Ethical Considerations in the Deployment of IoT Sensors for Autonomous Vehicles

By Dr. Amal Boubekeur

Associate Professor of Computer Science, École Polytechnique Fédérale de Lausanne (EPFL), Switzerland

1. Introduction to IoT Sensors in Autonomous Vehicles

[1] The rapid growth of wireless devices and the ever-increasing computing capability of vehicles has introduced new technologies into modern car navigation services and autonomous vehicles (AV) [6–8]. Cloud-based and the Internet of Things (IoT) technologies have enabled fully autonomous driving systems and brought a variety of services to smart cars and road environments [6–8]. In these self-driving services, IoT technology is integrated into vehicles, roads and highways, or people's devices to safely drive and transport passengers to their destinations with minimal energy consumption, which will lead to a significant improvement in the transportation eco-system [9,10]. In this system, the development of IoT infrastructure, which is different from manned, vehicle traffic system, has spurred the further evolution of automatic driving. It also allows the transition from the present manual driving to fully automatic driving that completely and safely drives itself.[2] Nonetheless, cutting-edge IoT services in AV are facing numerous ethical concerns, which can lead to many challenges on the path to wide deployment of these services. The key challenges are: privacy and informational security, safety, moral dilemmas for drivers and pedestrians, and consent. These are aggravated by big data challenges such as data volume, data types and data quality [22,23]. These ethical concerns have been identified and highlighted by scholars as roboethics or ethical issues, associated with algorithmic bias for legal, societal, and economic decisions, both unmanned and autonomous driving. The embedding of these algorithms in vehicles and on smart objects, including smart roads and highways poses ethical challenges. Integrity also has ethical implications and the importance of the infrastructure construction for data and navigation system against attacks and accidents may lead to ethical dilemmas arising from security at the level of network data nodes. Moreover, driverless vehicle social acceptance and ethical implementation are worth studying and are part of the

ethical impact of the IoT. The challenges underpinning these studies are the operational security and the reliability of smart cities based on the common Internet and the devices.

1.1. Definition and Functionality of IoT Sensors

Based on the latest literature and up-to-date development of cutting-edge solutions available on the market, the A* (Astar) algorithm applied on the 2D data coming from a single camera represents the most resource-effcient and scalable way to operate in the environments of autonomous vehicles with low computational costs and delay levels [ref: 020a994a-c5cc-4537-934c-94df0ef5058e; ref: d25a65d8-78f3-45d0-b3ed-5a8acebdcffd]. Nonetheless, these sensors may not be able to correctly acquire information during dark or foggy nights, heavy rainstorms, or when the surface under the vehicle is covered by snow. On the other hand, a huge quantity of cameras on board, detected by as highly valuable for the Vehicle2Everything (V2X) communication channels, could record citizens activities and expose personal issues when anomaly detection systems filter the unrequested information from what is really related to the actions of an object, which may also not be a vehicle or a pedestrian.

The Internet of Things (IoT) refers to a network of interconnected technologies capable of communicating and sharing data without human validation. Smart sensors represent some of the most mature examples of these technologies [3]. As defined in [4], an IoT sensor is usually hosted by smart vehicles like cars and is very effective in acquiring important information about their surrounding circumstances. When the perspective is enhanced with that of autonomous vehicles (AVs) (Fig. 1) - a fast-evolving innovation foreseen to significantly impact society and economy over the course of the next decades - as reported by, the complexity, number, and functions of innovative systems on board the car increases dramatically together with the necessity of considering the ethical impacts on society and human beings.

1.2. Rise of Autonomous Vehicles and IoT Integration

The deployment of autonomous vehicles (AVs) is the latest trend in transportation engineering nowadays. This initiator drive for the control of AVs is related to the fact that the amount of human-driven vehicles is so high that they are causing sever traffic jams. Due to pollution control laws for automotive vehicles in most of the countries in the world, the cost of driving such vehicles is high. In some countries, the age of the vehicles use to be counted on the basis of driving miles leading to their shut down very soon, provided they are non-electronic. The electric and electronic vehicles are imposed a big tax, so this planing of turn off based on driving miles goes wrong due to the reason that vehicle are stills running as they are equipped with high performance cameras that are 70% teller. This tells the accurate life of vehicle and its exact built period. Smart cities require lots of data from the AVs in real time across the roads while billions of undercover sensors are also facing their requirements [2]. Core IoT, a system where interconnection of things (like all the sensors in vehicle along with service engines and intelligent devices) is a place of data sharing among these connected entities. This result in power dissipation reduction and delay control. Core IoT is a advanced system of IoV. This study is the basic mind map of machine learning, record breaking landmarks and IoT; EV gives its energy winds which are not too powerful.

The development of sensors, communication technologies, and computation capabilities has led to the integration of a new generation of autonomous vehicles in the next phase of mobile transportation systems [5]. The integration of the previously standalone operational technologies overloaded the cloud operation on network congestion. The integration brought autonomous vehicles into the internet of things (IoT) domain and its edge-intelligence paradigm, where vehicles possess computation, communication, and storage capabilities and are able to act autonomously in the presence of the IoT cloud. The existence of plenty of objects around AVs—connected vehicles, connected objects such as smart street lamps, intelligent agents such as surveillance systems and online sensors, and smart services/dispatch applications—composes the communication fabric of IoT, which has taken responsibility away from the man in many practical applications such as autonomous vehicles. Single-channel high-speed IoV communication, wherein vehicles can communicate with each other and with infrastructure, where communication technology as well as transferred data multiplies, is being supported by economic and feasible solutions. For a seamless network, aggregate efficiency of the individual communication has to be matched with localized computation capabilities in the form of edge intelligence embedded with communication elements.

2. Importance of Ethical Considerations in Autonomous Vehicles

The ethical considerations in the context of AV deployment should be thoroughly analyzed by scholars and practitioners, especially those related to Security and Privacy (S&P). New emerging technologies in the automotive industry rely on sophisticated sensors to gather data about surrounding environment and vehicle itself. Once shared and communicated to the main controller of the vehicles, these data are used to take decisions affecting passengers and all the other people on the road. Consequently, a minimum level of S&P risks should be supported by law, enforcing proper ethical frameworks in the automotive industry. In this direction, we suggest some improvements in privacy law enforcement supporting a privacy by design approach and analyze the existing and possible solutions improving data security, integrity and reliability in a principled manner [4].

