3rd APSEI assignment

Technological Analysis

Daniel Madureira
Nº.Mec: 107603
João Luís
Nº.Mec: 107403
Rodrigo Aguiar
Nº.Mec: 108969

DETI
Universidade de Aveiro
May 2024

Contents

1 Scene 1 - Programming in the car

1.1 Introduction

In this scene the protagonist can be seen coding on the car. Helping him is a AI assistant who possesses very human-like behaviour, that is helping him write the code. The code is projected on the front screen of the car and while this is going on, the car is driving itself independently.

1.2 Technological Challenges

There are a few technological problems in reproducing this scenario in the real world:

- Car driving itself without human supervision
- Human-like AI coding assistant
- Where is the code located
- How is the code being projected

To address the first problem, we must first look to the current reality of self-driving technology in cars. For this, we can reference one of the biggest companies in this space.

Tesla's Autopilot technology claims to be a "suite of driver assistance features (...) that makes driving safer and less stressful"[13]. Autopilot has various features, such as traffic aware cruise control, auto lane change and auto steer, that could in theory make the car autonomous, as seen in the video, for most situations.

Still, Tesla claims that "Autopilot and Full Self-Driving features require active driver supervision and do not make the vehicle autonomous", indicating that the scene present in the video is not achievable yet.

Achieving Full Self-Driving would require predictive AI models, trained on large amounts of driving data, under different conditions, countries, road state and weather.

Training a single model with so many input parameters would take various years and would most likely make it too slow to deal with emergency situations, leading to various AI models needing to be trained to deal with different situations (which most likely already is the case with current full self-driving capabilities).

Still, for this to be a reality, it's imperative that the used model(s) have a near-perfect accuracy and speed, being able to deal with every possible situation in short time spans.

On to the second problem, a human-like AI coding assistant.

Many AI coding assistants already exist but none that have the level of human behaviour present in the video. It is significantly harder to train models on human behaviour than it is on coding knowledge, because human behaviour may be highly unpredictable given the same situation, while coding correctness can be trained through vast amounts of data present on the internet, which is more accessible.

Given this, it is and will be very hard in the future for AI models to totally mimic human behaviour and actions, given that the behaviour of different people in the same situation is not the same.

A possibility would be training a AI model on a specific person to mimic their actions and behaviour and then integrating this with another AI coding assistant in order to reproduce the scenario in the video.

Coding while on the car assumes there needs to be a connection to a computer or a network, either locally or remotely.

In this case, if its locally, we need to assume the car itself has a built-in computer, which may or may not be the same one regulating the car self driving mechanism, but that has the capability to segment these features, given that the car is fully self driving while the protagonist is coding.

It may also be the case that the code is not being rendered locally but instead accessed remotely, from another computer through the cloud.

In this case, a relatively good internet connection would be needed to access the remote computer from anywhere on the road or the user would experience frequent disconnects which would make the experience unenjoyable.

The projection of code on the car front mirror may be done through the use of a projector, connected to the car micro computer, where the screen is being rendered, which is currently doable, or the car mirrors are themselves displays, which seems more the reality of the video.

These displays would need to be by design transparent when turned off, so the driver can still see the road, but be able to turn ON and be controlled by the driver. The technology needed for this may already be present, through the use of transparent screens, but still needs evolution in order to be able to change from a transparent screen (normal driving situation, where the driver is using the screens as mirrors) to a normal screen (where some image or video is being displayed in it).

1.3 Laws and regulations

Replicating this scene in the real world currently offers many challenges in legal terms.

Currently, vehicles with self-driving capabilities still require the driver to be fully attentive. This may be ensured for example with requiring the driver to touch/shake the wheel every couple of seconds to ensure that he is still awake and paying attention.

In the occurrence of accidents, the driver is still responsible, unless a major system fault was detected that was not possible to be corrected by the driver.

This being the case, its still hard to determine who was at fault when accidents happen, being this one of the major legal problems with full self driving.

A full self driving car would assume that the driver could not pay any attention and the car would still drive itself perfectly, respecting all local driving requirements.

