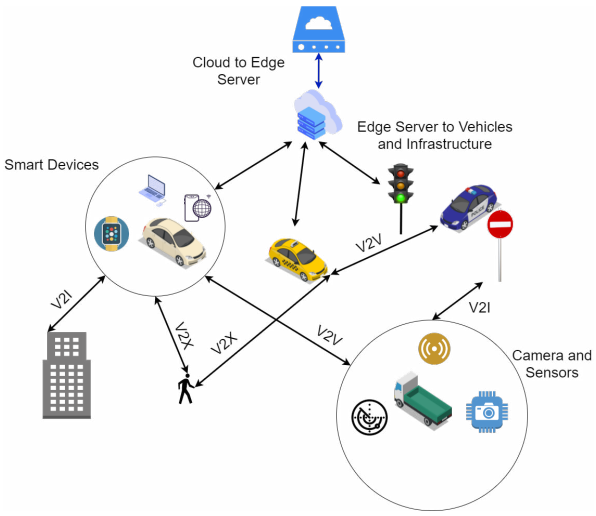

Fig. 1. Interaction of components in autonomous vehicle systems.

C. Communication Technology

Vehicle-to-everything (V2X) technology refers to the communication of all intelligent transportation systems on the road, including vehicles, pedestrians, communication channels, infrastructure, and telecommunication networks [12]. The connectivity of V2X produces more accurate information about the traffic situation across the entire network, and hence, improves the traffic flows and reduces accidents [13].

In V2X, the communication can be intra-connection (e.g., sensors in the vehicle) or inter-connection (e.g., vehicles to vehicles). The intra-connection network comprises a collection of sensors that are located in the vehicle. The interactions among sensors are bridged via Ethernet, ZigBee, or WiFi connections. Inter-connection network covers the communication between the vehicle and surrounding objects or devices. It comprises four entities: on-board unit, roadside users, roadside unit, and cloud server. An on-board unit is equipped in each vehicle to process the collected data and interact with surrounding entities. Besides, roadside users and units are human on the road (e.g., pedestrians, motorcyclists, bikers), and the transportation infrastructure unit on the roadside, respectively. All entities on the road, traffic are controlled by a cloud or central server. [12].

III. Emerging Privacy and Trust Issues

When considering privacy protection in AVs, an important question is what data will disclose an individual's privacy. Regarding this concern, we categorize AV data into two categories: primary and secondary data. Primary data such

as credit card details, location tracking, bio-metric, and financial records can directly disclose an individual's identity. Secondary data is not unique identifiers but can re-identify individuals when combined or linked with other information. Some secondary data are driving habits, environment information, and the gender of the driver or passenger.

This section will discuss AVs' emerging privacy and trust issues, focusing on privacy threats such as identity disclosure, location disclosure, user profile disclosure, and linkage attacks (e.g., linking data traffic with identity).

A. In-Vehicle

In AVs, the sensors situated in different vehicle parts will continuously collect data from their surroundings. These data are essential for the AVs to identity navigation routes, avoid obstacles or recognize traffic light signals. The data generated significantly affects how and who can access and exploit the data [14]. For example, when the users (driver and passengers) are inside the vehicle, the dash cameras' visual data shows their identity via their facial attributes. By observing the images and videos at a specific time, the adversary can learn the driver and passengers' behavior and other sensitive information related to the users. Also, the dash camera may capture the screen of smart devices, e.g., a smartphone, smartwatch, or a computer used inside the vehicle. This will lead to the reveal of messages, notifications, or entertainment content displayed on the screen. Consequently, the adversary can learn users' plans (companies' strategies), lifestyle preferences, and other sensitive information.

As shown in [15], it is possible to predict the gender, range of age of drivers and passengers through visual images with high accuracy. Similarly, abnormal medical symptoms or any user habits might also be revealed in the same manner. Such information can be sensitive when combined with other information retrieved from different data sources (e.g., nation, religion, individual interests, and identity information) to reveal the vehicle and driver's identity. As reported in [16], researchers can identify patients by linking anonymous medicare data with data from other sources. In addition to visual data, voice data also can be used for identifying a person. Hackers can use voices from the phone calls or conversations inside the vehicle to learn the driver or passengers' identity. Furthermore, by analyzing in-vehicle conversations, the hacker can discover users' interests at a specific time (e.g., buying a house, eating outside). Such information is valuable for marketing purposes.