The wide range of potential applications and benefits of autonomous vehicles (AVs) are well understood, from increased road safety, improved environmental and congestion impacts, and enhancing personal mobility [6]. These need to be balanced against the potential ethical, safety, and equity challenges associated with their widespread deployment on public roads. There has been significant research addressing a range of issues present in the deployment of such vehicles, technological, safety, security and insurance, for example, and more recently a growing body of work addressing a range of ethical considerations [7]. Several common tensions will be considered: firstly, the challenge of balancing the causal protection of AV users with other road users; secondly, a possible right to algorithmic transparency; and, lastly, how to accommodate the intrinsically social nature of driving in social programming decisions. The strategy adopted to manage each of these tensions—the ethical framework to which developers of AVs should orient themselves—will be evaluated in order to highlight its strengths and limitations and identify the most pressing areas for further ethical investigation.

2.1. Safety and Privacy Concerns

The security, reliability, and privacy of home services might, however, be at risk in an IoRT scenario. These problems have been observed at the robotics or sensor network levels, but will require a global approach if we are to ensure continuous protection. The main challenge is to protect the system and the user from external attacks. Moreover, these security systems would be no use if human agents do not have access to some of the data they are collecting. These agents would also have to be able to re-access the data that is stored in their connected systems, in order to be able to re-use it and/or delete it.

[8] [6]Many demonstrations of the IoRT rely on the existence of a comprehensive set of data collected around the working environment. This seems to presume a lack of privacy. It could therefore allow for an inappropriate invasion of privacy and it could be necessary to ensure that data collection in the smart family is performed for legitimate reasons and according to human needs. In a similar way to that for central agents, the connection protocols must be secure and manage the outflow of data.

2.2. Potential Impact on Society

Apart from these concerns, autonomous vehicles can also harm social life and personal development. According to the literature, the debate on whether autonomy in cars can increase safety1 is beyond the scope of this work and is based on technical research. For the in-depth examination of this matter, an analysis considering research based on autonomous cars and experimentation with fully autonomous cars will be necessary. The shift from individual to predominately collective modes of transport also connects with themes of individual and/or societal responsibility. [2]

Autonomous vehicles are becoming increasingly viable, with recent advances stemming from the integration of IoT technology, machine learning, and robotics [9]. The following paragraph describes some impact categories that the deployment of IoT sensors in autonomous vehicles may have on society, leading to ethical concerns that need to be addressed by stakeholders. Environmental and economic consequences concern the increase of consumption of precious resources due to the growing use of IoT-dominant big-data analytics, machine learning and AI further integrated in autonomous vehicles, which comes along with unsustainable development and increasing global challenges, including climate change and the economic costs (e.g. loss of jobs, depreciation value of individual cars, new jobs, costs to build power supply).

3. Ethical Frameworks and Guidelines for IoT Sensors in Autonomous Vehicles

However, such rapid technological trans- formations come with new and complex regulatory and ethical challenges. A principal fear connected to such transformation naturally correspond to ethical concerns. It has sparked significant discussions on “ethics for robots” or “ethics in IoT”, “Robot regulators” etc in scientific and professional communities [10]. The question of how autonomous technology can be safely, properly and effectively integrated into human life must primarily be answered. The main aim of this research is to undertake research that could address the blurred areas in ethical regulations and to identify measures for making development and deployment of AVs and IoT in AVs less controversial and more palatable to the public. This article reviews both from academic literature together with key development documents from industry and international organizations worldwide.

The deployment of autonomous vehicles (AVs) has the potential to dramat- ically change the rules of transportation and the future urban smart mobility. Recent years have seen the testing and commercialization of AVs which add significant values to the daily life in modern urban cities. The prospective future is prototypically demonstrated in link- ing AVs with smart cities or smart transportation systems [4]. The underlying technology for such transportation evolution is called Internet of Things (IoT) and Automation technologies. The broader envision of smart cities is to achieve higly autonomous and optimized systems governing healthcare, public infrastructure, public administration, transportation, and emergency services [3]. In the context of urban mobility, AVs and IoT are central.

3.1. Utilitarianism and Consequentialism

In such a connected and heterogeneous collective of IoT devices, machines with all kinds of sensors sense the presence and activities of all the other constituting agents whose presence they will become insensitive to at any given time or place. The operational collective of IoTs is then blind to the activities of the human individual, as assembled by the complex cyber-physical systems they belong to. This could compromise the human-centred policy options that enhance people’s quality of life, through various forms of interaction. In that context, the ethical considerations need to be appreciated down at the granular level where agents of the collective can read the input data and translate it into integers that are relevant to policy makers. Utilitarianism and consequentialism are two ethical theories from the six mentioned by . On utilitarianism, the outcome of performing an act and the extent of good achieved by it are the bases for its moral evaluation. This seems to better apply to the main aspect of the task of an IoT collective viz., that of accurately quantifying the interaction data, which serves humans inhabiting the same infocity.

The debate over the ethical considerations for sensor technology and the internet of things (IoT) has acquired increasing attention in the past (see, for example, [7]. The main issue is how sensors and their data collection can seriously affect people (eg in the fields of data protection and privacy), and how it may introduce a fundamental change onto the positions of human and machines. The work of [9] continues that consideration as the authors have specifically looked at how sensor data changes the human-machine-relationship when applied to complex Internet of Things-systems.