This would require the driver to relinquish his control of the vehicle to the car autonomous driving system / artificial intelligence, which would take control and drive the vehicle safely.

Given a full self driving car, the driver could not be held accountable for any of the driving faults or accidents caused by the car, since he wasn't the one controlling it.

In this case, it is troublesome to find who should be held accountable in the case of accidents. Should it be the manufacturer of the autonomous driving system, the company who designed it or the software developers who coded it ?

In order to cope with full self driving, legislation's regarding negligence, responsibility and accident investigations would need to be updated in order to provide clear guidelines in who is responsible for these accidents.

How will insurance work with self driving cars should also be taken in consideration. Given a situation with two self driving cars, which one is responsible for the accident? .

Traditional insurance focuses on driver behaviour to determine who's at fault for a accident, but in this case, no drivers are involved in the actions that lead to the accident, so insurance policies would have to shift towards manufacturers and driving systems, making it considerably harder and more costly to determine who is responsible.

There are also many problems regarding data collection and privacy in full self driving vehicles. For a full autonomous driving system to work, it would have to collect and generate vast amounts of data, which it could interpret in record times in order to make split-second decisions.

Regarding this, what type of data should this vehicles be able to collect? Only video of its surroundings or also sound ?

Could in this case the driver be sure he is not getting spied at any moment by authorities or by the vehicle's manufacturer?

What type of data collected by the vehicle could be used in a court case?

In this case, new laws may need to be created in order to establish guidelines on what information a autonomous vehicle may collect and store and how, to ensure that the driver's

privacy is still being respected.

A full network of full self driving cars would also require that there is a stable internet connection to many vehicles, which would require more investment in networking infrastructure by local governments. This could lead to autonomous driving only being available in some locations or unreliable, which could cause sudden disconnects leading to unexpected accidents. In this case, should local authorities be responsible for the accident? Given that the car loses connection to it's self driving system, should the car full break immediately or start flashing sound alerts for the driver to take over?

In emergency situations, who's safety should the car prioritize? The driver's safety or the pedestrian's safety? Should the priority change if the pedestrian is a kid?

The car autonomous system would need to be manually programmed to deal with this situations, and this priority system would need to disclosed to legal authorities and the driver, possibly leading to uninterest in self driving vehicles if the system doesn't prioritize the driver's safety.

Generally, reproducing this situation in the real world presents many challenges given the current legal frameworks, mostly in inducing responsability in the case of accidents, which would need to be redone or updated in order to accommodate scenarios involving full self driving vehicles.

1.4 Scalability and Cost

The reality present in the video would be very hard to achieve in large scale.

According to Qualcomm "most ADAS system architectures are made up of smart sensors with isolated processing and decision" [12] , ADAS meaning Advanced Driver Assistance Systems.

Incorporating a advanced autonomous driving system into each vehicle could be costly, since every vehicle would need to have a computer or processing unit that is capable of interpreting the data collected by sensors and cameras and predicting the best action possible.

The main challenge arises in the cost of training such models to predict the best possible action given a vehicle and a situation. These predictive AI models must be trained with data provided from each vehicle but be able to learn from all of them, which assumes that the model has to be updated over time with software updates(which is the current reality for Tesla's Autopilot), or that the model is centralized, stored in the cloud and every vehicle can access it.

As this model has to receive, process, and send back information to the vehicle, scaling it to serve millions of vehicles would prove itself a difficult task. While current cloud computing systems, such as AWS already provide scalable solutions to handle large amounts of data, the amount of processing power needed to have a full country or even continent running on autonomous vehicles would be immense.

Current self driving systems are based on AI's trained through Reinforcement Learning, which require large amounts of data in order to present high accuracy in their predictions.

Scaling this to a larger scale would assume that a single model would not be fitting for a global use, given that this system should be able to control various cars, which have different specifications and that drive on different conditions such as weather, road and wind conditions.

Given this, the training of AI autonomous driving models would need to be fully moved to the cloud, where real-world scenarios could be simulated in order to further improve the model.

