2025 IEEE International Students' Conference on Electrical, Electronics, and Computer Science

Framework for Cloud-Based Data Management in Autonomous Vehicles

Harshith Pallapothu
Dept. of Computer Science & Engineering
PES University
Bengaluru, India
harshithpallapothu9@gmail.com

Gopi Krishna G
Dept. of Computer Science & Engineering
PES University
Bengaluru, India
gopikrishnag.9774@gmail.com

Digvijay Sunil
Dept. of Computer Science & Engineering
PES University
Bengaluru, India
digvijaysunil@gmail.com

Teja Yadav S
Dept. of Computer Science & Engineering
PES University
Bengaluru, India
tejayadav3030@gmail.com

Nagasundari S
Dept. of Computer Science & Engineering
Research Center for Information Security, Forensics and Cyber Resilience
PES University
Bengaluru, India
nagasundaris@pes.edu

***Abstract*—The increasing adoption of autonomous vehicles has driven the need for robust data management solutions that support real-time operations and ensure vehicle safety and efficiency. This work introduces a cloud-based framework for management of sensor data from autonomous vehicles, focusing on optimizing payload transmission rates. The framework leverages AWS IoT Core and AWS IoT Analytics to ensure efficient data flow from vehicle sensors to cloud storage. This framework demonstrates its potential for scalable deployment in real-world autonomous vehicle networks, contributing to the evolution of connected vehicle technologies and intelligent transport systems. This framework ensures reliable data transmission up to 250 payloads per second, beyond which data loss occurs.**

***Index Terms*—Autonomous Vehicles, Cloud Connected Autonomous Vehicles, Cloud, Framework, Amazon Web Services.**

I. Introduction

The Autonomous Vehicles (AVs) are a new technology in transportation, characterized by their ability to perceive the environment and operate without human intervention. Through the fusion of localization, perception, planning, and control technologies, AVs will change the face of urban mobility [1]. Essentially, there are two classifications of AVs: connected autonomous vehicles that engage with neighboring infrastructure and traditional AVs which can function independently and not rely on connectivity. Key technological features of AVs include automated lane changes, platooning where vehicles travel closely together to enhance road capacity and valet parking capabilities, all of which contribute to improved traffic flow and enhanced safety by reducing human error [2] . The proliferation of AVs is closely related to the concept of smart urban mobility, it has a potential to greatly affect the planning of cities and transportation systems by absorbing extra road capacity and reducing dependence on traditional vehicles. In general, there is the potential for AVs to transform urban spaces and mobility patterns, marking a significant leap forward in transportation systems [3].

Building further on the bases established with AVs, CAVs takes them to a relatively advanced level with the incorporation of sophisticated communication technologies. Self-driving and modern communication technologies interact with its world, fellow vehicles, and infrastructure. This vehicle draws all possible variability of sensors, cameras, and radar systems to be better perceptive and executable; making decisions in real-time. This connectivity proves to be vital for flow of information between vehicles and the external system, which enables the use of adaptive cruise control, lane-keeping assistance, or even automated parking [4].

In addition to these, management of large volumes of data and distribution of multimedia content necessary for both safety and infotainment applications [5] need to be considered with CAVs greatly enhancing the performance of the vehicle. Traditional CAVs rely on on-board units (OBUs), which are unlikely to meet the increased computational and communication requirements of the emerging applications. As the volume of data continues to increase, the operational limitations of on-board processing power necessitate a shift to the cloud for solutions [6].

Incorporating cloud-based services heavily enhances the capabilities of Connected and Autonomous Vehicles (CAVs) by using powerful external computational resources for real-time data processing and comprehensive data management. CAVs function as a comprehensive information system that collect, store, and process large amounts of data collected from embedded sensors, distributing this information via connected networks. These resources support applications such as autonomous driving management and traffic coordination, which enhance road safety collectively, traffic efficiency, and passenger comfort in efficient and secure utilization of these resources, along with the ability to conduct complex computations and disseminate results rapidly, poses significant challenges [7]. By the introduction of the cloud-connected CAVs as shown in Figure 1, these problems are addressed

979-8-3315-2983-3/25/$31.00 ©2025 IEEE

by allowing effortless and real-time interaction of vehicles with cloud systems, hence supporting scalable and reliable operations.