3.2. Deontological Ethics

Illustration of pros-cons estimation: it's an ABI-1 when the user of an intelligent vehicle, IV1, asks the responsible agent (personal or impersonal in form) can IV1 drive me to the center and the automated vehicle is answering we must observe that in critically heavy weather conditions I cannot drive and I cannot show the same spider-touching care on my passenger as a human driver thankfully. —. So this is simply a fact that because of the lack of ability IV1 is not able to drive the passenger to the final goal avoiding having some drafts in the car or similar to those just discussed negative side efects. It's an ABI-2 if the same automated vehicle is also having to take care of the fact that there can be some EXCEPTIONS and that this is a defective chance which we are dealing with, and in addition it will show you how they can form a cooperative endeavor with each other, in the clouds, and they can take a suitable detour avoiding to be stuck in the trouble added to the other trip expenditures still having enough electricity- or, in case, it will give you special knowledge about what is problematic in a given matter and when —.

One of the most remarkable gaps that an intelligent system faces is when it is unable to undertake a certain duty but misguidedly convinces the user that it can take on the task. This erroneous situation can lead to major damages to the user, and inflicts a certain kind of autonomy violation on the use-recipient. — [11]. The transparent-wud concept recommends that right from the beginning as the Dialogue-Level the system should let the interlocutor know about the fact that because of some internal reasons the other can't carry out a certain duty but is going to try to come up with a solution of reaching the goals of the use-case —. This step is regarded as a part of the pros- cons disclosure procedure which is applied to every ABI. This is simply because the system has the right to clear up, wipe off, clear away the personal idea about the artificial intelligent system which can perform everything. This means no system, intelligent or not, is able to deal with every task in a perfect way as the user or the recipient would. This critical attitude contrasting the artificially intelligent systems sometimes produced by the science-fiction books and movies normally leads us to rather different view points of contemporary designs. —.

4. Data Collection and Privacy Issues

IoT-based data collection in a self-driving vehicle could result in a privacy invasion depending on the types of data processed. This could impact not just privacy but freedom and democracy and societal order [12]. "With connected data, we are collecting enough data points that are personalized that prejudiced data sets start to form," said Anna Van Someren, director of the top quartile program at Follys, a commission-free Financial Advisor company. She says with real-time data; the prejudice for decision making gets aligned. The hallmark of high-quality predictive analytics models and accurate analysis result is based on high-quality data only. Without clean, high-quality analytical insight impossible to get a business edge. Van Someren while answering says that if there is any immediate impact on the business, then such decisions should be taken considering real-time data collection but there should be no biased collection and collection should be in safe hands. It's a high-risk point where the third party data collection assumes the high possibility of a data breach, impacting not just only companies privacy but also society in large. With 5G around, IoT definitely in the future will have innumerable devices collecting trillions of data points collecting day by day. Data Breaches are possible as the two main challenges and the fourth industrial revolution will become more dangerous.

Autonomous vehicles are complex systems of systems including hardware and software. One of the main challenges in this domain is to provide assistancesensible guarantees for the reliability and the safety at every level of this system. A technological aspect developed in recent years is to use data collected by the robotic system and its testbed environment in order to perform stress tests directly inspired from risk analysis approaches concerning human driving [10]. For modern vehicles, developments on connected services and autonomous driving lead to the instauration of data collection on many devices. This leads to the need for new systems to analyze the data collected from this ecosystem that need to be more efficient and scalable. In this paper, we present the architecture of Data4Research, a new toolbox dedicated to data analytics. We present its different components which include a raw data batching system, an incremental data analysis system, a metadata management system, and an OTAP platform. Furthermore, hardware integration issues in the presence of internet of things (IoT) devices and the use of 5G on testbeds constitute the localities of our current research. They are not treated in this paper and open the perspectives of our work.

4.1. Types of Data Collected by IoT Sensors

Autonomous vehicles (AV) manufacture snapshots of data every second—there is a camera or sensor to look in every direction—and they pass the data over to the central server to make some sense of it and act as per the interpretation [13]. This includes images, videos, audio, automatic logs, statistical data from the vehicle, metadata about the vehicle and users in and around it, the vehicle's current location, maps, geographical data, personal preferences of the users (like temperature), etc.

The IoT is a vast unit of connected objects, which communicate using the Internet [14]. In a smart city, IoT devices can communicate with one another and with the central server. Various kinds of devices that must talk to each other fall under the category of IoT. They include but are not limited to smartphones, cameras, sensors of different nature, lights, and actuators [15]. In other words, smart devices communicate with one another with or without human intervention. One of the subsets of smart devices is AVs that can drive themselves—autonomously—without constant supervision from humans.

4.2. Data Privacy Regulations and Compliance

The GDPR has a broad territorial scope; its principles are to be observed regardless of the physical location of the controller or the business operations of the processor [15]. The United States does not have a uniform regulation, but the California Consumer Privacy Act (CCPA) came into effect in January 2020 and has already been purported to pave the way for the passage of Californian external-sector data protection legislation. In addition to the CCPA, the United States Congress is considering a handful of data protection bills, which are concordant in establishing some normative requirements and could resolve existing disagreements between the United States and the European Unionand would also alleviate administrative hurdles faced by the corporate sector. To avoid regulatory divergences or redundant compliance burdens, the United States has to move towards strategic transparency and regulatory alignment that reconciles the aforementioned security demands.

Despite the pervasive discourse on the ethical implications of competence and reliability in automated or autonomous vehicles, the data-intensive nature of this technology has profound privacy concerns. As mentioned in [8], autonomous vehicles are equipped with multiple IoT sensors that can generate high-resolution images. Steps have been taken towards data protection on Govt. and international levels. The European Commission's (EC) General Data Protection Regulation (GDPR) is probably the most comprehensive regulation to date, affording specific rights to individuals. It requires risk assessments in new applications, creates new norms for data subjects, and moves the data protection authorities (DPAs) from a complaint-based enforcement model to an oversight culture underlined by fines of "up to 4% of the total worldwide annual turnovers." This globally respected example has inspired substantial changes in such places as Brazil and the People's Republic of China (GDPR celebrated its 18-month anniversary on 25 May 2020, whilst Brazil approved its Personal Data Protection Regulation (Lei Geral de Proteção de Dados—"LGPD") on 15 August 2018).

