https://doi.org/10.65025/ICAIC25050n

Artificial Intelligence and Edge Computing to Improve Internet of Vehicles.

Emmanuel Judicael NGUINGUI
Bahcesehir Cyprus University, Cyprus.
emmanueljudicael06@gmail.com

Abstract
The widespread use of electronic devices (mobile and fixed) and the growing popularity of web applications and services have had both positive and negative impact on the Internet of Things (IoT), and in particular on the Internet of Vehicles (IoV) ecosystem. IoV technology is faced with complex challenges, such as data processing, more or less delicate and demanding IT task management and high-pressure calculations, as well as fast and efficient execution of IT tasks while respecting time constraints and taking different technologies into account. We can affirm that the IoV has transformed transport systems in so far as its ecosystem enables a dynamic exchange of information and data, creating an interconnection between vehicles (Vehicular Network) as well as with the entire road network, enabling autonomous and more intelligent driving. This technology faces a number of challenges, such as high latency, energy consumption, real-time decision-making and overloads that reduce the power of the IoV and contribute to making its ecosystem highly vulnerable. Artificial intelligence (AI) has managed to carve out an important, even crucial, place in the IoV environment, helping to improve the experience of the user. AI has enhanced the capabilities of the IoV through these multiple techniques, and its impact on this technology has led to considerable improvements, particularly, in the areas of autonomous vehicle driving, like enhancing safety systems and the reduction of potential accidents. Using AI, the sensors will collect, store and analyze data on vehicle and road conditions, based on GPS technology and the practical application of computer vision that monitor the condition of vehicles and passengers. We exploited the IT potential efficiently and optimally with all available resources (Storage Server, Peripherals), and also carried out an analysis of Mobil Edge Computing (MEC) technology. This technique offers a great advantage in that it minimizes delays during data transfers in a network architecture, which contributed to a better performance and improved the efficiency of the whole system as well as digital severities. With the evolution of technology and other entities that make up the IoV ecosystem, it seems that the exclusive use of a cloud architecture is no longer able to meet or satisfy the growing functional needs in terms of speed (reduced latency), large-scale reliability, and intelligent transport management of the various options and applications adopted or used today in the automotive field. This paper provides an in-depth analysis of the various methods and processes employed to reduce latency and energy consumption in an IoV environment. We incorporated and implemented a model that combines Artificial intelligence (AI) and Mobile Edge Computing (MEC). These two elements help create a flexible and reliable IOV environment that optimizes operations like data processing and security mechanism reinforcement. We have set up a hybrid framework made up of AI and MEC, so the study is done in a meticulous way, simulations have been made focusing on the different challenges that the IoV faces. This approach enabled us to prove and attest to the gains made, including reduced energy consumption, more accurate decision-making in real time, and an increase in the system's overall resistance and durability.

Keywords
Artificial Intelligence (AI), Mobile Edge Computing (MEC), Internet of Vehicles (IoV),

1. Introduction

Today, the emergence of the Internet of Things (IoT) has brought added value to the development of technology, and has also contributed to the evolution of Web technology. The acronym, Internet of Things is the composition of two words: “Internet” and “Objects”. The Internet of Things can be presented as the set of intelligent objects, such as cars (mechanical), household appliances (electronic) and other equivalent entities, which are interconnected and are able to pass messages (communication) using intelligent sensors and sophisticated or advanced applications, using the Internet network to collect, store and analyze data to communicate with the various entities that make up the system. According to the report entitled “The Mobile Economy 2025” published by the Global System for Mobile Communication Association (GSMA), the number of Internet users in 2025 will be 5.6 billion, and this number is expected to rise to about 6.5 billion by 2030, meaning that over a 5-year period, we will see a growth of around 900 million Internet users (GSMA, 2025).