Another source of information leakage inside self-driving vehicles comes from embedded software and applications installed in the vehicle and smart devices, respectively. For instance, the user's biometric data, i.e., fingerprint or voice, is used in the AV system for authentication purposes. In addition, a mobile application such as Google Map requires the sharing of GPS data for real-time navigation. GPS data, which provides real-time position and time information of a vehicle, can be leaked through transmission lines [17]. In detail, it includes start and stops destination, route information, speed, and duration. Learning this information allows hackers to precisely predict information related to address, workplace, family, job, and preference. Furthermore, movement history can reveal private trips, such as trips to psychiatrists, plastic surgeons, abortion clinics, or AIDS treatment centers [18]. Besides, current and future movements are known and predictable, resulting in location and time privacy threats. In the future, GPS data will be even more prone to be leaked out since they appear in many smart devices.

Typically, it might be challenging to trust that observing sensors in autonomous vehicles work all the time correctly. As a result, when it comes to safety, autonomous vehicles are not the best choice. In reality, staying inside an autonomous vehicle can be even riskier. This is due to low privacy protection in systematic software equipped in an autonomous vehicle, which controls the whole vehicle. By hacking this software, hackers can implicitly access any vehicles and control their movements without consent. In particular, hackers might attack the vehicle's controller system, thereby interfering with the vehicle's speed, route, and brake system. Software vulnerabilities may be the main factor that decreases the trust of the public in using AVs.

B. Vehicle-to-Vehicle

In vehicle-to-vehicle (V2V) networks, AVs broadcast speed, position, movement intentions, hazards, and traffic congestion on the roads to nearby vehicles. Such information is essential to enhance the driver's safety, avoid collisions, and recalculate the routes [19]. However, data sharing among vehicles poses serious privacy concerns because the vehicles on the roads are anonymous, and no clear information on how the shared data will be manipulated by another vehicle.

Since AV sensors can detect their surroundings, they can capture the vehicle's images from the opposite direction or near it. These images may consist of the driver and passengers' visual data, together with the car's information (model, color, and speed). Furthermore, the adversary can perform a linkage attack on a target with high accuracy if the vehicle is often detected in the exact location or specific period. The misuse of such information by unauthorized parties can cause the user profile and identity disclosure. In addition, users might lose trust in AVs due to the lack of knowledge of how sensor data will be shared and used by other vehicles.

C. Vehicle-to-Infrastructure

In vehicle-to-infrastructure (V2I) communication, vehicle On-Board Units (OBU) will communicate with static infrastructure and stationary objects on the road that possesses intelligent features such as parking management systems, traffic control systems, CCTVs, toll plazas, smart buildings, and billboards. With the rising trend in IoT development, these systems will be equipped with advanced functionalities, allowing more data exchange among devices and exposing more privacy threats to vehicle users. An example of communication between vehicles and infrastructure is the reservation for parking. Some systems, such as Bosch Automated Valet Parking, can collect data from an AV to process parking slots

[20]. All reservation requests are processed over the cloud such that no two AVs will occupy the same space.

Regarding personal information, it is used for various purposes for autonomous vehicles' operations, such as authentication and authorization, ensuring comfort and safety. If this data is leaked, it can re-identify the vehicle owner and other passengers who use the car before. This causes a trust issue for the user: whether the user can be sure that the vehicle will only send sufficient information and not the sensitive one outside, and the communication channel is secured enough not to be attacked by the adversaries.

The adversaries' attacks can also be a source of privacy threats. According to [21], below are some of the attacks related to V2I communication that can cause users' privacy breaches:

- **impersonation attack**, which enables attackers to pose as RSUs or OBUs to collect other users' data;
- **eavesdropping attack**, which allows attackers to gain access to confidential information;
- **RSU replication attack**, which moves an RSU or replicates it at another location to perform erroneous services.

In V2I communication, when the network usage among vehicles and infrastructure is recorded for an adequate amount of time, the adversary can find the data patterns for more analysis. In [22], the authors stated that an adversary can still extract information by simply observing and analyzing network traffic patterns despite data encryption. Then, combining the data with prior knowledge, an adversary can perform a linkage attack to derive a vehicle's location and the type of information during the data exchange.