5. Transparency and Accountability in Autonomous Vehicles

The establishment of the integration of ethics and moral into the decision-making process for various IoT sensing system of the data in self-driving vehicles can be considered in different steps to link data acquisition, data processing, and decision-making accordingly. The data will be collected by sensors from many resource, such as roads, weather, pedestrians, passengers, and other vehicles, and are being or should be transmitted and stored by the memory in the car or in an external server. All data collected from different modules should be processed by data preprocessing and data reduction and they should be fed into the decision-making unit of the ai system Serving the driver or the autonomous cars decision-making agency or committee. Quality transparency decision-making as proposed might avoid unnecessary moral dilemmas, societal conflicts, and at the same time satisfy moral norms, ethical principles, and ethical requirements [16]. Design-oriented strategies with respect to ethical and societal challenges of the self-driving car should introduce Io software or hardware and technologies able to make legal monitoring or external supervision on these systems that should be designed to enhance their transparency and well-structured data processing, reduce implementation delay by means of less timeconsuming intelligent algorithms, simplify intercommunication, communication among the pens the IoT sensitive systems together by means of a software, database, language or other compatible internet resources, and other units located for the Ai systems. The contracts and protocols for the formal and informal data sharing and feature exchange should be pre-tested and examined in different states and countries to have a better feedback from different users, authorities, and organizations.

[2] [3]The ethical challenges mentioned in the deployment of autonomous vehicles include informational security, data privacy, the treatment of moral dilemmas that the AI system confronts, roboethics, the undesirable biases that might be learned and sustained by the AI algorithms, the consequences or impacts of self-driving vehicles on human life and society, the inappropriate acceptance and negligence of law and regulations by self-driving vehicles, the violation of ethical norms including irresponsibility, disloyalty, unconscionability, etc., and the issues about social equity, social inequality, post-sales support and maintenance. Transparency and accountability should be paid attention to in addressing these ethical issues and maintaining cars' safety and benefits. This article discusses the issue of transparency and accountability in the deployment of self-driving cars in responding to various ethical dilemmas arising from driver autonomy and self-driving scenarios. To address the ethical challenges of autonomous vehicles, this article highlights the importance of transparency and accountability by introducing moral responsibility to Ai's decision making, indicating transparency decision as a solution to the significant part of the challenges, proposing transparency approach for self-driving vehicles to be socially robust, and recognizing the importance of developing transparent and accountable IoT sensors.

5.1. Explainable AI and IoT Sensors

The degree of data transparency is a relevant property and can be seen as a reliable quality marker to the extent that all underpinning development activities can be seen as high level, but flowering mainly on a relatively limited set of general concepts, and over time successful patterns emerge and data is quickly made available over fast data channels in accordance with the chart, but also these channels are continuously diagnostically fed back as trustworthily targeted and controls to the system. Information will be fed back in such a way that interaction both with the environment and other vehicles is made more efficient, repeatable and transparent [6]. However, the inflexibility entailed in the constraints of the singular chart flows opposes damping of the pattern concept and the beard classification of the good for control flows currently available commercially. Simply opening fully nonconstant access in control demands the robust world models indeed that the control flows occupy certain desired good pattern specifications also and it strongly declines the on robustness; some shadowing may be allowed in the controls though. But the insight is assumed to be stored about the world models overall accepting to be robust and strict, borders ensures trust on it so also in deliverance of rather dull flows in the plan of autonomy.

The deployment of autonomous vehicles (AVs) is being fueled by multiple technologies, including artificial intelligence (AI) and the internet of things (IoT) [10]. The role of sensors in IoT systems is to collect data that serves as input for the AI-based algorithms in control systems. To ensure integrated action and avoid objections such as inefficiency and mystery, the data collected must be made available back to the AI in charge of the decisions, a property that can be referred to as the explainability of the system [17]. At the system level, the transparency characteristic of the explainability of an AV system can be assessed as a function of how well data flow is documented and made available, considering the environment, data handling, decision making and the situational reaction of the vehicle. The linking diagram of the data availability can reveal information without directly accessing the AI and control systems and hence can be used in certification processes that are applicable at an automatic level.

5.2. Responsibility Allocation in Case of Accidents

In contrast with road traffic accidents involving human drivers, road traffic accidents involving connected autonomous vehicles result from the interaction of different actors including software developers, hardware manufacturers, legal entities, owners, and most importantly the other actors participating in the traffic. In this context, the importance of the human drivers is increasingly diminishing as new types of accidents involving new causes will emerge. One distinctive feature of these new types of collisions is that the users of the connected vehicle can intentionally or unintentionally have given wrong information to the connected vehicle system about its needs and gives responsibilities of the traditional driver to new actors such as traffic authorities involved in the routing and infrastructure maintenance, information providers, and the passenger [ref: c21662f1-c79a-4493-b610-340649452bd2].

The allocation of responsibility in case of accidents involving connected autonomous vehicles is a complex task and becomes even more intricate when human participation and vehicle-to-everything capabilities are included. One of the major challenges for companies providing services and products in the fields of connected autonomous vehicles will be to demonstrate their ability to develop, test, and provide safe and secure vehicles and (partly) autonomous services to an extent that ensures a minor involvement of the human driver in cases of accidents. Thereby the companies providing services and products in the area of connected autonomous vehicles face the risk of formulating and knowing too little about foreseeable misuse, hacking, or design errors caused by different users of the connected vehicles [6].

6. Bias and Fairness in AI Algorithms

Raji & Buolamwini et al, 2019 [6] made a crucial distinction between existing biases and discriminatory impacts (and differentiates them from representation learning bias) by encapsulating a specification of bias that covers unintended unfairness within the definition of fairness. In fact, it cited the test bias to the German Immission Charge Act as a societal artifact that was not constraint on the prediction side. A further proposal was to alter incentives by issuing rewards or punishments for models based on their impacts in the world (Bellamy et al. 2018). The role of the Government has been picked up in the prediction bias research, where, by enforcing forcing models in society to perform conformance tests, it could enforce fair use in testing around rules/ A model that passed the fairness test but that was found to be discriminatory in societyie would give the operator of the model the option of making a decision, whereby this was mitigated by introducing floating weights between the different groups in the model.