Cloud systems still require some type of physical infrastructure, and the amount of hardware needed in order to process this magnitude of information and with very fast speeds would be unfeasible with the current rates of hardware manufacturing, given the very recent Chip shortage caused by the COVID-19 pandemic.

Strong networks and infrastructure would need to be present everywhere for this to be a reality in a large scale. The amount of data transfer through the network between so many vehicles would quickly overwhelm most current networks and infrastructure making it unfeasible.

All vehicles would need to support the same, light-weight, protocol in order to communicate with each other.

In the case of a security breach in a autonomous driving AI model or infrastructure , how and when would a security update should be shipped ? If the update implies that there would be a downtime, a lot of vehicles and people could be affected, but a security breach could also compromise millions of vehicles at a time. Given the amount of people affected, careful consideration would have to be taken into account in how updates for the driving models are made.

Many challenges are present in scaling the reality present in the video to a bigger scenario, especially in the training of models that are able to collect and treat vast amounts of data and how the communication between vehicles are handled.

The change from normal driving to autonomous driving would require that many old vehicles are swapped for new ones that have the self driving capability. As is the current reality with electric vehicles, governments would have to offer incentives to the population in order to buy these vehicles, which would be by nature more expensive than normal vehicles.

This would incur several costs in both new vehicle purchases by consumers and local governments, who would have to not only offer incentives for the purchase of vehicles with autonomous driving but also advertise them if they want it to be a reality.

2 Scene 2 - Driving the car with a controller

2.1 Introduction

In this scene, the protagonist first asks the car to clean its camera lenses in order to stop recording. After this, he shuts the car computer system down, takes out a controller, connects it to the vehicle and then starts racing, driving the car with the controller.

2.2 Technological challenges

This scene presents various technological challenges in its realization in the real world:

- How can a car be driven through a controller
- How can the user shutdown the vehicle AI system
- The separation of the car autonomous driving from its other capabilities

Driving a vehicle with a controller is not such a distant reality at the moment.

"During Sony's recent CES 2024 press conference, the Japanese tech company unveiled its long-awaited AFEELA project in partnership with Honda. Spectacularly hitting the stage, the concept car was surprisingly controlled with a Sony PlayStation 5 controller." [8]

In partnership with Honda, Sony recently revealed a futuristic car that may be able to be driven through a Dualsense Controller. Although this was just a short demo, this shows that a future where cars can be driven through controllers may not be so far away.

Driving simulators are also a relatively new technology that is often used in driving schools, to help students learn how to properly drive in different scenarios, or in games, usually with fully simulated vehicle equipment that is able to control the in-game vehicle.

A example of this can be seen in the below YouTube video by Matthias Fulczyk:
https://www.youtube.com/watch?v=lCy4kWMWrLs

These two examples effectly prove that a car may be driven through means other than the normal steering wheel and pedals, being able to be controlled remotely, either through a controller or a full driving rig simulator.

In the start of the scene we can see the protagonist ask the car to clean its camera lenses, so it stops recording, and then shuts down the car AI through the keyboard.

Although the vehicle AI is shut down it still continues driving and doesn't stop abruptly, which assumes that the autonomous driving system and the AI system in the vehicle are separated or at least able to be controller separately.

The vehicle following commands from the protagonist requires that it would need to have some Optical Recognition System, that is able to recognize it's owner(s), as following orders from every person who talked to it would not be minimally secure, given the power a generalized AI system imbued in the vehicle has.

As seen in later scenes, the vehicle AI system has access to many information of the owner, such as his relationship status and bank transfer. For this to happen, we can either assume that this AI may have access to a general network, where it can access information of its owner or that it learns from what it sees, through its cameras.

In the case of integration with other systems, such as bank account, does this integration have to be manually done or does the car have access to everything by default?

The driver shutting down the car AI system easily also assumes that it does not have a major impact in the vehicle safety, as the driver should not be able to shut it down if its necessary to maintain the safety of the vehicle. We can also see this in later scenes where the car says it "lost consciousness for a minute", when it was shut down by the driver.

Given this, its imperative that there are strong authorization algorithms to identify the vehicle owner in order to not leak information to outsider's, the car possesses a minimum set of functions even when its shut down (such as autonomous driving, which can be seen in this case), and that integration's with other systems, such as banks, are designed and though out.