This growth has encouraged progress in IoT, but particularly, in the field of the Internet of Vehicles (IoV). Vehicle manufacturers have played a major role in the advancement of IoV technology, as vehicle design and materials have been adapted to new technologies, and vehicles are moving from independent embedded environments to interconnected systems. Today, through various transmission media such as Wi-Fi and Bluetooth technology, as well as sensors incorporated into vehicle design, vehicles have been promoted and can communicate with one another through Vehicle-to-Vehicle (V2V) technology, and also, they are able to exchange with entities in their environment through

Vehicle-to-Everything (V2X) technology, forming a basic architecture and competent transport platforms that are also intelligent. This progression is at the root of several considerable challenges, reducing the effectiveness of IoV technology. These issues are the subject of several research topics, such as latency reduction, improved real-time decision-making, bandwidth management and data security. Artificial Intelligence will enable or grant vehicles a number of cognitive computing capabilities and skills, such as moving without a driver (autonomous driving), anticipating traffic and recognizing different objects instantly and in real time. However, the fact that these functions or AI tasks are performed in the cloud generates a certain delay, and also, depends on the state of the Internet connection, which can be of good or poor quality. The implementation and use of edge computing brings data processing capabilities closer to their sources, as processors installed in vehicles or at the edges of the road environment provide an option that offers faster response and can support artificial intelligence for instantaneous actions.

The aim of this paper is to create and analyze a framework that combines Artificial Intelligence and Mobile Edge Computing in the structure of connected objects for vehicles, in order to guarantee fast, safe and intelligent services for vehicles.

2. Background and Motivation

Intelligent transport systems have made great strides with the concept of the Internet of Vehicles (IoV). This term integrates cars by linking them with different communication options and integrating network processing capabilities. We are witnessing the rise of independent cars (autonomous driving) capable of being connected, equipped with detection or sensor equipment such as Lidar, Radar, Cameras and satellite displacement models, as well as networks specifically dedicated to vehicles (VANETS). The quantity and throughput of data or information generated by these entities (vehicles) has progressed considerably. According to recent estimates, an independent vehicle could generate almost four tera-bytes (4TB) of data and information (Nirvikar k, Abhay S, Namita C, Raju S, Sudhir K, Mohd, Faraz Husain, 2024). Cloud-based IT architectures are becoming less efficient, ineffective and even vulnerable. This can result in prolonged response times, creating the possibility of congestion and unreliable security in the IoV environment, creating significant challenges.

Edge computing plays a very important role in reducing latency, as its main aim is to bring data closer to the end-user and shorten the data processing path, resulting in an immediate reduction in bandwidth, enabling instantaneous decision-making, avoiding collisions, changing direction and spotting passers-by. AI, on the other hand, increases the intelligent capacity of options and sensors incorporated into vehicles, thanks to two major techniques: Machine Learning (ML) and Deep Learning (DL). A particular feature of AI architectures is the use of multiple modes to process information from a variety of sources in order to perform various tasks (object identification, path planning and behavior prediction). The implementation of AI architecture in vehicles must respect the technical limits of computing and take current technology into account (Xiaolong X, Haoyuan L, Haoyuan; X, Weijie; L, Zhongjian; Y, Liang; D, Fei, 2022).

New research into AI's ability to reduce latency by comparing models based on cloud-based architectures shows that advanced systems that rely entirely on AI can reduce latency by almost 60% compared with environments that rely entirely on the cloud, but are also capable of restoring the accuracy of decision-making whose demand requires immediate action (Wang, Z., Li, Y., & Zhang, K., 2024). However, this incorporation also raises issues such as the management of dynamic resource allocation, system flexibility, various cyber security threats, and the adaptation of architectures to a new mobile environment. It is essential to carefully analyze and propose AI- MEC solutions in the IoV environment.

3. Literature Review

Edge Computing has become an important solution for better real-time data and information processing, as it enables data to be analyzed and manipulated from the original source of collection, which is vital for IoV network architectures. During data transfer in the IoV environment, every millisecond is important during the process. Research by Ahmed et al (2022) confirms that device load balance offers that are considerable capabilities and benefits in intelligent vehicles, and goes on to reaffirm that it can reduce latency by up to 55%, enabling an even more constant flow of data in densely populated metropolises. In the article “Edge-Enabled Vehicular Computing: Opportunities, Challenges and Future Direction”, the main problem was to compensate for Cloud Computing's limitations in terms of direct decision- making, higher latency and high data flow. The solution proposed was Edge technology in connection with components such as Edge Servers, Road Service Units (RSUs), the MEC and a Fog system. What they recommended for future research was an intelligent load balancing technique using artificial intelligence and applied machine learning methods, and a security design model for different device nodes (Ahmed, M., Rehman, S. U., and Hussain, F, 2022) .