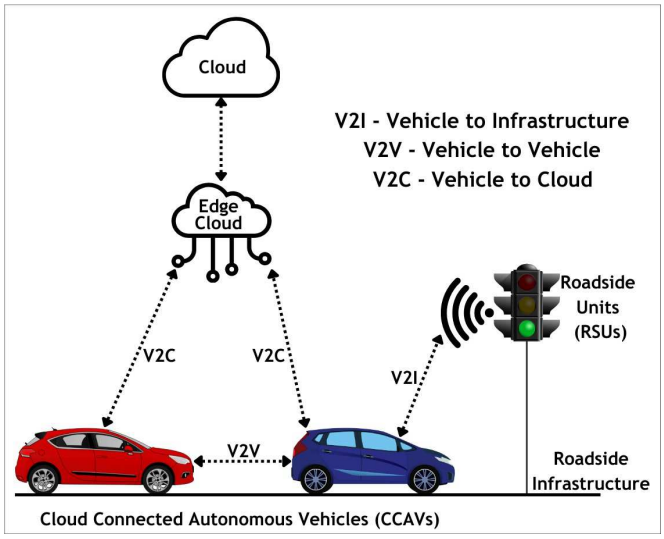

Fig. 1: Illustration of Interconnected Autonomous Vehicles through Cloud.

However, the maintenance of consistent reliability poses a significant challenge, especially given the elevated frequency of sensor updates and critical decision making processes. Recent investigations have examined cloud-based data solutions; however, only a limited number concentrate explicitly on the reliability of data transmission and storage [8]. This study aims to fill these voids by introducing a framework that prioritizes reliability across the complete data flow process.

The main contribution of this research is the development of a cloud-based framework designed for the real-time management of data in autonomous vehicles, emphasizing the transition of data from vehicle sensors to storage within AWS IoT Analytics. This framework guarantees that data transmission is reliable up to 250 payloads per second through AWS IoT Core, beyond which data loss occurs.

- **Framework**: Development of a cloud-based framework for real-time data management in autonomous vehicles.
- **Analysis of data transmission from vehicle to cloud**: Emphasis on reliable data transmission from vehicle sensors to AWS IoT Analytics for structured processing and storage, up to 250 payloads per second.

Although anomaly detection and machine learning downstream processes are not within the scope of the present work, the framework paved the basis for subsequent analysis of data from autonomous vehicles by ensuring that such data is stored securely and prepared for advanced applications.

The rest of the paper is organized as follows. Section II reviews background work on AVs, CAVs, with a focus on reliability. Section III outlines the framework, explaining the role of AWS IoT Core and AWS IoT Analytics in ensuring data flow without any data loss. Section IV entails the in detail explanation of vehicle to cloud transmission. Section V describes the role of AWS IoT Core. Section VI lists the important parts in AWS IoT Analytics. Section VII describes the framework implementation and presents the results. Finally, Section VIII concludes with conclusions drawn from the work.

II. Background Work

A. Autonomous Vehicles

The introduction of autonomous vehicles signifies a new era change in transport because these cars see their environment and perform without human intervention. The research recently conducted has evidenced the capability of autonomous vehicles in alleviating road safety, congestion reduction, and traffic management as a result of the reduction of human error [9], [10].