2.3 Laws and regulations

The existence of a generalized AI within a vehicle requires that the information that it can collect, store and share must be regulated.

In this scene, the protagonist shuts down the vehicle AI system, which stops it from collecting data about whats happening, although keeping its autonomous driving functionality intact.

In the next scene, the cop can be seen asking the car for "whats your story?", meaning that the information the car collects may be used legally, for or against the driver.

Given this, would it be legal to be able to shutdown the vehicle's AI system at will, essentially blocking it from gathering any information, which may be used in legal cases? Various new laws and regulations would have to be implemented in order to define if the car AI should be able to be shutdown by the driver, and if yes, in what conditions.

Driving the car with a controller may bring some legal issues as well.

Normally, drivers have to get a license in order to drive a car. If vehicles are now controllable through a controller, do drivers still need to take a license in order to drive vehicles, or its not needed anymore?

Should a controller driver's license be implemented, so people can go undergo training in how to drive a car with a controller?

Current laws do not account for vehicles being driven through gaming controllers, and so they would have to be changed in order to provide clear guidelines if this can be done, by who and in what situations, if possible at all.

Being able to drive a car through a controller would essentially "gamify" the driving experience, which could lead many drivers to drive recklessly, causing more strain in local authorities in order to keep the roads safe, reinforcing the idea that the use of controllers to drive vehicles would need to be legally regulated and constrained.

In order for manufacturers to introduce driving vehicles through unconventional methods (in this case, with a gaming controller), extensive testing would need to be done in order to prove that it is safe to do so and compliant with existing laws and standards.

Gaming controllers are not designed for the precision and responsiveness required for operating a vehicle in life or death situations, so the use of this method for driving would have to be thoroughly tested to ensure that it does not pose a safety risk for the driver, pedestrians and other vehicles on the road.

The public perception on such a driving method would most likely be mixed. While the younger generation, which is already familiar with this method through gaming, would like that they can now also drive in real life with a controller, possibly making the learning experience of driving a vehicle easier for them, the older generation would be skeptical about such a change and most likely would be against it.

In general, driving with a gaming controller could face some legal challenges in order to be a reality, especially in the safety of driving with this device and how it would be perceived by the public.

2.4 Scalability and Cost

Scaling up the concept of controlling vehicles with gaming controllers to encompass all of Europe would introduce additional challenges and considerations.

Infrastructure: Implementing such a system would require significant infrastructure upgrades and standardization across multiple countries. This would include adapting existing roadways, traffic signals, and vehicle fleets to accommodate the new control method and this new driving style.

Regulatory Measures: Coordinating regulatory frameworks and standards across European countries would be essential to ensure consistency and interoperability of the technology. For example, would all vehicles produced support the same controllers for driving or no, do these

controllers share a common interface to communicate with the vehicle or does each manufacturer have his own protocol. Many issues may arise with negotiations involving Intellectual Property of companies and the support for each other's controllers for driving. This would likely involve negotiations and agreements between member states of the European Union which could make scaling this concept take a lot of time and money.

Cost: The cost of implementing such a system on a European scale would be substantial. It would involve not only the development and deployment of the technology itself, to drive vehicles with a controller, but also the necessary upgrades to infrastructure, vehicles, and regulatory processes in order to support this new style of driving in such a critical section, transport.

Technology Adoption: Convincing both consumers and automotive manufacturers to adopt this new control method would require extensive marketing, education, and incentives. There may be resistance from traditional automotive industry stakeholders who are invested in conventional vehicle control systems. Fans of the classic steering wheel and pedals or people who dislike this new driving method may also push back, which may cause it to not be implemented in some countries.

Safety and Reliability: Ensuring the safety and reliability of the system across diverse driving conditions and environments would be paramount. Rigorous testing and certification processes would be necessary to gain public trust and regulatory approval. This process could take a lot of time in some countries due to the heavy regulatory nature of the European Union when it comes to customer safety and protection.