Apart from the threats during communication, since information exchanged among parties can be retained in their storage, users' privacy can be compromised by possible third-party data breaches beyond their control. An example is the government traffic control system, which can record a vehicle's details on the road. Using such information, attackers can trace and analyze the route history and link details of a driver to a particular vehicle.

D. Summary of Privacy and Trust Issues

Several privacy threats related to user profile, location, and identity can occur at different communication types in AV systems. Eventually, these privacy threats will lead to trust issues that can degrade the public confidence and acceptance to use a self-driving car. Whether they can trust their vehicles to send the correct information to the proper recipients and ensure the communication is not interfered with by unwanted third parties will cast doubt on the general public to use autonomous vehicles.

Besides the privacy concerns mentioned above, the potential threats and risks in autonomous vehicle systems also cause trust issues.

- Hackers steal personal identifiable information (PII) through sensors: personal trip, location data (destinations, start point, and endpoint), time, entertainment preferences, financial information.
- Digital keys, wireless keys, and supporting mobile apps can be hacked.
- Mobile applications of the AVs are easy to be hacked, and hackers can get unauthorized access to control the steering wheel and brake system
- There is a lack of security built into many software and hardware components in the first generations of connected cars.
- Failure to use the latest security and updates. As new threats and attacks are discovered, the only effective solution is to ensure that the platforms can be easily and securely updated once deployed into the field.

IV. Technological Solutions

Smart devices in autonomous vehicle systems typically communicate over non-standard protocols that are very difficult to manage or integrate. In many cases, the system assumes that trusted resources exist to perform communication, queries, and computation for applications deployed and controlled in the vehicles or infrastructure. Therefore, there is a need to limit sharing of data generated by vehicles and smart devices. In addition, a secure protocol is essential when sharing data with other devices or infrastructures. Although there are laws and regulations for data protection, such as General Data Protection Regulation (GDPR) in the EU and Data Protection Act (DPA) in the UK, it is difficult for AV manufacturers to comply. This is because the vehicle may consist of components from different suppliers, and some companies may not be compliant with the privacy protection regulations. For instance, data types stored and transferred by separate systems within the vehicle can cause confusion and privacy concerns.

A. Edge Computing

In autonomous vehicle systems, most of the data generated by the sensors are processed in the vehicle, and various in-vehicle software requires the transfer of data to the cloud. However, due to privacy concerns, data pushed to the cloud could be limited, i.e., only transfer non-sensitive data to the cloud. Edge computing (also known as fog computing) is a paradigm that extends cloud computing to the edge of the network [23]. The basic idea of edge computing is to push the frontier of applications, data management, and services away from the centralized cloud to the network's edge. The edge architecture creates a hierarchical infrastructure for local (at the edge) and global analytics (at the cloud). With edge computing, most of the real-time process and analyze at the edge. This brings data transmission costs down and protects the sensitive data leaving the vehicle [24].

With multiple devices from different users and vehicles contributing to data in the edge, the time and cost needed to retrieve and share data will be much less compared to continue sending and receiving data from the cloud. However, data sharing at the edge must be carefully managed because raw data is generated directly from the users or devices.

B. Privacy-Enhancing Technologies

Due to the recent global developments in the privacy regulatory landscape, the stakeholders of the entire AV ecosystem should take privacy as a key element in designing a connected vehicle. The privacy-enhancing technologies (PET) can be used to provide fundamental data protection principles to an AV system, e.g., minimizing personal data use, maximizing data security, and empowering individuals [25]. For instance, privacy-by-design requires that appropriate technical and organizational measures be considered from the beginning of the product development process. It consists of several principles that can be applied from the onset of systems development to mitigate privacy concerns and achieve data protection compliance [26].

Differential privacy is a strong notion of privacy that guarantees privacy protection in the presence of arbitrary auxiliary information [27]. Intuitively, it aims to limit the information leakage from the output while a small change on the inputs. Differential privacy has been adapted to the context of location-based services to personalize the information provided to a user [28]. In the context of the AV system, we can apply differential privacy to vehicle location data. Notably, the system can add noise to vehicle location data to obfuscate the actual position of the driver or passengers.