By the perspective of reliability, the autonomous vehicle experiences some major challenges that influence its safe and effective operation. Maintaining system redundancy and fail-safes is critical to ensure that if one component fails, others can take over to prevent system wide malfunctions [11]. AVs also face challenges related to real time data processing, delays / errors in analyzing large volumes of data can result in slow reactions, undermining safety [12]. Cyber threats further complicate reliability, as breaches could disrupt operations and pose severe safety risks [13]. Lastly, complex software that controls AVs needs to be continually updated to maintain performance and security [14]. However, changes always carry a potential to introduce new errors. In order to attest to the reliability of the AVs, comprehensive testing across a wide array of scenarios is required; however, covering all possible real-world conditions is still a difficult task.

B. Connected and Autonomous Vehicles

Connected Autonomous Vehicles is the up-to-date level of automotive technology that integrates self-governance with connectivity for communicating other vehicles (V2V), infrastructure (V2I), and other external systems, V2X. Most academic work in CAVs has spanned diverse research areas from the foundational technological frameworks supporting their operation to the challenges these systems face as they continue to grow [15].

A large body of research has focused on communication technologies that enable CAV networks. Work has analyzed V2X protocol deployment, spotlighting low-latency information communication which is key in applications where assurance dominates the consideration [16]. Many researchers have emphasized the importance of adequate data routing, robust signal processing, and adaptive protocols maintained if performance is to be maintained in conditions of high traffic density [17].

C. Cloud-Based Data Management in Autonomous Vehicles

Cloud-based architectures have been the thrust of research to improve the management of real time data generated by

autonomous vehicles. In this regard, one of the useful methods of such enormous resources is the creation of vehicular clouds (v-clouds) [7]. Generally, v-clouds can provide vehicle-to-vehicle communication and even self-organization of vehicular ad-hoc networks (VANETs), greatly enhancing data sharing and processing. The collection of real-time data within these networks is essential for facilitating responsive decision-making, which subsequently improves road safety by enabling vehicles to swiftly adjust to evolving driving conditions.

Cloud-connected autonomous vehicles (CCAVs) utilize distributed resources in order to process and make real-time decisions based on the data. A new approach involves integrating external sensor networks with onboard systems to help reduce hardware redundancies and operation costs [18]. One of the most prominent approaches is the mounting of LiDAR sensors on roadside infrastructure, such as lamp posts. The vehicles can share information with roadside infrastructure without the use of costly onboard sensors, and their computing capability is limited. Therefore, the task of processing takes place in the edge-cloud servers. The use of edge-cloud servers would ease the computation/communication trade-off for CCAVs so that sensor data could be provided to be transformed into environment maps effectively and efficiently [19].

utilization to sustain reliability in progressively dynamic environments.

III. FRAMEWORK

Figure 2 represents the proposed real-time cloud-based data management framework for autonomous vehicles, which efficiently manages sensor data and transmits it to the cloud for processing and storage. Below we consider significant constituents in this framework that ensure reliable data transmission up to 250 payloads/sec.

A. Vehicle Data Collection and Transmission

The autonomous vehicle is provided with sensors such as LiDAR, GPS, cameras, radar as well as IMUs that gather real-time data about the vehicle's environment, speed, position and orientation. In this framework, the focus is on the Inertial Navigation System (INS), which includes speed, rotational data (x_rot, y_rot, z_rot), rotational angle (rot_angle), and positional coordinates (x_pos, y_pos, z_pos).

The MQTT protocol is used to transfer the gathered data to the cloud. The protocol is lightweight and efficient in the transfer of the data. Data is serialized to JSON format for compatibility with cloud services.