Accessibility: Consideration would need to be given to ensuring that this technology is accessible to all members of society, including individuals with disabilities or those who may not be familiar with gaming controllers.

Training and Education: Introducing a new method of vehicle control on such a large scale would require comprehensive training and education programs for drivers, law enforcement personnel, and other stakeholders to ensure safe and effective use.

3 Scene 3 - Caught by the police

3.1 Introduction

In this scene,the protagonist is caught by the police, and the police officer stopped the protagonist. Through a drone with a display, the police officer interrogates both the protagonist and the car, and the protagonist blames the car for the speeding. After that, the officer believes in the protagonist's story and instructs him to take the car to the inspection as soon as possible.

3.2 Technological challenges

This scene introduces a lot of technological challenges:

- Drone Design and Functionality
- Communication and Command
- Authority recognition from the AI
- Data access on demand to user data

In this scene the drone is performing its law enforcement duties. In this case, catching a speeding car and stopping it are clearly the most outstanding in terms of current drones. To catch the car, the drone must at least top the car in terms of speed and have enough battery life to endure the chase, as well as be able to perform fine movements and effectively stop the car.

To this date, the fastest filming drone was developed to be able to film the RB20 RedBull F1 car for a full lap at the Silverstone circuit, with 5.8km.[14]

This shows that we have the technology to make drones fast, but the real problem here is its autonomy. Although 5.8km seems like a good starting point, the full length of the video rounds up to 2min, which isn't that impressive.

So, the issue here is how to make drones that are able to achieve top speeds needed to chase down cars and make them last more than a couple minutes.

The solution may take two directions: either we implement a distributed network of drones, segmented by area, where each drone is responsible for chasing oversee its own area; or we extend the drone's battery life to endure anything from a full chase to regular inspections.

The distributed network arises more problems, because then we would need a way to guarantee synchronism between drones.

On the top of that, the red bull drone is totally manual driven, while the one we see on the scene seems to be either fully autonomous or partially automatic. In this case, the drone would need advanced navigation systems to track the vehicle accurately and predict its movements. This might involve using GPS, radar, LiDAR, or other sensor technologies to maintain a lock on the target vehicle.

In order to predict the movements, the drone would need to perform interception maneuvers safely and effectively. This includes factors such as calculating optimal paths, adjusting speed and altitude, and ensuring collision avoidance with other objects in the environment.

Another issue is how the drone would stop the car itself. We may assume that the protagonist recognized the police and retrieved his controller, but during the conversation the officer asks the car its version of the story, and the car answers the officer with the event "logs". We could assume that the car answers everyone but it seems unsafe. In order to recognize the police either the car or the drone must identify the other part and recognize the authority, to ensure that the part asking the questions has enough authority to do so.

The car also appears to have access to the protagonist's agenda, as well as more detailed information. We see the car asking the protagonist if he wants to inform his long term girlfriend of his delay.

To achieve this, the car should have a proper way to secure the connection to this data, or at least have the ability to make the call to the long term relationship girlfriend. The data is

either in the cloud, where it can be accessed as needed, or locally and updated when the user enter the car. Either cases would need to rethink how the communication would happen, given the large number of cars seen in this prior scene, and still ensuring that the communication itself is secure and fast, as the suggestion given by the car was made as the protagonist spoke.

3.3 Laws and regulations

Through this scene, we see three potential legal issues:

- Drones use and legislation
- Drones use for law enforcement operations
- AI access to personal data

The first issue has to do with the drone itself. The Federal Aviation Administration oversees the use of drones, includes those used for law enforcement. In their regulation, they require operators to obtain a Remote Pilot Certification[4] and adhere to specific drone operation rules and restrictions, that may vary from state to state, and from country to country. This poses a barrier to shift immediately to the use of drones to these kind of operations, given the fact that almost no police officer has this qualification.

To pose another barrier, the European Union has strict legislation on the use of autonomous UAS (unmanned aircraft systems). In order to be recognized as one, the drone must first pass a set of technical verification's[1], which are very strict. this makes the process of having autonomous drones harder, as they must pass a myriad of checks to be able to be used in this context.

