AI-driven Adaptive Access Control Mechanisms for Autonomous Vehicle Systems

By Dr. Ngozi Oluwafemi

Associate Professor of Artificial Intelligence, Covenant University, Nigeria

1. Introduction

When considering road infrastructure for autonomous vehicles, it would be natural to imagine this infrastructure with a potentially different configuration compared to current infrastructure. The assembly of different types of road, equipped with different sensors, that have to communicate with each other, would increase risk of failures and attacks. Therefore, equipping the road infrastructure with loosely coupled IoT sensors and detectors to enhance road safety and security for autonomous vehicles is a non-sense task. Indeed, road-side infrastructure has applications mainly for driver-assistance and can generally rotate at low frequency, thus it does not need high data rates. Therefore, we should integrate this detection system for potential dangers in the vehicle or directly in the inter-V2V communication process.

Nowadays, autonomous vehicles are the cutting-edge technology in the automotive industry due to the numerous benefits they bring, as can be seen in [1]. Transportation systems are known to facilitate people's lives by offering them the mobility to travel from one place to another at the expense of time, effort, and money. Smart cities and efficient transportation systems are essential today to reduce environmental impact and insure the wellbeing of people living in urban environments, as stated in [2]. Autonomous vehicles are a key to provide safety and reliable transportation systems. The number of vehicles is expected to drastically increase, leading us to move from standard driving systems to intelligent transportation systems. This evolution requires thinking about new adaptive access control mechanisms to meet higher requirements in terms of safety, comfort and security as can be seen in [3].

2. Background and Significance

[1] [4]In recent years, AI-driven decision-making technologies and big data analysis technologies have developed rapidly, which led to the premise of this article, related to the driving risk of autonomous vehicle systems transformed from the intelligent transportation system. The operational lifecycle management of autonomous vehicle systems is obtained in terms of the development and maintenance phases. The behavioral characteristics of risk assets in the networked environment facilitate the satisfaction of security requirements in the market-oriented operation of the system, and have gradually evolved in this direction. The monetization and interactive security verification methods as well as the dynamic maintenance approach based on big data analytics are introduced for adaptive control to respond to dynamic security threats and changes in the user driving environment based on the characteristics of dynamic security threats such as the preference and driving level of the user in terms of ADS operational lifecycle management.[3]Licensing, electronic stability control, and tire pressure monitoring system technologies are gradually introduced into a vehicle development process by type. The cognitive functions of the vehicle operator are reduced during vehicle operation. These factors have increased the risk of driving safety. At present, the simulation test and road test of an autonomous vehicle cannot cover various traffic scenarios, so an AI-driven autonomous vehicle system is prone to unknown driving safety problems. The method can be dynamically responded to in the face of driving threats such as environmental factors and driving scenarios based on the dynamic cognitive level, emotions, and vehicle operating level of the vehicle user.

2.1. Autonomous Vehicles

An AV can be divided into several high-level subsystems, such as perception, localization, planning, control, and system operations. The system may also be further divided based on specifics, including an application (for instance off-road AVs, as perceived through RGB-D sensors instead of visual cameras) or the specific decision-making algorithms used (like hand-coded rule-based systems, or learned perception-action systems based on high-dimensional representations). For the scope of this paper, the five high-level subsystems can be taken as an example—a system-wide hierarchical architecture. This provides an organizing framework for understanding the diverse kinds of expectations that go into the AV system's AI model [5].

Autonomous vehicles (AVs) are capable of operating on a road network without a human driver and are the subject of significant investment, research, and development worldwide [1]. Much like other autonomous systems, AVs operate on the premise of taking in information about the world in which they exist, processing it into a representation that can be used for decision-making, executing actions in the real world, and evaluating the consequences of those actions before taking further decisions. The majority of the on-board processing occurs automatically without human feedback or intervention; however, current commercial systems still require some level of human input (see Level 2 or 3 driving automation). There is a common perception that the development of autonomous systems will revolutionize modern transportation by providing safe, efficient, and cost-effective access to individuals of all mobility needs [6]. Figure 1 shows the hierarchical architecture of an autonomous vehicle (AV) vestibular system, providing a metaphor for the key components of an AV system that operate together for autonomous navigation and lessens reliance on human perception.