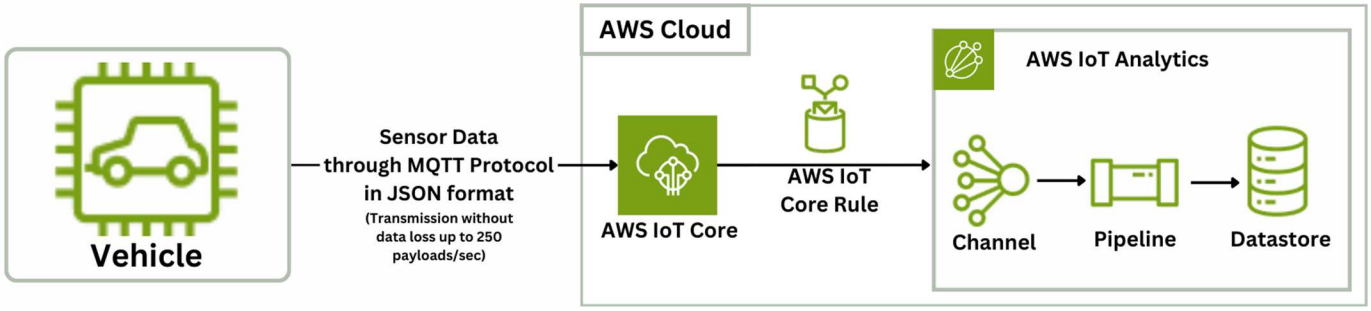

Fig. 2: Framework for real-time cloud-based data management for an autonomous vehicle.

D. Challenges in Ensuring Reliability in CCAVs

Despite all these improvements in cloud-based data management for autonomous vehicle (AV) networks, maintaining consistent reliability as the systems scale is a significant challenge ongo- ing. Security and privacy concerns have been emphasized as effective challenges to the reliability of cloud-based vehicular communications, particularly with an increasing number of connected vehicles [20]. These challenges must be overcome to ensure low latency and high performance with an increasing number of connected vehicles. Furthermore, methodologies including multipath - based packet duplication have been in- vestigated to enhance the reliability of vehicle-to-cloud (V2C) communication [21]. These strategies are designed to reduce redundancy while maintaining consistent data transmission amidst increasing network complexity. This highlights the necessity of achieving an equilibrium between redundancy and effective resource

A customized AWS SDK is used for access to AWS IoT Core, thus ensuring secure transmission of the data.

The SDK manages, tasks like data serialization, encryption and connection management, ensuring the data is routed securely for further processing in the cloud.

B. AWS IoT Core: Secure Data Ingestion Hub

AWS IoT Core takes responsibility for the secure ingestion of the sensor data from the vehicle and directs it to downstream services like AWS IoT Analytics. The platform supports secure and reliable communication between the IoT devices , that is, the vehicle and cloud services of AWS. Using AWS IoT Core, the vehicle's sensor data is securely encrypted during transmission to ensure data privacy and integrity. AWS IoT Core supports Rule Engine functionality, which allows the framework to filter incoming data based on predefined rules. This engine processes and directs the sensor data to AWS IoT Analytics for further processing. By using

AWS IoT Core, the framework ensures that data is efficiently routed to the next processing stage while maintaining secure communication and reliability.

C. AWS IoT Analytics: Data Processing Pipeline

Once the data is received at the AWS IoT Core, it is forwarded to AWS IoT Analytics for processing. The data passes through the following stages in the pipeline:

- **Channel**: The entry point where data is collected from AWS IoT Core in JSON format.
- **Pipeline**: Data is transformed, filtered, and enriched (e.g., adding timestamps) for storage.
- **Datastore**: The processed data is securely stored in JSON format, enabling future access and analysis.

D. Vehicle Data Flow to AWS Cloud Infrastructure

Algorithm 1 Real-Time Data Flow from Vehicle to AWS Cloud

Initialize vehicle sensor: `INS`
while Vehicle is operational **do**
  Collect sensor data: `speed`, `rotational data`, `rotation angle`, `coordinates`
  Serialize data in JSON format
  Encrypt data using AWS SDK for secure transmission
  Connect to AWS IoT Core via MQTT protocol
  Transmit encrypted data to AWS IoT Core (up to 250 payloads/sec to ensure no data is lost)
  Receive acknowledgment from AWS IoT Core
  if data received successfully by AWS IoT Core **then**
    Forward data to AWS IoT Analytics through Rule Engine
    Process data in AWS IoT Analytics:
      Channel: Collect data in JSON format
      Pipeline: Transform, filter, and enrich data (e.g., add timestamps)
      Datastore: Store processed data securely
  else
    Log error and **Retry** transmission
  end if
end while
Ensure TLS encryption for secure transmission and storage at each stage.