The second issue leads with the drone operation in order to fulfill law enforcement duties. As we see on the scene, the officer speaks with the protagonist through the drone, which may imply record of these interaction. Even if it isn't the case, the video is being transmitted from the drone to the police post. This may imply that this occurrence is quite common, but under the GDPR and other data protection laws this may be an issue, since there is a data handling process that may not be authorized. On the top of this, drone surveillance must be done with caution, as private property invasion. So either before every interaction there is a request for consent or the police drone has some kind of built in warrant or legal protection to be able to attain this kind of information.

The third and final issue takes in consideration the AI responses. As we see in the scene, the AI is very much compliant with all officer's requests, being able to give accurate information about the situation as needed. The question here is the validity of this information in case of an accident. Does the AI "logs" can be used in legal situation? Can the AI be take as a witness in these cases?

Continuing on this topic, the AI also appears to have access to the user personal information, as shown when the AI refers the long time girlfriend of the protagonist. This implies that the AI has access to enough personal data about the protagonist that can deduce that his current girlfriend has "stepped up" to a long time girlfriend. According to the GDPR and similar data protection policies, this can't happen, as it constitutes a clear breach to these legislation's. To be able to recreate this scene, the legislation around personal data access through AI must be reviewed and rethought. As for now, this is the principal pain point for this scene.

3.4 Scalability and Cost

This scene is perhaps the one that has more scalability issues and may have more costs.

The first issue has to do with the infrastructure needed to support the drone network. Implementing a system where drones are employed for widespread traffic monitoring and law

enforcement would require significant investment in infrastructure. This includes establishing drone deployment hubs, maintenance facilities, and communication networks to support remote operation.

Speaking of drones, we need to acquire a full fleet of drones. The upfront costs of acquiring drones capable of performing law enforcement duties can be substantial. Additionally, ongoing expenses for maintenance, repairs, and upgrades must be factored into the budget. This can get as expensive as further we want to expand the network and how much area we want to cover.

If we assume that the drones aren't fully autonomous, we must assure that the personnel that operates the drones has the necessary qualifications to do so. Training law enforcement personnel to operate drones effectively and safely represents a significant cost. Additionally, deploying personnel to monitor drone operations, analyze data collected, and respond to incidents adds to the overall expenses.

Another issue rises as we think about this network's data layer. The drones can and will generate a lot of data, some useful and other not. Managing the vast amounts of data collected by drones requires robust data processing and storage infrastructure. Costs associated with data processing, analysis software, and secure storage facilities can be significant, especially considering the volume of data generated during continuous monitoring operations.

The bandwidth is the principal issue here. As the network grows further, we need to be able to ensure adequate drone coverage, maintain communication bandwidth, and coordinate operations effectively across multiple locations. This can add up cost for maintenance and new infrastructure.

Compliance with regulatory requirements adds another layer of cost to drone operations. This includes obtaining necessary permits and licenses, adhering to airspace regulations, and ensuring compliance with privacy laws and data protection regulations.

These type of operations may have risks associated with them, including the potential for accidents, liability claims, and cybersecurity threats. This requires investment in risk management strategies and insurance coverage to mitigate financial exposure.

Finally, a issue that this network will face is the "transition" between the actual systems and the ones we see in this scene. For us to be able to ensure a seamless integration with existing law enforcement systems, such as surveillance networks and dispatch centers, it will involve additional costs for system integration, software development, and training.

4 Scene 4 - Speaking with the car

4.1 Introduction

After the encounter with the police officer, the protagonist and the car engage in a short conversation about the ownership of the car. The car quickly tells it belongs to CityBank, and when asked who is making the payments the car answers "You are". After that, the protagonist order the car to leave and the scene ends.

4.2 Technological challenges

This scene is the most realistic of all four scenes in the video. Although it may seem simple, this still brings a couple technological challenges to the table:

- AI integration with the car
- Integration with existing systems
- Low latency communication
- Handling data securely:
  - Transport data safely
  - Access to personal data
- Passenger detection and validation (authentication)

The focus on this scene is clearly the conversation between the car and the protagonist. But let's take a step back and decompose this into its core components. The AI is deeply integrated with the car and can access the protagonist banking data on demand.