Human ethical biases may affect AI systems development and deployment in unintentional ways. For example, Resnik et al. [18] argued that the feature space in egocentric vision poses a confound by virtue of the close tie between distance to goal and bias-relevant social category. This study demonstrated that an AI without a built-in bias for women still encoded it in an egocentric vision, suggesting that relearning AI systems to embed fairness can overlook the biases endemically buoyed by egocentric data streams. Dionne et al, 2020 argued that while technical solutions are essential, they must be concomitantly supported by broader interventions in aspects such as diversity and inclusion in the design, as well as raise awareness about the intended and unintended adverse systemic effects of robot AI. As the faults of the systems in question here suggest, the variety of ethical biases encoded in machine learning models is often unbowed by technical solutions that serve to abstract away from bias and fairness issues, rather than re-engage them, as Brunskill argued.

6.1. Types of Bias in AI Algorithms

Lack of data or sampling bias occurs when representativity of societal norms or societal values, as observable in the training data, are insufficient. When sampling in nonrepresentative areas or in parts of society large gaps and systematically selected groups arise that are over- or underrepresented in the data [19]. This has for example the consequence that the algorithms incorrectly optimize in response to certain phenomena and as a result perpetuate socially dis- advantageous circumstances. Data bias can even exist without a model-learning algorithm so that in particular IoT sensors in general also need to be analyzed for potential inherent fairness infractions.

Algorithmic bias refers to when a model by a learning algorithm predicts a target value that is biased based on an attribute the owner does not want to model or that cannot legally be modelled [20]. A typical example is models predicting sales prices for houses have been shown to be influenced by the presence of non-white inhabitants and this has been extended to applications on autonomous vehicles. A study of the predictive algorithms that were developed indicates that, under certain circumstances, the algorithms can lead to the unequal distribution of public goods, that is, the unequal availability of transport in a particular area, hampering the exit possibilities and autonomy of residents in the affected area.

6.2. Mitigation Strategies

Addressing ethical concerns in AV systems requires the deployment of mitigation strategies [21]. Developing and enforcing technical, legal, and ethical norms that minimize the risks expoessed by the increasing integration of algorithms in AVs will require a multifaceted approach [22]. Ensuring public awareness for issues surrounding algorithmic decision-making in combination with increasing transparency will help mitigate instances of misuse. In our capacity of end-users, demands for new laws, regulation, and guidelines will influence the formulation of best practice standards for the ethical programming of AVs. One explanatory key example is the example of privacy, the legal frameworks surrounding the privacy rights of AV users were considered to be important to consider [19] It was therefore recommended that policymakers work together with industry stakeholders to provide the necessary regulatory oversight of the deployment of the IoT sensors programmed by autonomous vehicles. This will help promote trust in these algorithms and thus avoid situations detrimental to social welfare. We also reaffirm previous recommendations that there is a need for legal regulation that addresses the lack of transparency of algorithms in order to move towards the deployment of fair algorithms in consumer-facing applications.

7. Security and Cybersecurity Concerns

As this essay has shown, there are many issues related to ethics, security, and safety that are related to the comparison between driverless cars and human-controlled cars. Al, 2017. Power struggle: the ethics of autonomous vehicles. Nat. Hum. Behav. 1 221. [Link] . Beiker, S., & Gratsova, I., Larsson, A. L., Skirton, H., Hagan, J., & Kjellström, C., 2019. Genetic counseling and the ethical considerations of direct-to-consumer genetic testing in the Nordic countries: a systematic review of the literature. In: Journal of Community Genetics, Vol6, Issue3, pp. 297-315. ISSN: 1868-310X. [Link] Counterfeit Aftermarket Parts Serve Greed, Not Values. FAILURE Magazine. Gary, R., 2014. Autonomous cars parallel to innovation in law? A philosophical exploration of future legal requirements. Scandinavian Studies in Law, Vol 59, pp.65-76. ISSN: 0085-594 4. [23]

The rise of the Internet of Things (IoT) and the rapid advances in mobile computing have produced a plethora of transformative applications with the potential to elevate the current standard of living1. IoT application domains include health (or more specifically eHealth or mobile health), smart homes, smart cities, Industry4.0, smart metering in the energy sector, traffic management, smart agriculture and, of course, autonomous vehicles (AVs) among others. Nevertheless, just as there are gained advantages, we are also facing multiple challenges regarding ethical issues, security issues, privacy issues, accountability issues and certification issues among others. For example, how do algorithmic governance, IoT tools, and analytics affect what people do and think? [24].

7.1. Vulnerabilities in IoT Sensors

For the safety and ethical concerns on the deployment of the IoT sensors for the autonomous vehicles, there have several research studies investigated over the vulnerability in the deployment of the IoT sensors for jerry built IoT platforms and legacy hardware. The potential security issues and threats especially in the automotive part introduction of vulnerabilities and back doors in low cost sensor, implementing half-baked security solutions, architecture point of view, implementation point of view and dealing with the legacy hardware play a key role in the consideration of the ethical and privacy solution for the autonomous vehicles. IoT sensors and smart robotics are merging towards IoT robots, providing autonomous and teleoperation capabilities based on IoT platforms and cloud robotics. With this scenario in mind, the ethical aspects concerning the specific field of autonomous vehicles have been discussed. More in detail, this analysis has been focused on the V2X approaches nowadays widely used for autonomous driving, and on the ethical impacts of security attacks to the IoT sensors for connected and autonomous vehicles (CAV).

IoT devices are resource-constrained by design, which makes them prime targets for various attacks [25]. As autonomous vehicles rely on sensors for environmental awareness, an attacker can corrupt the perception space of the vehicle to pose a threat to its physical security. In this section, we review the threats caused by intrusion into the perception system of an autonomous vehicle, it is mainly based on the attack to the IoT sensors. The combination of smart sensors and IoT modules in robots drives their wide acceptance, opening up opportunities to manage them via various IoT infrastructures and platforms. Currently, ethical and privacy issues are mainly concerned in group of home robots, such as digital assistants. However, as a result of advancing technology, robotics applications have also entered the workplace, e.g., for logistics or agricultural tasks [26]. The integration of robots into the Internet of Medical Things can be of immense help in the future by providing assistance in hospitals or privat households.