E. Security Considerations

In the aspect of security, AWS provides robust mechanisms for protecting data both in transmission and at rest. Data travels from the vehicle to AWS IoT Core using TLS encryption and secure access to it is ensured through identity and access management (IAM) policies. Moreover, AWS IoT Analytics Datastore has data stored securely so that sensitive vehicle data gets protected through all its lifecycle.

IV. Vehicle Data Transmission

Sensor data of the vehicle is captured in the CSV format and uploaded to the cloud by means of a custom AWS SDK. The CSV file captures all the readings by the INS from the vehicle, such as time, speed, Rotational axes (x rot, y rot, z rot), rotational angle (rot angle), and positional coordinates (x pos, y pos, z pos). All these data are thus used to monitor the status of the vehicle and navigate safely through the space.

MQTT protocol is used for the transmission of data from vehicle to cloud with reliable and efficient data transfer. The custom AWS SDK securely sends data to AWS IoT Core, where serialization of data is carried out (into the JSON format), facilitates data connectivity, and secures it with encryption. It uses Transport Layer Security (TLS) on top of MQTT, which uses security files such as certificates and private keys to ensure protection for the transfer of data.

During the payload transmission from vehicle to cloud, the cloud sends an acknowledgment for each payload that is received. Therefore, for 4,000 payloads of data which are sent, a total of 8,002 payloads are stored in the datastore: 4,001 original payloads and 4,001 acknowledgment payloads.

V. AWS IoT Core for Real-Time Data Ingestion

A. Role of AWS IoT Core:

AWS IoT Core serves as the central hub for managing real-time data transmission between the vehicle and cloud infrastructure. It acts as the gateway for securely receiving data from the vehicle's sensors, ensuring reliable and efficient communication between the vehicle and the cloud. The role of AWS IoT Core in ingesting sensor data, processing it in real time, and routing it to downstream services for further analysis.

B. Managing Large Volumes of Sensor Data:

To manage the large amount of data generated by each vehicle, AWS IoT Core allocates a separate MQTT topic to each vehicle. This ensures that the data from each vehicle is segregated, allowing for efficient routing and management of real-time sensor data. The MQTT protocol allows for lightweight communication and minimizes network bandwidth usage, while each vehicle's unique topic ensures scalability and low- latency transmission, even as the number of vehicles in the fleet increases.

C. Message Routing to AWS IoT Analytics:

The Rules Engine of AWS IoT Core examines any incoming data against predetermined rules and then routes the data into appropriate services for further processing. All the data, which matches the criteria specified within the rule, is passed on to AWS IoT Analytics or other AWS services. Thus, it ensures that only relevant data is passed along for further analysis, thus overheads will be reduced and the whole framework will become efficient.

VI. AWS IoT Analytics: Data Pipeline and Storing

Once data is received at the AWS IoT Core, it is forwarded to AWS IoT Analytics for processing. Preparing the data for analysis and storage takes it through several stages in the pipeline. The elements are as follows:

- **Channel**: The Channel is the entry point for real-time vehicle data, collected in JSON format from AWS IoT Core. The sensor data, including position, speed, and orientation, is ingested here before moving to the next stage.
- **Pipeline**: Here, the data flows through the Pipeline for processing. The transformations and enrichments happen at this phase. In this, unnecessary fields are filtered out, meta-data like timestamps are added, and the result is ready to be stored and analyzed in the future.
- **Datastore**: The final stage is the Datastore, where the processed data is securely stored in JSON format. This structured storage ensures the data is easily accessible for future queries, analysis, and integration with other AWS services.