Nowadays, most AI present in cars serve purposes such as driver assistance, route guidance or even basic voice assistance. And even if these features are continually improved, as we can see in this YouTube video of the presentation of a new Mercedes dashboard at CES: https://www.youtube.com/watch?v=pvSkLHPEafs, we can see that the AI present in the car in the video goes far beyond that, having in addition to all these capabilities, knowledge about the personal life of its occupant and the ability to "connect" or acquire new information about it, as we can see when the protagonist asks who makes the payments.

An AI with these capabilities must then be able to get responses from the network with little latency. Today's cars use the 3G/4G mobile network to try to have a persistent wireless data connection and are also capable of connecting to WiFi networks. However, mobile coverage does not yet exist in 100% of the area covered by humans, so in this case the AI would have some features disabled, such as accessing external data on demand, but would still have to serve the car and its occupants locally.

Another key concern when it comes to autonomous vehicles is their ability to communicate securely and protect themselves from cyberattack's. Nowadays, there are still a lot of aspects that need to be worked on, mainly measures against Machine Learning (ML) attacks on deep neural networks (DNNs) [7]. In addition, the transmitted data must travel through an IpSec tunnel in conjunction with the use of the SSL/TLS protocol, in addition to the use of AES to encrypt the data being sent, as proposed in [3]

Finally, on the question of authentication, nowadays all you need is a key or a card to access and drive a car. Using a mobile phone with the manufacturer's app is also a solution that is starting to be used. However, with the presence of an AI that has the occupant's personal context, it becomes necessary to identify that person(s), and methods such as voice detection via a microphone and a camera for face detection can be used for this.

4.3 Laws and regulations

In terms of laws and regulations, a lot would have to be developed and established. Would it be possible to have standards for this scenario? Or would each company's AI have to mould itself to the law of each country? In both scenarios, who would be responsible for ensuring that the law is being followed?

In the area of personal privacy, would be legal to have an AI with access to so much information about an individual? Could AI make request to external sources to know more information about that individual?

Then, in terms of authentication and monitoring the vehicle's occupants, where would the sensitive data be stored? What monitoring data could be sent to and processed by the manufacturer's?

Furthermore, at the moment when the protagonist asks who owns the car and who makes the payments, there could be two different interpretations:

- The protagonist is in an instalment purchase scheme with CityBank, so the owner of the car is the protagonist.

- The protagonist is using the car for an occasional service, as if it were a taxi, which belongs to CityBank. In this case, there would also have to be regulation for how this service would work, payments, fees to be paid to the state, etc, similar to the process that regularised TVDEs in Portugal.

In general, the legal framework would have to change a lot and at the same time verify whether people would feel safe and comfortable with AI and all its knowledge about them.

4.4 Scalability and Cost

In terms of scalability, the main problem would be being able to access data on demand, since the car would always have to have some kind of network coverage in order to get a response to its requests.

Network coverage may be a big problem in terms of cost, because there would to be upgrades to current infrastructure, or the building of new one, which in addition to manufacturing and labor costs could still see some trouble when dealing with local authorities in the implementation of this infrastructure. In addition to this, the network should be fast enough to ensure fast responses given a high number of vehicles utilizing it.

Integrating a general-purpose AI in a car could also be a big pain point. AI is currently a very hot field where various companies are "fighting" to see which one has the best model. This could lead to problems of interest between vehicle manufacturers and AI companies, which could charge more to certain companies who don't make agreements with them or only service a certain AI model in their vehicles.

The cost of implementing a AI model that is capable of this level of intelligence would most likely be very high.

The cost of training GPT-4 reportedly surpassed 100 million dollars, as reported by Sam Altman. The news website Semafor spoke with eight sources and came to the conclusion that GPT-4 contains one trillion characteristics. [10]

Given the cost of training GPT-4, which is one of the most advanced AI models at the moment, we could assume that the cost to train a general-purpose AI model as seen in the video could be in the hundreds of millions or even billions.