Li et al (2023), conducted a study entitled “Integrated Sensing, Communication and Computation for IoV toward 6G”. They aim to establish a unified model capable of efficiently organizing sensing, information exchange and requirements for latency and throughput issues in 6G-compatible IoV environments. To this end, they have developed an Integrated Hierarchical Sensing, Communication and Computation (ISCC) model. Li et al (2023), put forward an IoV environment that is compatible with 6G technology, and is capable of improving reliability, architecture coverage and joint optimization of resources. They suggest an AI-based model that can be used for future

research, and also, highlighted the issues that may occur as a result of the evolution and challenges that manifest with the technology (Li T, Xu C, Zhang Y, Chen M, 2023).

Over the years, the Internet of Things (IoT) has witnessed a lot of progress, particularly in the sector of IoV. This major advance has been driven by AI on the edge, which brings together data processing on the edge with federated machine learning to contribute to decision-making while guaranteeing data security. Authors Wang et al (2024), in their paper, "Cooperative Edge AI for Connected Vehicle: Design, Implementation and Performance Evaluation" seek to solve a set of problems such as, a requirement for exchanges in V2X, the desire to reduce high latency and an equitable distribution of activities by reinforcing data sharing. They proposed a collaborative model between AI and peripheral computing, using a two-stage method in which the first stage consists of distributing the various maneuvers or tasks to the server, and the second stage prepares the exchange process. This was implemented in a simulation platform. For future research, the authors suggest that researchers focus on implementing the project in the real world, so as to be able to test and validate the effectiveness of the functionalities and different modules, taking privacy into account and introducing machine learning mechanisms (Wang, Z., Li, Y., And Zhang, K., 2024).

AI has managed to carve out an important place for itself since it contributes to the implementation of autonomous vehicle driving, particularly, in terms of vision, positioning, organization and verification. The various models of Deeps Learning and their practical application, such as the Convolutional Neural Network (CNN) and the Recurrent Neural Network (RNN), are used for deep analysis and understanding of driver behavior, object identification and trajectory prediction. Zhou et al (2024), in a recently publication entitled "Federated Deep

Reinforcement Learning Route Planning in IoV" aims to strike a balance between collective route improvement and safety in the IoV using the federated deep reinforcement learning method. Their method contributed to an improvement of about 18% in acceptable path performance and to a significant simplification of the electronic parasitic that most lead to congestion at the model level during the simulation period. As recommendations, the authors suggest a number of avenues, such as strengthening the architecture's resistance to data that is not identically distributed between cars and lowering communication costs. Moreover, they advanced the need for the practical application of the "distributed" environment (Zhou B, Liu Z, And Wang J, 2024).

4. Proposal For AI and Edge Computing Architecture in an IoV Framework

The system we are presenting is a blend or association of two major components - Artificial Intelligence and Edge Computing - within the IoV environment, enabling reliable decisions to be made at all speeds and in response to changes in the environment, guaranteeing reduced latency, collaborative detection and enhanced vehicle capabilities. This model has been built on the basis of three parts or layers, namely the cloud part, the peripheral part and the vehicle part, connected by V2X data and information exchange protocols. The system makes it possible to carry out exploits such as examination and analysis within precise timeframes, to facilitate joint and shared learning, and then, to be able to upgrade the various activities in relation to variations in the network environment. The architecture is as follows.

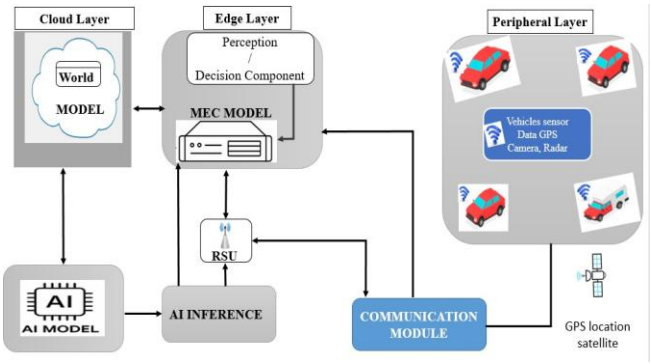

Figure 4.1: AI and Edge Computing architecture in an IOV

4.1. Parts description

- **The cloud:** The cloud is an important part of IoV architecture, as it enables data to be centralized and processed and it examines the data produced by all networked vehicles. It can also handles communication between the various players in the environment, providing predictive analysis and services, as well as adapting resources to the different needs of the IoV, taking into account the number of vehicles in operation and introducing the notion of security.