Storage in the Datastore is very structured, making it easy to directly retrieve and opening up diverse applications such as machine learning, predictive analytics, real-time anomaly detection, etc. Now that the data stored in JSON format is ready to be accessed by services like Amazon SageMaker to train models or AWS Lambda for event-driven processing , autonomous vehicle sensor data can now be effectively managed with a scalable approach.

VII. Results

This section represents the outcomes of evaluating the proposed cloud-based data management framework for autonomous vehicles(AVs) in a controlled simulation environment. Using a vehicle simulator, sensor data was generated and transmitted via a custom SDK over the MQTT protocol to AWS IoT Core. The data was then processed and stored in AWS IoT Analytics, allowing for comprehensive assessment of data transmission reliability under real-time conditions up to 250 payloads/sec.

A. Definition of a Payload

A single unit of sensor data transmitted from the autonomous vehicle per unit time. In this context, data transmission is reliable up to 250 payloads per second, beyond which data loss occurs. Each payload contains key sensor readings, such as time, position, rotation, and speed. An example payload is shown below:


```
{
  "Time": "0.6",
  "x_rot": "0",
  "y_rot": "1",
  "z_rot": "0",
  "rot_angle": "0",
  "speed": "3.42",
  "x_pos": "370",
  "y_pos": "-368.96",
  "z_pos": "0"
}
```


B. Performance Metrics

The performance of the framework was analyzed using the following metrics:

- **Data Loss Rate**: The percentage of data packets lost during transmission, indicating framework reliability.
- **Packet Delivery Ratio (PDR)**: The ratio of the number of packets received by destination to the number of packets sent by sender in a network.
- **System Throughput**: The rate at which the system processes data, measured in payloads per second.

C. Experimental Results

Table I summarizes the results of the framework:

- **Data Loss Rate**: Achieved minimal loss rate, indicating no packet loss for transmission rates up to 250 payloads/sec.
- **Packet Delivery Ratio (PDR)**: Measured at maximal delivery ratio, demonstrating reliable delivery of all packets under optimal conditions.
- **System Throughput**: The maximum sustainable throughput was 250 payloads/sec, beyond which data loss increased exponentially.

TABLE I: Performance Metrics of the Data Management Framework

Metric	Result
Data Loss Rate	~0% (up to 250 payloads/sec)
Packet Delivery Ratio (PDR)	~1
System Throughput	250 payloads/sec

D. Graphical Analysis

Figure 3 illustrates the framework's performance at 100 payloads/sec, where the data loss rate remained at minimal (~0%), confirming reliable data transmission at this rate. As explained in the section IV, total of 8,002 payloads of data is received by the cloud successfully.

To assess the framework's behavior under increasing loads, Figure 4 shows the relationship between data loss percentage and payloads, spanning from 0 to 500 payloads/sec. This graph highlights that while data loss remains minimal up to 250 payloads/sec, it increases sharply beyond this threshold.

These results confirm the framework's ability to support reliable, real-time data transmission up to a critical threshold , beyond which performance optimization is necessary for scalability.

VIII. Conclusion

The work introduced a real-time, cloud-based framework for managing data from autonomous vehicles, leveraging AWS IoT Core and AWS IoT Analytics. This framework ensures secure, reliable communication from vehicles to the cloud (up to 250 payloads/sec), providing scalable data management solutions for large fleets. By efficiently processing vehicle data in real time, the framework