C. Access Control

Access control involves user authentication and authorization that is usually used to confirm the identity of the users to prevent activities that could breach the system's security [29]. In the cloud, access control is used to ensure that the system's resources and services occur according to the rules defined in related security policies. It is not viable for vehicles and smart things at the edge to utilize the same access control policy over heterogeneous networks. Smart things are expected to share their resources and computation power with others. Hence, the same device can act as an access control subject or object at the same time. In the dispersed edge environment, smart things may have different administrative domains. Therefore, an appropriate access control policy should be available to limit network connection, resource access, and service communications. In other words, AVs should be able to feed data collectors only with the data required for a specific service or application. In contrast, data collectors can authenticate users and vehicles as legitimate data owners. For example, a location-based data access control solution has been proposed in [30] to ensure the vehicles can access data only if they arrive at a designated location and their attributes satisfy the access policy.

D. Data Anonymization

Many technologies offer ways to help protect privacy on personal data and sensitive information. Data anonymization is an exciting solution to protect the privacy of the users and also to bring the awareness of privacy protection during data collection [31]. The concept of k-anonymity is that each released data is indistinct from at least (k-1) other data [32]. However, k-anonymity is found vulnerable against background knowledge attacks in [33]. Hence, Machanavajjhala et al. proposed another privacy model called l-diversity model was proposed in [33] to complement the k-anonymity model. This model requires representing sensitive attributes in the released dataset with at least l "well-represented" values. In [34], a notion known as k_i–anonymity has been proposed to allow users to choose their preferred anonymity level during the data collection. Some attacks and privacy models in data publishing can be found in [35].

E. Cryptosystem

One trivial solution to achieve secure data sharing in autonomous vehicle systems requires the data owner to encrypt their data before sharing them with others; however, this approach requires additional computation power to decrypt the data before being used. In particular, the data owner needs to send the keys that are used for the data encryption to other parties; also, if the data owner revokes access rights to any user or device, he or she must re-encrypt the data with a new key and distribute the new key to other parties in the group. Therefore, this solution is impractical for deployment in the real-time application as the number of smart devices in the autonomous vehicle system could be very large.

However, cryptography is still a promising method that can be used to protect sensitive data. In 1982, Andrew Yao introduced the first two-party computation protocol, which is known as the millionaires' problem [36]. His idea was to find a way to allow two individuals to compare their wealth without revealing the extent of their wealth to each other. Since then, various secure multi-party computation (SMC) protocols have been proposed in the literature. For example, an efficient SMC protocol has recently been proposed for secure and privacy-preserving cooperative control of connected autonomous vehicles [37].

F. Federated Learning

Recently, federated learning (FL) has received significant attention from the research community due to its capability to support collaborative machine learning. FL can be used to address data governance, and privacy without requiring data exchange in a distributed environment [38]. For instance, AVs and smart infrastructures can train a machine learning model without sending data to a central server. The advances and open problems for federated learning can be found in [39]. Recently, blockchain has been used to overcome the limitations of FL, such as single point failure and possible adversarial attacks such as model update poisoning, data poisoning, and inference-time evasion attacks. In [40], blockchain-based federated learning has been proposed for a privacy-aware and efficient vehicular communication network.

V. Conclusion and Future Directions

In conclusion, we have discussed some emerging privacy and trust issues for autonomous vehicle systems and shown

that they negatively affect users' privacy and trust. By examining some technical aspects of autonomous vehicles and their communication types, we have also demonstrated that autonomous vehicles are prone to various threats and attacks that could harm users' privacy and trust in autonomous vehicle systems. Some technological solutions have also been mentioned in this paper to tackle the challenges. It is recommended that more research focusing on developing secure and privacy-preserved mechanisms while developing autonomous vehicle systems and communications is needed to ensure a better driving experience, keep users safe in traffic and their personal information protected. In that way, the autonomous vehicle industry could increase the public's acceptance and confidence to use that future kind of vehicle.

REFERENCES

[1] T. Litman, "Autonomous vehicle implementation predictions: Implications for transport planning," 2020.

[2] C. J. Haboucha, R. Ishaq, and Y. Shiftan, "User preferences regarding autonomous vehicles," *Transportation Research Part C: Emerging Technologies*, vol. 78, pp. 37–49, 2017.