Taking into account that the AI seen on the video can also have access to user data on demand, the cost of developing and maintaining integration's between various systems, for example with the protagonist's bank, can also be high.

No less important is the fact that the car manufacturer need to be able to update its AI over-the-air, without having to recall the cars to their center's in order to ensure a good user experience.

Bibliography

[1] URL: https://www.easa.europa.eu/en/the-agency/faqs/drones-uas#category-regulations-on-uas-drone-explained (visited on 04/29/2024).

[2] Haibo Chen & Subhajit Basu Jo-Ann Pattinson. *Legal issues in automated vehicles: critically considering the potential role of consent and interactive digital interfaces*. URL: https://www.nature.com/articles/s41599-020-00644-2 (visited on 04/27/2024).

[3] Mariia Bakhtina and Raimundas Matulevicius. *Information Security Analysis in the Passenger-Autonomous Vehicle Interaction*. 2021. DOI: 10.1145/3465481.3470045. URL: https://doi.org/10.1145/3465481.3470045 (visited on 05/02/2024).

[4] *Become a certificated remote pilot*. 2024. URL: https://www.faa.gov/uas/commercial_operators/become_a_drone_pilot (visited on 04/29/2024).

[5] Wipro Digital. *Talking cars: A survey of protocols for Connected Vehicle Communication*. June 2018. URL: https://medium.com/@wiprodigital/talking-cars-a-survey-of-protocols-for-connected-vehicle-communication-178a6277ea58 (visited on 05/02/2024).

[6] Lance Eliot. *Getting to scale for self-driving cars is going to be a heck of a stretch*. Oct. 2019. URL: https://www.forbes.com/sites/lanceeliot/2019/10/17/getting-to-scale-for-self-driving-cars-is-going-to-be-a-heck-of-a-stretch/ (visited on 05/01/2024).

[7] Anastasios Giannaros et al. "Autonomous Vehicles: Sophisticated Attacks, Safety Issues, Challenges, Open Topics, Blockchain, and Future Directions". In: *Journal of Cybersecurity and Privacy* 3.3 (2023), pp. 493–543. ISSN: 2624-800X. DOI: 10.3390/jcp3030025. URL: https://www.mdpi.com/2624-800X/3/3/25.

[8] Nicolaus Li. *Sony and Honda's AFEELA Project Is Driven With a DualSense Controller*. URL: https://hypebeast.com/2024/1/sony-honda-afeela-project-car-driven-with-dualsense-controller-ces-2024-info (visited on 04/28/2024).

[9] Kayla Matthews. *Legal implications of driverless cars*. URL: https://www.americanbar.org/news/abanews/publications/youraba/2018/december-2018/legal-implications-of-driverless-cars/.

[10] Naologic. *How much did GPT-4 cost to train?cost of large language mode*. URL: https://naologic.com/terms/artificial-intelligence/q/cost-of-large-language-models/how-much-did-gpt4-cost-to-train (visited on 05/01/2024).

[11] NOVELIC. *Passenger monitoring is at the key of the driverless future*. Apr. 2024. URL: https://www.novelic.com/blog/passenger-monitoring-in-future-autonomous-vehicles-world/ (visited on 05/02/2024).

[12] Qualcomm. *Unleashing the potential for assisted and automated driving experiences through scalability*. URL: https://www.qualcomm.com/news/onq/2024/03/unleashing-potential-for-assisted-and-automated-driving-experiences-through-scalability (visited on 04/27/2024).

[13] Tesla. *Autopilot and Full Self-Driving Capability*. URL: https://www.tesla.com/support/autopilot (visited on 04/27/2024).

[14] Tom Ward. *World's fastest filming drone: how it was built*. Feb. 2024. URL: https://www.redbull.com/pk-en/worlds-fastest-filming-drone-build (visited on 04/28/2024).

[15] Georgie Woolmer. *Driverless cars: The legal concerns and what measures could be needed to overcome these challenges*. May 2023. URL: https://www.irwinmitchell.com/news-and-insights/expert-comment/post/102ifsi/driverless-cars-the-legal-concerns-and-what-measures-could-be-needed-to-overcom (visited on 05/01/2024).