High-Performance-Computing Application: Connected Autonomous Vehicles

'*A modern automobile will be a supercomputer rolling on wheels.*'

Day-after-day, the reliance of the automotive industry is increasing on High-Performance Computing or HPC. Every aspect of the modern vehicle, from design, manufacturing to electronics, will depend on HPC in some form or another.

One such innovation involving HPC lies in the area of Connected Autonomous Vehicles (or CAVs). As per the report of NHTSA (National Highway Traffic Safety Administration), CAVs could eliminate 94% of serious crashes that happen primarily because of human error. With more than 35,000 people dying every year in road crashes, economically accidents are also causing an impact of almost $600 billion ***[1]***.

With a growing concern for safety on roads, HPC empowers engineers to contrive lifesaving algorithms for future automobiles. Taking this in mind, the dependence on HPC to develop CAVs is only set to increase exponentially.

The question then comes what role does exactly HPC play in the area of modern CAVs, and how can it improve road safety?

Before diving into the answer, it is crucial to know that at the core of CAVs lies a networked environment that is capable of performing high-speed computing transactions with other vehicles (V2V), pedestrians(V2P), and infrastructure (V2I). This ability to collect, identify, process, and transmit real-time information empowers drivers with a greater sense of the events, threats, and hazards on the road.

When amalgamated with intuitive technologies that present advices, alerts, and warnings – drivers of CAVs can make informed and safer decisions while driving. Not only that, when further united with automated vehicular technologies, CAVs can respond without taking any feedback from the driver.

While advancements in AI (artificial intelligence), IoT (Internet of things), and 5g network support the development of connected vehicles, data management, and cybersecurity, on the other hand, seem to be a big problem.

The IT giant *Intel* predicted that a fully connected autonomous car would generate around four Tb (Terabytes) of data in about an hour of driving – this indicates data management is something that needs to be addressed. Moreover, relying fully on wireless networks for V2X communications, cyber threats will also be inescapable.

Not to forget, as connectivity integration grows, several trust components with a car are monitored and controlled by complex electronic systems. These electronic systems use embedded operating systems to enhance user experience. This, in short, has led to a modern vehicle – a system of interconnected sub-systems. With this level of connectivity, threats will become inevitable.

Moving forward, safeguarding the connected vehicles ecosystem is a daunting task, and the stakes are high. It is no brainer that the advances in the area of connected autonomous vehicles will bring new potential threats; however, with the growing awareness about cyber security among federal, state, public, regulatory bodies, and local governments, these threats are hardly insurmountable. For instance, in 2016, the NHTSA and the FBI issued a warning to OEMs, the general public, and other manufacturers of automotive components to "maintain awareness of potential cybersecurity threats related to connected autonomous vehicle technologies" ***[2]***.

Furthermore, the U.S. Department of Transportation and Intelligent Transportation Systems Joint Program Office (ITS JPO) funded nearly $25 million in cybersecurity research to support connected vehicle cybersecurity threat assessment ***[3]***.

The development of SCMS (Security Credential Management System) for connected vehicles was another leap towards cybersecurity; the system was developed continually for about 17 million cars in the 2017-2020 timeframe.

The SCMS is typically a public critical infrastructure-based system that ensures secure and trusted V2V (vehicle-to-vehicle) and V2I (vehicle-to-infrastructure) communications. It employs highly innovative methods of encryption and certificate management practices to ensure a secure connection between entities that have not previously communicated with each other – and would remain anonymous (as in the situation when different vehicles encounter each other on the road).

Coming to data management, at present, even at lower levels of autonomy, connected autonomous cars generate about 25 Gb of data per hour. On top of that, as more self-driving features are being advanced inside connected cars, the architecture required will only become increasingly complex. Notably, the number of sensors employed in CAVs has been increasing rapidly, and this rate will not stay the same.

Every sensor serves a specific purpose in the proper functioning of a connected autonomous vehicle. Depending on the number and setup, the amount of data generated can vary significantly. Below is a table (Referred from Lucid Motors) depicting the amount of data generated by various sensors ***[4]***.

Vehicle Automation Sensors		
Sensor	**Quantity**	**Data Generated Per Sensor**
LIDAR	1 to 5	20 - 100 Mbit/sec
Camera	6 to 15	500 - 3500 Mbit/sec
Radar	0 to 6	0.1 - 20 Mbit/sec
Ultrasonic	8 to 15	< 0.01 Mbit/sec
Vehicle Motion, GNSS, IMU	-	< 0.1 Mbit/sec

Automakers are challenged constantly with implementing intricate technologies to deal with the amount of data generated by partially and fully connected autonomous vehicles.

To tackle the problem, software companies are collaborating to address future challenges. One such example is the *Fusion Project* ***[5]***, which integrates technologies for data management from five industry providers. The aim is to assist automakers in evaluating and introduce the solution in the next-generation connected autonomous vehicles. The solution contrives an efficient and capable data lifecycle platform from data ingestion through OTA (over-the-air) machine learning model updates to maximize system decision accuracy and minimize data fidelity.

The five companies listed are a part of the *Fusion Project* –

- Cloudera – Data lifecycle solutions from Edge to AI
- Teraki – Edge data AI
- Wind River – Intelligent systems platform software
- NXP – Vehicle processing platforms
- Airbiquity – OTA (over-the-air) software management.

To summarize, data management and cybersecurity are the biggest challenges in HPC and connected autonomous vehicles. At the same time, cybersecurity algorithms are continually developed and improvised to tackle the upcoming cyber threats. Data management, on the other hand, is going towards 'big data' that would deal with managing vast amounts of constantly changing data. Additionally, the advancement of scalable IT infrastructures capable of rapid data collection, processing, and analysis is vital ***[6]***.

Getting past that hurdle will require a distributed, scalable IT infrastructure capable of supporting rapid data collection, ingestion, and analysis. Global Private connectivity to dense ecosystems of providers and enterprises/partners also enables the fast, secure exchange of data, insights, and AI models to accelerate ADAS innovation across the industry.

References –

1. https://www.nhtsa.gov/technology-innovation/vehicle-cybersecurity
2. https://www2.deloitte.com/us/en/insights/focus/future-of-mobility/cybersecurity-challenges-connected-car-security.html
3. https://www.its.dot.gov/factsheets/pdf/cv_%20cybersecurity.pdf
4. https://www.tuxera.com/blog/autonomous-cars-300-tb-of-data-per-year/
5. https://www.lhpes.com/blog/how-does-big-data-impact-automotive-industry
6. https://blog.equinix.com/blog/2020/06/03/a-driverless-future-depends-on-data/