- **Mobile Edge Computing (MEC Server)**: Allows for an intelligent deployment of RSUs and MEC points for multiple access of Edge Computing in urban areas and intersections, and contributes to the stabilization of data from multiple sources (vehicles) to create a

collaborative modeling circuit. Moreover, it helps to interface operations such as combining objects and predicting paths, as well as classifying activities.

- **AI and Edge incorporates:** Vehicles are equipped with detection and protection options including camera, GPS, radar and Light Detection and Ranging (LIDAR), as well as graphics processors such as the GPU (NVIDIA Jetson), which sends information to the Restricted Stock Unit (RSU) through the communication module to sensors and also, to nearby entities. It also applies Deep Learning systems that do not require sufficient resources for local perception (YOLOv7, MobileNet), and participates in federated learning (FL) based on updating systems rather than using unprocessed data (raw data).

5. AI techniques for edge-IoV systems

The fact that Edge/IoV systems manage to correct vehicle options as normal, proves that its aim is to achieve considerable improvement by bringing the intelligence of cars closer together and implementing efficient, decentralized AI processing in direct link with the entities (vehicles) with a view to having minimal or completely reduced latency guaranteeing accelerated, fluid decision- making, data protection and information that also enables instantaneous choices to be made. Here, we look at the most essential AI methods used in Edge-IoV models, including Federated Learning (FL), Machine Learning (ML), Reinforcement Learning (RL), Deep Learning (DL), and their deployment in the context of cars.

5.1. Using machine learning to manage traffic and forecasts

Machine Learning is a crucial technique for estimating and regulating traffic. It enables reliable forecasting and manage traffic flow flexibly by implementing methods such as LSTM and GNN, as well as converters to use in an approach that can anticipate traffic speed and road congestion by establishing systems that take into account factors like space and time. It also allows for the management of traffic signs and improves route choice instantaneously. Ultimately, it reduces response time for an intelligent transport system.

5.2. Deep Learning for object recognition

Deep Learning has brought many positive developments to the computer vision sector, particularly in the areas of object identification and scenario interpretation, but these skills are also important for various intelligent models, including driverless cars and robotics. Object identification involves the recognition and location of various objects in a scenario or image. Neural networks or Convolutional Neuron Networks (CNN) and recent models such as YOLOv7 and converters are commonly used to identify and sort different entities (objects) such as cars, people and road signs in real time. The way to understand scenarios in the environment is based on the set of detections with a fragmentation of meanings and geographical links in order to decipher complicated frames, which is very important in relation to uses such as driving.

5.3. Reinforcement learning for component and displacement management

Reinforcement learning, also known as RL, has established itself as a highly effective tool for enhancing resource management and mobility in complex, evolving environments such as WI-FI networks, intelligent metropolises and advanced transportation systems. This tool enables different systems to develop the best ways of making decisions by interacting with their contexts, without first establishing the rules of marked datasets. In the field of resource management, reinforcement learning methods are used for the judicious allocation of resources in terms of exchange, energy and computer components. For example, in advanced computing and WI-FI networks, reinforcement learning is capable of dynamically upgrading the maximum throughput, processing intensity and spectrum utilization in a scalable way according to needs in a given context, taking into account network circumstances, thus maximizing transmission flow, reducing delay and minimizing energy consumption with regard to movement, RL is much more important for coordinating a number of tasks, in this case routing information at entity (vehicle) level. This technique includes multiple independent agents, such as networked cars and base sites, supporting coordinated decision-making and system operation. As the environment is constantly changing, the actions of different users changes too, while RL offers robust, adaptable and automatic coordination approaches, which are becoming increasingly important in a context where some maximization processes are focused on fixed rules that are inadequate due to instability, variations and the need for instantaneous response.