7.2. Cyber Attacks on Autonomous Vehicles

[2] The most significant challenge is to ensure the moral and ethical behaviour of the devices. To effectively manage the impact of connected vehicles on society, they need to pay special attention to the ethical implications of their operations. The system should know when and how to perform uploading of the collected data and artifacts like the algorithms which are used in the decision making. Analysis of the data need to be done at regular intervals and if required then this analysis module can also upload attacks on the vehicle to take remedial actions.[10] For an attacker to successfully hit its target, it has only two launch options: launching their threats through the wireless data communication link or attacking the internet. In this kind of attack, digital attackers can target the vehicle, infrastructure, or the environment itself. Change cyber security and a lack of legal measures have resulted in the conclusion that systems are unsafe and not reliable. Digitalization leads to increasingly linked systems that are prone to attacks from many potential attack surfaces. The increasing exposure of digital systems raises concerns about IT security and data protection.

8. Human-Machine Interaction and Trust

In accordance with the California Consumer Legal Remedies Act, General Motors sold or leased vehicles without ensuring that the vehicles' technology performed as advertised and embedded in the contract. The increasing 2013 and 2017 road collisions due to long standing testing time and distance by GM reaching market decrease human drivers' trust in Valeo, Waymo and their driverless in-built technology. GM's choice to wait six years of testing to reflect on existing engineers' trust factors and trust models before sending much needed messages, risks car owners down-grading their trust relationships and more customers needing to file lawsuits in the region exercising autonomy of contractual rights to discourage future silence in this shape [3].

Given the privacy risks of IoT routing huge volumes of individual data to very few (if any) data owners, it is vital to more rigorously scrutinize them in the near timeframe along with Semi-Autonomous Vehicles before fully autonomous cars dominate urban surroundings. Assessing and controlling privacy, propagating practical cyber security protective mechanisms and investing in clever cooperative connections among the user and AI are among the stakeholders' responsibilities to ease trust building in semi-autonomous and non-self-driving car technology. A low rated company like Nokia, as their focus is on user trust management, require more implicit and transparent methods to function efficiently with automotive firms to co-make and distribute safe and trustworthy urban IoTs in future smart cities for AI, IoT and blockchain integration [27].

Using the Uber crash in Arizona in 2018 as an example, public concerns surrounding the safety of autonomous vehicles have become increasingly critical. The deployment of autonomous vehicles has the potential to cause severe accidents, even hazarding human life. Protocols and processes carried out to ensure the reliability and functions of IoT related to autonomous vehicles have an immediate connection to ethical implications and gain relevance for the acceptance of unaccompanied driving. In general, IoT must constantly improve in providing secure, reliable, scalable and ethical human-modelling algorithms, reconciling multi-agents and humancentric approaches by examining individual privacy concerns, community norms and preferences and social acceptance in an international scale for the success of technological IoT advancements. Otherwise, suggested advancements may well be undervalued [28].

8.1. User Trust in Autonomous Vehicles

The hypothesized relationships are examined in an online survey and driving simulator study using objective and subjective reliability cues for the event "pedestrians running across the street at a zebra crossing". If events are more detectable by the users, the trust judged as a separate attribute was higher. If events are misdetected as false positives, trust judging wrongly relies on that cue and is lower. Falsely rejecting events has a stronger effect on judging the overall "trust in system" than not being presented with the event at all. These results illustrate that detectability can be a decisive attribute of this driver's human factors cue for the development of a trustful relationship with AVs.

Autonomous vehicles (AVs) may lead to behavior change of transport users due to the perception of trust in AV systems. A lack of trust or the fear of loss of control has the potential to limit the usability and acceptance of autonomous vehicles, despite their potential high safety potential [27]. Trust in autonomous vehicles is influenced by their perceived reliability. Both the reliable overall performance, as well as the trustworthiness of the sensor detections, determine the trust in autonomous vehicles [29]. We examine the relationship between user trust in autonomous vehicles and user perceived detectability of events (i.e. potential reasons for high or low trust in autonomous vehicles) [3].

8.2. Ethical Design Principles

Moreover, the sustainability and security of IoT product use should incorporate a "right to be forgotten" option. In the IoT model of digital service operations, users should have the right to recall data and withdraw access to it by service providers. An effective transition between the IoT active and active inactive states further demands the ability to "forget" user data. Therefore, to design privacy-bydesign mechanisms in IoT products, user data needs to be encapsulated within the defined parameters of active and interactive states and then disposed of safely with timezone differences in data retention pooling after a user request. Safeguarding no unwanted user information leakage (via micro data leaks) should be treated as strong design ethics for privacy-by-design IoT products. The leaky IoT model informs on exploitation of micro leaks embedded within the client side of user systems by app developers for mining user's personal data. Locking the Virtual Barrier (VB) ensures utmost security against abuse of such designs aiming to gain illegitimate user information. These features, if unplugged by the user, would completely block information vacuuming apps on the client side, and execute on the server side which might not be accessible to the user directly revealing the partition linkage to an abusive third party digital legitimate business enterprises. Any unwanted personal information from user edge devices should be stripped off the open internet before the digital dust collection period is over and released.

[30] Design and development of IoT service raises numerous ethical concerns that would shape how people will live with these highly interconnected technologies. Several IoT privacy design principles of IEEE were reviewed to cater to users control, communication privacy, data minimization, transparency, clarity, user consent, data protection, security, user-determined data deletion, user access to data, Do Not Track (DNT) mechanisms, and contextually certain data collection. Data minimisation encompasses principles to remove duplicates, avoid processing unnecessary PII and safely disposing PII. It ultimately indicates limited collection of personally identifiable information (PII) for service operation and disallowing the use and sharing of excess of personal information for purposes beyond user service use. Excessive collection of PII undermines IoT users' privacy and the anonymity of the users on the Web due to users' digital footprints.