[3] "Connected car market by service (connected services, safety security, and autonomous driving), form (embedded, tethered, and integrated), network (dsrc, and cellular), end market, transponder, hardware, and region - global forecast to 2025," MarketsandMarkets, 2017. [Online]. Available: https://www.marketsandmarkets.com/Market-Reports/connected-car-market-102580117.html

[4] T. K. Bijal V. Vakil and T. S. Rizzo, "Self-driving cars: Balancing safety and data privacy considerations," Available at https://www.whitecase.com/news/media/self-driving-cars-balancing-safety-and-data-privacy-considerations (2019/11/04).

[5] S. Arumugam and R. Bhargavi, "A survey on driving behavior analysis in usage based insurance using big data," *Journal of Big Data*, vol. 6, no. 1, pp. 1–21, 2019.

[6] Z. El-Rewini, K. Sadatsharan, D. F. Selvaraj, S. J. Plathottam, and P. Ranganathan, "Cybersecurity challenges in vehicular communications," *Vehicular Communications*, vol. 23, p. 100214, 2020.

[7] A. Greenberg, "Hackers remotely kill a jeep on the highway—with me in it," Tech. Rep., 2015.

[8] Z. Cai, A. Wang, W. Zhang, M. Gruffke, and H. Schweppe, "0-days & mitigations: Roadways to exploit and secure connected bmw cars," *Black Hat USA*, vol. 2019, p. 39, 2019.

[9] K. Lazányi and G. Maráczi, "Dispositional trust — do we trust autonomous cars?" in *2017 IEEE 15th International Symposium on Intelligent Systems and Informatics (SISY)*, 2017, pp. 000 135–000 140.

[10] B. Paden, M. Čáp, S. Z. Yong, D. Yershov, and E. Frazzoli, "A survey of motion planning and control techniques for self-driving urban vehicles," *IEEE Transactions on intelligent vehicles*, vol. 1, no. 1, pp. 33–55, 2016.

[11] C. Badue, R. Guidolini, R. V. Carneiro, P. Azevedo, V. B. Cardoso, A. Forechi, L. Jesus, R. Berriel, T. M. Paixao, F. Mutz *et al.*, "Self-driving cars: A survey," *Expert Systems with Applications*, p. 113816, 2020.

[12] A. Alnasser, H. Sun, and J. Jiang, "Cyber security challenges and solutions for v2x communications: A survey," *Computer Networks*, vol. 151, pp. 52–67, 2019.

[13] A. Siemens, "Vehicle-to-x (v2x) communication technology," *Mobility. Siemens. Com*, p. 2015, 2015.

[14] M. McCarthy, M. Seidl, S. Mohan, J. Hopkin, A. Stevens, and F. Ognissanto, "Access to in-vehicle data and resources," *Study comissioned by European Commission CPR2419. Brussels*, p. 10, 2017.

[15] D. H. Khaung Tin, "Gender and age estimation based on facial images," *International Journal : ACTA TECJNICA NAPOCENSIS Electronics and Telecommunications*, 09 2011.

[16] "Not so anonymous: Medicare data can be used to identify individual patients, researchers say," ABC News, Dec. 18, 2017. [Online]. Available: http://www.abc.net.au/news/science/2017-12-18/anonymous-medicare-data-can-identify-patients-researchers-say/9267684

[17] W. Rahiman and Z. Zainal, "An overview of development gps navigation for autonomous car," in *2013 IEEE 8th Conference on Industrial Electronics and Applications (ICIEA)*, 2013, pp. 1112–1118.

[18] "The privacy implications of autonomous vehicles," Data Protection Report, Apr. 27, 2018. [Online]. Available: https://www.dataprotectionreport.com/2017/07/the-privacy-implications-of-autonomous-vehicles/

[19] C. V. S. C. Consortium *et al.*, "Vehicle safety communications project: Task 3 final report: identify intelligent vehicle safety applications enabled by dsrc," *National Highway Traffic Safety Administration, US Department of Transportation, Washington DC*, 2005.