5.4. Federated training for cooperation that preserves protection

Federated Learning (FL) is an independent tool that enables multiple devices to adopt a common architecture, avoiding the need to share original information (raw data). The use of this approach makes it possible to take into account the evolving uncertainties linked to the personal protection of data and information, an aspect which is relevant within sensitive sectors such as the medical industry, the financial industry and independent devices. In the context of Federated Learning, every user forms an architecture on his or her own equipment by exploiting personal data, and can only transmit

adjustments or system parameters to centralized computers, also known as servers or converters. These adjustments are put together to optimize the overall system, while the original information always remains in the local device. This technique greatly attenuates the possibility of an intrusion capable of causing a data leak, and ensures compliance with privacy protection regulations such as the General Data Protection Regulation (GDPR). FL promotes data-protection cooperation for dispersed information resources, and enables safe, flexible AI in an increasingly connected environment. FL is much more widely used for forecasting in the sense of mobile keyboards for intelligent traffic infrastructures.
In this study, we opted for the Federated Learning technique and the Deep Learning technique, as both fit with the model we have developed and proposed.

6. Installation and Peripheral System

It is imperative to set up a system of IoV computing peripherals, so that simultaneous analyses can be carried out and feedback can be provided in the shortest possible time, enabling concrete, intelligent choices to be made. In addition, the evolution of technology has opened up an important avenue for vehicles to become autonomous, which means that resources are consumed, relying solely on central digital infrastructures (Cloud), no longer able to operate efficiently due to response times, transmission limits and issues relating to the security of resources and data. Edge computing overcomes these restrictions by placing computing capacities in different locations where end-users are located (this could be in the heart of vehicles, in RSUs and also, in mobile servers.

Components of the edge computing model: Peripheral architecture includes the computer programs and the various hardware components that make up the network, enabling the information processing process to take place close to the original source. All these components must be in communication to meet functional requirements. These components can be classified according to their functions as presented below:

1. **Peripheral equipment:** This is the starting points for data and information, and includes the following;

- ✓ IoT/IoV sensor (climate, pulse, environment)
- ✓ IP/CCTV camera (surveillance video)
- ✓ Wearable device (smart watch, tracking device)
- ✓ Electronic equipment (smart speaker)

These entities produce large volumes of data that need to be analyzed locally.

2. **Peripheral points/transition systems:** These are transition intervention systems which;

- ✓ Organizes and reinforces information derived from different digital devices.
- ✓ Executes and performs a basic analysis on information or inference based on artificial intelligence.
- ✓ Transfer data and information towards the Cloud system.
- ✓ Implement data protection rules as well as information.

3. **Edge/Micro-Server data center:** this is a robust piece of IT equipment located close to our peripherals.

- ✓ Host different activities (machine learning models)
- ✓ Résiste à la redondance et à la commutation automatique
- ✓ They frequently include on-site data backup and virtual machine set-up.

Possibility of being housed in telecoms antennas and maintenance centers, as well as in installations or mobile units.

4. **Networking and interconnection between entities**

- ✓ 5G and LTE technology: wireless transmission with reduced transmission times
- ✓ Ethernet and fiber optic support: for high-speed connections.
- ✓ LPWAN: To ensure IoT(IoV) transmission for low-cost energy use and guaranteed range.

Optimized routing has been seen as part of the network coordination options for devices, as well as wireless transmission (SD-WAN) and compliance with QoS policy.

7. Modeling Practical Case Studies

In the Internet of Vehicles (IoV), modeling and simulation scenarios offer a concrete perspective on the viability, efficiency and adaptability of artificial intelligence-based edge computing for IoV technology. In this section, we discussed all practical applications, as well as testing and verification during simulations, with the aim of demonstrating the importance of cooperation between Artificial Intelligence and Edge computing in maximizing latency reduction, accurate decision definition and bandwidth utilization.