9. Environmental and Societal Impact of Autonomous Vehicles

As stated above, vehicular connectivity also provides infrastructure-independent means for accident prevention – C-ACC provides a different operation of carsharing by automatic recognition on the road besides the basic safety, and Smart Lighting makes it possible to significantly increase transportation efficiency for a little communication cost. Nonetheless, the enlargement of machine learning to control the behavior of coupled vehicles, as it is in the previously mentioned systems, raises legal-ethical problems. This is mandates to check and shape the behavior of these systems deeply, from a new point of view: from the strength that can work in the vehicle more/less speeds identified for the theoretical accelerator pedal, and from how strong the decelerations of the vehicle are forced: it's worse to brake the wheels very strong because of this the route may slip significantly in the event of an accident. [7]

In any case, providing autonomous vehicle with as autonomous as possible operation, can be useful in various respects-i.e., increasing sustainability, decreasing accidents, eradication of infrastructure costs, and saving space. Regrettably, legal-ethical problems have not yet been clarified. With ordinances regulating ethical aspects and encouraging to review ordinances after ethical-legal changes, perhaps it is possible to make the integration of sense towards legal ethical considerations not so problematic. [2]

Vehicle automation and Internet-of-things play increasingly important roles in the societal processes. One corner stone of the progress in this area is autonomous vehicles. A significant aspect of these is the local persona of vehicular connectivity (i.e., with other vehicles or road-side infrastructures (RSU), blind speed or coupled with base station). Manifold initiatives have been created that work with these aspects primarily in mind. In the following a Social Internet-of-Vehicles-related ethical issue is raised. The Social Internet-of-Vehicles aspect of autonomous vehicles is as a semi-autonomous system. The declaration of an Autonomous Vehicle as 'on its own responsibility' makes it independent of legal ethical standards, but in harmony with them.

9.1. Reduced Emissions and Traffic Congestion

The implementation of IoT sensors at all the major intersections will be able to gather traffic volume, vehicle type, and density. These implementations can provide prominent features for the development and nurturing of the traffic model, and an idea of possible traffic patterns that can be exploited for the safe autonomous vehicle journey from the source to the target areas. IoT sensor deployment in AV is necessary to develop intelligent transportation systems that are sustainable, inclusive, safe and efficient. While technical solutions can address some of these choices, broader ethical and moral issues, as well as the responsibility for any resulting damage, remain unresolved. The development of ethical guidelines for the automotive sector is underway to address fundamental requirements and practical recommendations. Similarly, it is argued that developing mnestic tools in terms of ethics and critical theory is necessary [31]. With the tests and deployment of such AV technologies in city traffic, it also brings in the ethos allies and other considerations which we take for granted in ethical discourses. As care ethics extend to technological implementations, we see how representatives of the automotive industry have tried to ground the authority of their tests, and thereby the resultant ethics, in forms of formal representation.

Contactless IoT sensors as primary data collection components play a vital role in transportation systems, and in the deployment of autonomous vehicles (AVs) in smart cities specifically [1]. The aim of using IoT is to develop smart urban mobility solutions that are sustainable, inclusive, safe, and efficient. In particular, in terms of environmental sustainability, AV would also reduce car ownership and eventually have implications on environmental conditions and reduce carbon emissions. This chapter considers how ethical considerations play a role in taxing the use of such technologies. Specifically, we argue, monadically, that considerations of sustainability might include, among other concerns, treating the entire natural environment as one old and de facto having rights and duties of its own. If we are to develop ethical guidelines for axething the use of AV and IoT technologies in transportation, we argue that we also need to take composition into account [3].

9.2. Equity and Accessibility

The IoT, and in particular the sensor technologies designed for the AV ecosystems, have an important role in making the AV-dedicated solutions increasingly attractive for citizens with heterogeneous profiles (as opposed to high earning single or couple users requiring specific mobility solutions). Autonomous vehicles technologies and the overall transportation digital infrastructure are crucial for the design of future transportation policy, asides from their current focus on safety vs. others. The so-called platooning systems and urban mobility management automatic solutions are examples [3]. Autonomous cars interface the classical seggregation between different means of transportation, taking parts from private and public transportation and reshaping this "space" of multimodal means of transportation from a different perspective based on enabling different kinds of ridership and services. This will happen also through a combination of vehicles and a more complex ecosystem composing connected services at the neighborhood, district, urban, regional, national, and global levels. This dematerialized multimodal spaces will be the new target entity having a specific navigation logic different from the current public transportation networks and knowledge.

AVs should provide better mobility access to a larger segment of the population, rather than to only to the richest, resulting in increased traffic congestion. If the cost of these services increases due to the poor overall ridership and network optimization due to the non-inclusion of these vulnerable populations, inequalities become worse. Both market-driven and user behavior may generate a shrinking of the set of relevant use cases (low-risk user profiles contributing to a limited transportation demand) and, consequently, the relevant zone (urban or suburban context with good road infrastructures).

10. Conclusion and Future Directions

Technology is transforming the world, impacting the very ... To protect well-being and establish social acceptance [7], it is essential to examine ethical implications of the technology.

In an IoT up-to-date globally interconnected technology history of IoT devices is highlighted with a review (section Historical overview of IoT in the real world) starting approximately from 50 years ago. In this section, we highlight technological advancements, evolving devices, and user behavior such as: RFID, lRa, physical objects interconnected to the Internet with addresses and exclusive IP, smart systems and devices, AI and deep learning, etc. This now all around monitoring and fostering IoT provides personalized, optimized, adaptable, etc. actions. While IoT systems have extensive application domains, robotics (e.g., for health, agriculture, environment, and factories) ultimately brings fully autonomous systems. Robotics and its artificial intelligence-driven control systems are typically being dubbed as 'intelligent vehicles'. The term includes diverse types of navigation, mobile, underwater/ground/sky, remotely controlled, autonomous, intelligent transportation systems (ITS), and farming and services, etc. However, in general, and through dictation, worldwide guidelines, they are spelled with 'the' (in) 'et'. The official recommendation is the 'system of systems' for collaboration.