[20] Bosch Global, "Automated valet parking – fast, safe, driverless." [Online]. Available: https://www.bosch.com/stories/automated-valet-parking/

[21] Z. El-Rewini, K. Sadatsharan, D. F. Selvaraj, S. J. Plathottam, and P. Ranganathan, "Cybersecurity challenges in vehicular communications," *Vehicular Communications*, vol. 23, p. 100214, 2020. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S221420961930261X

[22] D. Kozlov, J. Veijalainen, and Y. Ali, "Security and privacy threats in iot architectures." in *BODYNETS*, 2012, pp. 256–262.

[23] H. F. Atlam, R. J. Walters, and G. B. Wills, "Fog computing and the internet of things: A review," *big data and cognitive computing*, vol. 2, no. 2, p. 10, 2018.

[24] S. Shurpali, "Role of edge computing in connected and autonomous vehicles," San Jose USA, Tech. Rep., 2020.

[25] V. Seničar, B. Jerman-Blažič, and T. Klobučar, "Privacy-enhancing technologies—approaches and development," *Computer Standards & Interfaces*, vol. 25, no. 2, pp. 147–158, 2003.

[26] P. Schaar, "Privacy by design," *Identity in the Information Society*, vol. 3, no. 2, pp. 267–274, 2010.

[27] C. Dwork, "Differential privacy: A survey of results," in *International conference on theory and applications of models of computation*. Springer, 2008, pp. 1–19.

[28] E. ElSalamouny and S. Gambs, "Differential privacy models for location-based services," *Transactions on Data Privacy*, vol. 9, no. 1, pp. 15–48, 2016.

[29] R. S. Sandhu and P. Samarati, "Access control: principle and practice," *IEEE communications magazine*, vol. 32, no. 9, pp. 40–48, 1994.

[30] M. Jiang, H. Wang, W. Zhang, H. Qin, and X. Sun, "Location-based data access control scheme for internet of vehicles," *Computers & Electrical Engineering*, vol. 86, p. 106716, 2020.

[31] K.-S. Wong and M. H. Kim, "Privacy-preserving data collection with self-awareness protection," in *Frontier and Innovation in Future Computing and Communications*. Springer, 2014, pp. 365–371.

[32] L. Sweeney, "k-anonymity: A model for protecting privacy," *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, vol. 10, no. 05, pp. 557–570, 2002.

[33] A. Machanavajjhala, D. Kifer, J. Gehrke, and M. Venkitasubramaniam, "l-diversity: Privacy beyond k-anonymity," *ACM Transactions on Knowledge Discovery from Data (TKDD)*, vol. 1, no. 1, pp. 3–es, 2007.

[34] K.-S. Wong and M. H. Kim, "Towards a respondent-preferred ki-anonymity model," *Frontiers of Information Technology & Electronic Engineering*, vol. 16, no. 9, pp. 720–731, 2015.

[35] B. C. Fung, K. Wang, R. Chen, and P. S. Yu, "Privacy-preserving data publishing: A survey of recent developments," *ACM Computing Surveys (Csur)*, vol. 42, no. 4, pp. 1–53, 2010.

[36] A. C. Yao, "Protocols for secure computations," in *23rd annual symposium on foundations of computer science (sfcs 1982)*. IEEE, 1982, pp. 160–164.

[37] S. Gong, "Autompc: Efficient multi-party computation for secure and privacy-preserving cooperative control of connected autonomous vehicles," in *SafeAI@ AAAI*, 2019.

[38] K. Bonawitz, H. Eichner, W. Grieskamp, D. Huba, A. Ingerman, V. Ivanov, C. Kiddon, J. Konečnỳ, S. Mazzocchi, H. B. McMahan *et al.*, "Towards federated learning at scale: System design," *arXiv preprint arXiv:1902.01046*, 2019.

[39] P. Kairouz, H. B. McMahan, B. Avent, A. Bellet, M. Bennis, A. N. Bhagoji, K. Bonawitz, Z. Charles, G. Cormode, R. Cummings *et al.*, "Advances and open problems in federated learning," *arXiv preprint arXiv:1912.04977*, 2019.

[40] S. R. Pokhrel and J. Choi, "Federated learning with blockchain for autonomous vehicles: Analysis and design challenges," *IEEE Transactions on Communications*, vol. 68, no. 8, pp. 4734–4746, 2020.