Scenario Edge computing and AI

This involves setting up a shared Artificial Intelligence model across an urban agglomeration using devices installed at different roadside locations (RSUs) and 5G mobile computing (server) backup equipment (MEC), as shown in the following diagram:

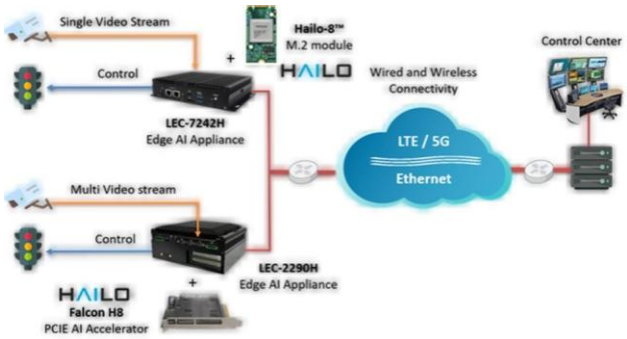

Figure 7.1. Architecture Edge computing and AI

In this implementation, the AI techniques put into practice include cooperative learning for collaborative training of network systems, Convolutional Neural Networks (CNN) for entity (object) location, and Graphical Neural Networks (GNN) for traffic prediction. This will enable us to improve traffic management based on the following model.

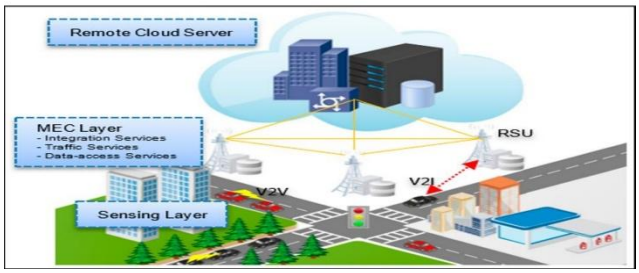

Figure 7.2: Optimization of traffic management in the metropolitan area through RSU AI performance

How it works: Automobiles perform a local analysis of basic Artificial Intelligence, RSUs compile and manage updates of regional or local structures, and finally, MEC infrastructures, more precisely MEC servers, which carries out a global reorganization process and re-share updated models. The results are as follows:

- ✓ Approximately, there has been a reduction in time of about 28 percent over a period of time until the system reaches a solution.
- ✓ Waiting time has improved, as it has been reduced from 92 ms (strictly at Cloud level) to 27 ms (taking peripherals into account).
- ✓ Reducing the size of system updates has saved 34% in bandwidth usage.

Decentralized Artificial Intelligence on the periphery preserves confidentiality while remaining capable of achieving high levels of definition or precision in studies for functionalities fundamental to protection.

8. Protection and Confidentiality

The IoV environment supports and focuses on Artificial Intelligence (AI), and thus, depends on Mobile Edge Computing (MEC) technology for its operation. Given the sheer volume of data created, analyzed and shared by automobiles instantaneously, equipment such as Roadside Units (RSUs) and peripheral servers pose major challenges in terms of tasks and confidentiality. In parallel with peripheral computing systems that allow for the creation of modules capable of large- scale verification, edge computing configuration presents a vulnerable, distributed risk surface, requiring precise solutions and processing to guarantee the principle of CID (Confidentiality, Integrity and Availability).

8.1. Security risks in the IoV or Artificial Intelligence environment

In the environment of edge-linked IoV systems using Artificial Intelligence, we have noticed a rise in protection risks emanating from both networks and the various AI zones. Factors encompassing system-related dangers include man-in-the-middle (eavesdropping), identity theft, denial of service as well as cyber-attacks and intrusions, as well as other factors affecting V2X exchanges. We need to note that, in relation to the subject of AI. Certain deceptive cases have the potential to damage perception systems, deformed architectures risk hampering the evolution of federated learning, there may be hacking of information and confidential data due to intrusions by means of inference. Peripheral links, such as RSUs and vehicles, are exposed to the risks of hardware exploitation and the addition of malicious tools. The high mobility of these devices contributes to the complexity of validation, sustainable verification and trust management.

8.2. Privacy Policy

In many IoV-AI-Edge architectures, confidential data and information, such as precise car locations, travel behavior, sensor information and individual passenger identification, are broadcast at all times and distributed across the connected cars. Signaling or roadside communication units (RSUs) and backup machines at the network's periphery. During the traffic flow examination period, lack of robust protection can lead to information merging illegally or what is referred to as system renovation. Another problem caused by traffic flow is the exposure of information. As a result of federated and collaborative learning, threats to private identity have increased. Variations and adjustments to architectures are likely to reveal confidential data. In order to ensure the security of privacy, we need to implement a number of techniques, such as discretion, secure grouping, flexible confidentiality and the application of rigorous rules for managing the various useful connections.