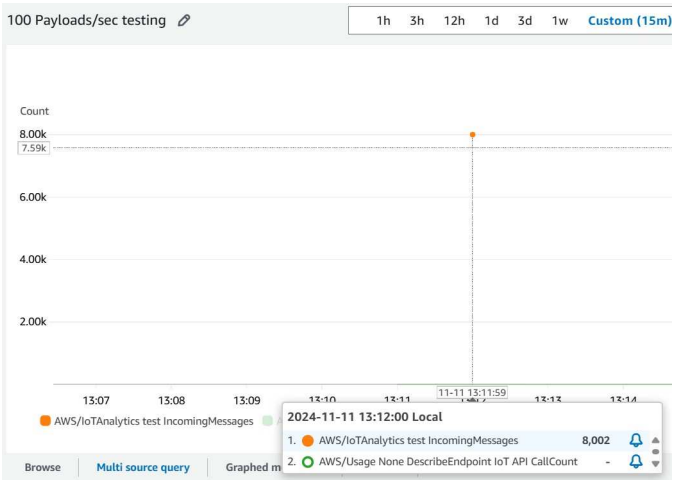

Fig. 3: Framework performance at 100 payloads/sec showing minimal (~0%) data loss.

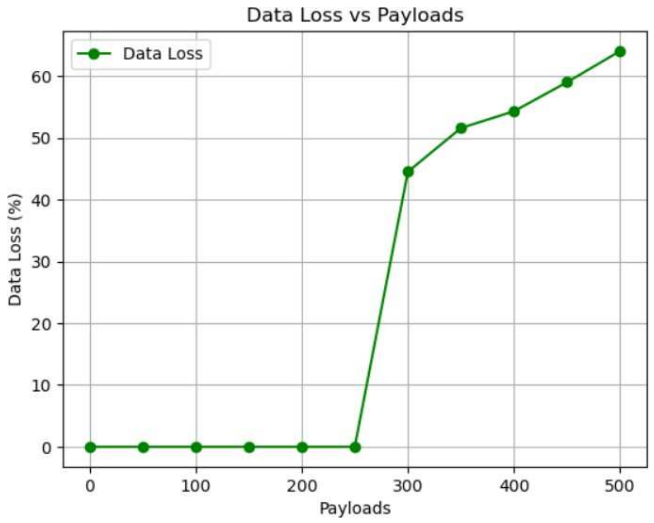

Fig. 4: Loss percentage vs. payloads (0 to 500), showing the exponential increase in data loss beyond 250 payloads/sec.

prepares it for advanced analysis, including machine learning and predictive maintenance. The integration of AWS cloud services addresses critical challenges in data ingestion, processing, and storage, establishing a robust foun- dation for modern autonomous vehicle operations. The results demonstrate the framework's reliability, making it a viable solution for the evolving needs of connected and autonomous vehicle technologies.

REFERENCES

[1] S. Kuutti, S. Fallah, K. Katsaros, M. Dianati, F. Mccullough, and A. Mouzakitis, "A survey of the state-of-the-art localization techniques and their potentials for autonomous vehicle applications," *IEEE Internet of Things Journal*, vol. 5, no. 2, pp. 829–846, 2018.

[2] A. Faisal, M. Kamruzzaman, T. Yigitcanlar, and G. Currie, "Understanding autonomous vehicles," *Journal of transport and land use*, vol. 12, no. 1, pp. 45–72, 2019.

[3] K. Bimbraw, "Autonomous cars: Past, present and future a review of the developments in the last century, the present scenario and the expected future of autonomous vehicle technology," in *2015 12th international conference on informatics in control, automation and robotics (ICINCO)*, vol. 1, pp. 191–198, IEEE, 2015.

[4] H. U. Ahmed, Y. Huang, P. Lu, and R. Bridgelall, "Technology developments and impacts of connected and autonomous vehicles: An overview," *Smart Cities*, vol. 5, no. 1, pp. 382–404, 2022.

[5] R. W. Coutinho and A. Boukerche, "Guidelines for the design of vehicular cloud infrastructures for connected autonomous vehicles," *IEEE Wireless Communications*, vol. 26, no. 4, pp. 6–11, 2019.

[6] I. W. Damaj, J. K. Yousafzai, and H. T. Mouftah, "Future trends in connected and autonomous vehicles: Enabling communications and processing technologies," *IEEE Access*, vol. 10, pp. 42334–42345, 2022.