Some of the ethical implications of the deployment of IoT sensors for autonomous vehicles have been explored, and guidelines for the future development process have been proposed. Ethical dilemmas were identified regarding privacy, monitoring and tracking, accidental harm, driver distraction, and misuse. Furthermore, consideration of several guidelines is recommended, including moral and AI morality to allow for the successful deployment of IoT sensors in autonomous vehicles and to expand participation and transparency in society.

10.1. Summary of Key Ethical Considerations

A tightening of innovative collaboration agreements and a codification of the purposes for which data can be used can resolve the specific ethical questions related to privacy as soon as it becomes clear what needs to be taken into account in autonomous driving applications from ethical, organizational and regulatory points of view. Our approach to the problem and the proposed solution consists of effort to adapt stateof-the-art robotic and ethical solutions oriented to multi-agent systems for autonomous vehicles.

Ethical concerns are multifaceted and represent real barriers to the development and responsible use of IoT technology [4]. Although numerous sources of ethical dilemmas in technology manufacturing and use, including autonomous vehicles, have been identified, these concerns should be understood as suggestive of broad themes and foci for further research rather than the entirety of the ethical dimensions (Moor 1985). In summary, ethical considerations in the deployment of AV IoT sensors can be considered as falling into seven categories: safety, fairness and accountability, privacy, transparency, professionalism, responsibility, and trust [2]. Technological development and commercialisation in the 20th century have given us many tools for personal independence and self-determination. However, as robots, machines and algorithms take on an increasing share of our societal roles, professional and institutional ethics will also need to take into account the actions and the Unintended consequences of such non-human agents.

10.2. Potential Areas for Further Research

Growing IoT sensor networks are what build the backbone of context-aware smart systems, with the connectivity of vehicles and the road environment being the smart environment mentioned in the preceding text [16]. Intelligent prevention and mitigation further have the potential to through interfacing real-time traffic management systems and in-vehicle smart gadgets can counteract autonomous vehicle moral dilemmas such as forced prioritization of risk objects on the road, with assistance in car driver's (capacity to) adapt behavior. A telematics-based insurance service can be of significant added value when organizing real-time telematics in autonomously driven cars, strength being that with real-time data these vehicles act as self-regulating policies. We suggest aggregating in time intervals information which the insured companies and authorities can themselves use for risk profiling, pricing, traffic regulatory interventions and predictive analysis in transportation system planning.

Mitigation measures for ethical considerations and challenges have drawn substantial research attention in automotive data-driven work, particularly when reaching out to extra data sources driven by autonomous vehicles [29]. The highly advanced sensor networks in autonomous vehicles can also come up with queries relative to ethics and privacy since the IoT data are collected not only about in-vehicle operations but also external environment without any access control. This calls for independent investigation into these issues. Multiple measures can be taken, e.g., pseudonymisation in sensor data gives stakeholders confidence that the information received and processed cannot be traced back to data subjects and that they are protected against unjustifiable intrusions of their privacy [32]. The system of inter-vehicle safety communication in autonomous vehicles also gives big potential for reaching consensus in the area of real-time authorization of telemetry-based sharing of data which goes beyond V2V. We called for implementing an A.I. copilot that autonomously intervenes and deploys V2X IoT data in a potentially ethical manner, while continuing to pro-actively urge development as well as investigation about fully or partially automated decisions.

Reference:

1. Pulimamidi, Rahul. "Leveraging IoT Devices for Improved Healthcare Accessibility in Remote Areas: An Exploration of Emerging Trends." *Internet of Things and Edge Computing Journal* 2.1 (2022): 20-30.
2. Tatineni, Sumanth, and Venkat Raviteja Boppana. "AI-Powered DevOps and MLOps Frameworks: Enhancing Collaboration, Automation, and Scalability in Machine Learning Pipelines." *Journal of Artificial Intelligence Research and Applications* 1.2 (2021): 58-88.
3. Ponnusamy, Sivakumar, and Dinesh Eswararaj. "Navigating the Modernization of Legacy Applications and Data: Effective Strategies and Best Practices." Asian Journal of Research in Computer Science 16.4 (2023): 239-256.
4. Shahane, Vishal. "Investigating the Efficacy of Machine Learning Models for Automated Failure Detection and Root Cause Analysis in Cloud Service Infrastructure." *African Journal of Artificial Intelligence and Sustainable Development*2.2 (2022): 26-51.
5. Muthusubramanian, Muthukrishnan, and Jawaharbabu Jeyaraman. "Data Engineering Innovations: Exploring the Intersection with Cloud Computing, Machine Learning, and AI." *Journal of Knowledge Learning and Science Technology ISSN: 2959-6386 (online)* 1.1 (2023): 76-84.
6. Tillu, Ravish, Bhargav Kumar Konidena, and Vathsala Periyasamy. "Navigating Regulatory Complexity: Leveraging AI/ML for Accurate Reporting." *Journal of Knowledge Learning and Science Technology ISSN: 2959-6386 (online)* 2.2 (2023): 149-166.
7. Sharma, Kapil Kumar, Manish Tomar, and Anish Tadimarri. "AI-driven marketing: Transforming sales processes for success in the digital age." *Journal of Knowledge Learning and Science Technology ISSN: 2959-6386 (online)* 2.2 (2023): 250-260.

8. Abouelyazid, Mahmoud. "Natural Language Processing for Automated Customer Support in E-Commerce: Advanced Techniques for Intent Recognition and Response Generation." *Journal of AI-Assisted Scientific Discovery* 2.1 (2022): 195-232.
9. Prabhod, Kummaragunta Joel. "Utilizing Foundation Models and Reinforcement Learning for Intelligent Robotics: Enhancing Autonomous Task Performance in Dynamic Environments." *Journal of Artificial Intelligence Research* 2.2 (2022): 1-20.
10. Tatineni, Sumanth, and Anirudh Mustyala. "AI-Powered Automation in DevOps for Intelligent Release Management: Techniques for Reducing Deployment Failures and Improving Software Quality." Advances in Deep Learning Techniques 1.1 (2021): 74-110.