8.3. Protection systems for IoV at AI scale

IoV-AI-Edge systems are based on several protection measures, including PKI certification, public key

infrastructure authentication, secure V2X communication encryption and function-based access control. Immediate identification of threats or risks is made possible by the use of an intrusion detection tool in the peripheral zone, as well as AI-guided observations and analysis of disturbances. The implementation of robustness techniques has all the antagonistic training, secure Federated Learning as well as flexible protection which helps to combat aggression within the models, yet different tamper-proof equipment then protected startups that support nodes and hardware hence all of these elements increase and improve system robustness, privacy preservation as well as reliability within interconnected vehicle infrastructures.

8.4. Privacy technology

IoV systems rely on AI, and with the development of AI, it is possible to keep information private by concealing personal information using pseudonymous identifications and certifying rigorous connections to reduce the dissemination and vulnerability of confidential data. Federated Learning, combined with a protected collected and privacy rules, avoids the transfer and communication of original information in time, and ensures adjustments to architectures. Various encryption strategies, such as Uniform Encryption, make it possible to perform calculations on encrypted information, while controlling it, or carrying out in-depth audits based on the Block Chain, ensuring efficient coordination and clear, reliable, tamper-proof information management. By combining these different approaches, we have succeeded in striking a balance between the importance of private information and rigorous privacy security.

9. Suggestions for Future Research

This study has made an in-depth analysis and the results have indicated the capabilities of AI and MEC within the IoV environment, although it should be noted that there are still many diverse areas of study which it would be important to explore further. Here is a list of the future work we have proposed.

1. With AI-Edge, the deployment of these two methods amplifies the demand for resources, and then energy use becomes increasingly intensive. Future work should focus on building learning systems that are less robust in terms of energy consumption, but exploit optimized neural networks and multiple processing devices capable of running on renewable energy generators (Ahmed S And Kim H, 2022).

2. Putting test models into practice in real-life situations: much research is based on several models and virtual trials. However, concrete implementation of large-scale IoV environments with AI remains a less common practice, and it is important that future work focus on practical implementation in the real world, using different technological environments such as NVIDIA, Jetson, Huawei or even infrastructures (Servers) that support 5G technology, including the MEC system, with the aim of better analyzing results taking into account real conditions and car movements to confirm the impact of the results obtained (Hui Z, Jian X And Feng Z, 2023).

3. Despite Federated Learning's protection of data and privacy. IoV remains exposed to cyber-attack threats as well as contamination of algorithms that can compromise their reliability and performance. Future projects must be based on solid techniques to protect AI, such as flexible security and block chain verification systems (Li Y, Huang T And Zhao Q, 2023).

4. Despite Federated Learning's protection of data and privacy. IoV remains exposed to cyber-attack threats as well as contamination of algorithms that can compromise their reliability and performance. Future projects must be based on solid techniques to protect AI, such as flexible security and block chain verification systems (Wang Z , Li Y, And Zhang K, 2024).

10. Conclusion

As we come to the end of our study, we can say that we are satisfied with the work we have done, while respecting the ethics of science. This research has examined in depth, how AI and MEC technology can be combined within the IoV environment, aiming to alleviate or eradicate major problems in IoV environments such as response times, bandwidth limitations, data and information security, instantaneous decision-making in logistics and intelligent traffic devices. This paper has shown that the incorporation of AI and the MEC system, taking into account all the infrastructures on the periphery, has the potential to bring an additional point capable of considerably optimizing the connection and exchanges in a vehicular architecture, allowing applications related to safety and efficiency to remain optimal. In this article, we have highlighted the challenges arising from traditional Internet of Vehicles techniques based on cloud computing, notably long response times and susceptibility to system overloads. It has been shown that edge computing offers a decentralized architecture based on the exploitation of data and information close to the final entities (vehicles), which helps to reduce response times while reinforcing robustness. In parallel, Artificial Intelligence techniques such as Deep Learning for detection, Reinforcement Learning for orientation and Federated Learning for building architectures while protecting confidentiality, are important and can be used to promote rapid decisions and anticipatory calculations. A model was suggested for mixing AI and Edge Computing technology within automotive systems (vehicle networks)