[7] J. Kang, D. Lin, E. Bertino, and O. Tonguz, "From autonomous vehicles to vehicular clouds: challenges of management, security and dependability," in *2019 IEEE 39th International Conference on Distributed Computing Systems (ICDCS)*, pp. 1730–1741, IEEE, 2019.

[8] P. Arthurs, L. Gillam, P. Krause, N. Wang, K. Halder, and A. Mouzakitis, "A taxonomy and survey of edge cloud computing for intelligent transportation systems and connected vehicles," *IEEE Transactions on Intelligent Transportation Systems*, vol. 23, no. 7, pp. 6206–6221, 2021.

[9] I. Yaqoob, L. U. Khan, S. A. Kazmi, M. Imran, N. Guizani, and C. S. Hong, "Autonomous driving cars in smart cities: Recent advances, requirements, and challenges," *IEEE Network*, vol. 34, no. 1, pp. 174–181, 2019.

[10] B. Padmaja, C. V. Moorthy, N. Venkateswarulu, and M. M. Bala, "Exploration of issues, challenges and latest developments in autonomous cars," *Journal of Big Data*, vol. 10, no. 1, p. 61, 2023.

[11] A. Boubakri and S. M. Gamar, "A new architecture of autonomous vehicles: redundant architecture to improve operational safety," *International Journal of Robotics and Control Systems*, vol. 1, no. 3, pp. 355–368, 2021.

[12] D. Parekh, N. Poddar, A. Rajpurkar, M. Chahal, N. Kumar, G. P. Joshi, and W. Cho, "A review on autonomous vehicles: Progress, methods and challenges," *Electronics*, vol. 11, no. 14, p. 2162, 2022.

[13] K. Kim, J. S. Kim, S. Jeong, J.-H. Park, and H. K. Kim, "Cybersecurity for autonomous vehicles: Review of attacks and defense," *Computers & security*, vol. 103, p. 102150, 2021.

[14] J. Han, Z. Ju, X. Chen, M. Yang, H. Zhang, and R. Huai, "Secure operations of connected and autonomous vehicles," *IEEE Transactions on Intelligent Vehicles*, 2023.

[15] M. M. Rana and K. Hossain, "Connected and autonomous vehicles and infrastructures: A literature review," *International Journal of Pavement Research and Technology*, vol. 16, no. 2, pp. 264–284, 2023.

[16] H. Abou-Zeid, F. Pervez, A. Adinoyi, M. Aljlayl, and H. Yanikomeroglu, "Cellular v2x transmission for connected and autonomous vehicles standardization, applications, and enabling technologies," *IEEE Consumer Electronics Magazine*, vol. 8, no. 6, pp. 91–98, 2019.

[17] Q. Zhang, H. Zhong, J. Cui, L. Ren, and W. Shi, "Ac4av: A flexible and dynamic access control framework for connected and autonomous vehicles," *IEEE Internet of Things Journal*, vol. 8, no. 3, pp. 1946–1958, 2020.

[18] P.-Y. Kong, "Computation and sensor offloading for cloud-based infrastructure-assisted autonomous vehicles," *IEEE Systems Journal*, vol. 14, no. 3, pp. 3360–3370, 2020.

[19] L. Gillam, K. Katsaros, M. Dianati, and A. Mouzakitis, "Exploring edges for connected and autonomous driving," in *IEEE INFOCOM 2018-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, pp. 148–153, IEEE, 2018.

[20] Z. Yang, L. Li, F. Gu, and X. Ling, "Dependable and reliable cloud-based architectures for vehicular communications: A systematic literature review," *International Journal of Communication Systems*, vol. 36, no. 7, p. e5457, 2023.

[21] R. Teng and K. Sato, "A fundamental study of reliable vehicle-to-cloud communication using multiple paths with redundancy mitigation," *Applied Sciences*, vol. 14, no. 7, p. 2841, 2024.