supported by simulations and the results confirmed that this mixer method favors reduced waiting time, optimized resource utilization, improved traffic forecast accuracy and also enhanced car protection compared to conventional techniques. Aspects such as security and privacy were also addressed in this research, highlighting that Federated Learning and techniques based on Block Chain technology offer favorable prospects for protecting data and information flows directly linked to vehicles from digital threats and malicious attacks. In this work we have listed the future steps that need to be taken to improve the capabilities of the IoV environment. As a contribution to this field, we have highlighted and demonstrated that AI techniques and MEC technology are not just simple elements that complement each other, but also, beneficial and indispensable factors in advancing the IoV field. The inclusion of these two innovative, adaptable, constant, intelligent and protected vehicle network architectures will influence the outlook for traffic, transport and intelligent routing.

References

[1] Ahmed S And Kim H. (2022, May 17). *Green Edge intelligence for IoV : Emergence- aware AI Models and Renewable-Powered Edge Servers*. Retrieved from IEEE Xplore Digital Library: https://doi.org/10.1109/ACCESS.2022.3201234

[2] Ahmed, M., Rehman, S. U., and Hussain, F. (2022, August 29). Edge-Enabled Vehicular Computing: Opportunities, Challenges, and Future Directions. *Future Internet.*, 14(9):257. Retrieved from Future Internet: https://www.mdpi.com/1999-5903/14/9/257

[3] GSMA. (2025). *The Mobile Econmy.* London: 2025.

[4] Hui Z, Jian X And Feng Z. (2023). *IEEE Internet of Things Journal*. Retrieved from IEEE Explorer Digital Library: https://doi.org/10.1109/JIOT.2023.3245678

[5] Li T, Xu C, Zhang Y, Chen M. (2023, January 24). Integrated Sensing, Communication and Computation for IoV Toward 6G . *IEEE Xplore*, 27-42. Retrieved from https://doi.org/10.1109/TITS.2022.3178941

[6] Li Y, Huang T And Zhao Q. (2023). Blockchain-enhanced federated learning for secure edge-assisted IoV. *IEEE Transactions on Intelligent Transportation Systems*, 6789–6802. Retrieved from https://doi.org/10.1109/TITS.2023.XXXXXXX

[7] Nirvikar k, Abhay S, Namita C, Raju S, Sudhir K, Mohd, Faraz Husain. (2024, 4 30). AI in Autonomous Vehicles: Opportunities, Challenges,. *Educational Administration: Theory and Practice*, 6255-6264. Retrieved from Educational Administration: Theory and Practice: https://www.researchgate.net/publication/380836855_AI_in_Autonomous_Vehicles_Opportunities_Challenges_and_Regulatory_Implications

[8] Wang Z , Li Y, And Zhang K. (2024). Cooperatif Edge AI for Connected Vehicles: Design Implementation and Performance Evaluation. *IEEE Communication Surveys & Tutorials*.

[9] Wang, Z., Li, Y., & Zhang, K. (2024). Cooperative Edge AI for Connected Vehicles: Design, Implementation, and Performance Evaluation. *IEEE Xplore,*, 12-25.

[10] Wang, Z., Li, Y., And Zhang, K. (2024). Cooperative Edge AI for Connected Vehicles: Design, Implementation, and Performance Evaluation. *IEEE Communications Surveys & Tutorial*.

[11] Xiaolong X, Haoyuan L, Haoyuan; X, Weijie; L, Zhongjian; Y, Liang; D, Fei. (2022, April 2). Artificial intelligence for edge service optimization in Internet. *IEEE Xplore*, 270 - 287. Retrieved from IEEE Xplore: https://ieeexplore.ieee.org/abstract/document/9552656

[12] Zhou B, Liu Z, And Wang J. (2024, June). Federated Deep Reinforcement Learning for Cooperative Route Planning in Internet of Vehicles". *IEEE Internet of Things Journal*, 123-125. Retrieved from IEEE Internet of Things Journal: https://doi.org/10.1109/JIOT.2024.3371986