2.2. Access Control Mechanisms

In order to procure a secure and reliable autonomous vehicle (AV) system, we have to combine appropriate features of network, AI, IoT and embedding systems. Consequently, in this part, we will propose an AI-based approach of the access control mechanism according to the potential constraints and constraints to enforce. This will be concerning the projection of an advanced intrusion detection framework, solid privacy means and collaborative community radicals, coming to obtain a security architecture (for AV) and a threat model [3]. This will be in the aim of having effective data protection corresponding to the level of autonomy of the vehicle. The collaborative process will be necessarily carried on on the access control model based on the risks of the adaptive and continuous threats overcoming the static monitoring only.

[7] In an autonomous driving system environment, classical security mechanisms such as encryption and authentication can play a pivotal role in some aspects such as communication security and data privacy. In fact, they are completely necessary in a fully connected AD system based on Software-Defined Networking (SDN). However, in order to enforce a solid security for this comprehensive paradigm, it is proportionally essential to define access control policies and authorization mechanisms that can match with the level of autonomy, capability, rights and adaptation of the expected levels of an AD system. In point of fact, the

composition and organization of accessing processes, while integrating aspects of AI/ML and progresses provided by IoT, constitute the elements to guide the design of access control mechanisms. Consequently, this area is a field of actual and active research about intelligent driving in order to integrate AI and embedded systems security in ADSCA on the basis of the titles, six to eight answers and especially nine and 10 papers well referenced [8].

2.3. Role of AI

[9] Studies have indicated the inevitability of data breaching, whether in autonomous vehicles, healthcare applications, cloud services, or others. Perhaps one of the major security concerns for autonomous vehicles is the risk of unexpected adversarial incidents where an attacker can fool a machine learning model, and as a result a vehicle may execute unintended driving behaviors. This implies that AVs should be capable of capturing and understanding a wide range of contextual details beyond environmental contexts to be secure and resilient. In fact, research has shown that there is a close relationship between humans' environment understanding and their perception of the isolated environmental contexts. Consequently, human-like AVs should have the environment understanding ability to ensure their decision making being influenced by different legitimate but conflicting criteria simultaneously.[2] AI is at the center to build AVs in the near future and has recently become a must-have core technology in several challenging domains including healthcare, financial, security, farming, and energy. The pattern of the plethora of intelligent applications and services stands for what is being called oversmart and it impacts all aspects of our lives to make us addicted users of newly composed intelligent services. Currently, the major applications of AI technologies in AVs are autonomously predicting the states of ego vehicles and road users, intelligent hazard\obstacle detection, intelligent driving assistance, and autonomous high-level decision-making not limited to overtaking, parking, changing the lane and routing and re-routing. AI is also in charge of context awareness at a variety of cognitive levels through which AVs could support the development of effective esafety solutions through synergistic cooperation among AVs, road users, and infrastructures. AVs are expected to make their decisions considering explicit user preferences, industry rules and long-term collective experience and expert knowledge about road vehicles, the upcoming road networks, environmental stochastic models, market trends, and human-driven vehicle profiles.

3. Literature Review

Additionally, the on-board image/viedo data processing software simulates and realizes the functions which should be operated by human before the infusion of AV [10]. Actually, autonomous driving heavily depends on the quality and reliability of perception presented by the sensors. Recent journals and prespective have studied the responsible AI in intelligent vehicles and traffic researchers take notice in AI-Smart cities. A system should funnel requisite information for the AI modules from a tremendous amount of big data generated from various sources, e.g., surveillance cameras, traffic signals, road side units, infrastructure sensors, traffic lights, smart phone GPS data, dedicated short-range communication (DSRC) devices on vehicles, radio-frequency identification (RFID), etc. This huge amount of data will contribute to information on topographic, environmental, traffic, mobility, user, etc., for the backend AI modules.

Autonomous vehicle (AV) systems are envisioned to redefine urban mobility by making our roads safer, greener, and more inclusive and make commuting by car less stressful for the human driver [11]. AV systems are built on a strong foundation of state-of-the-art (STA) technologies which include communication, cloud computing, big data and information and communication technology (ICT). These STA technology sets drive the construction of autonomous driving, a core technology for AV systems. Flooded with data generated from the sensors of autonomous vehicles and the mobility services used for intelligent traffic, there is a deluge of data around us, which has brought us to the ‘big data era’ [2]. How this huge volume of varied data will be transformed and distributed by using ICT is critical to the future of AV systems for urban mobility. To enable efficient AV systems for urban mobility, the urban infrastructure will have to communicate real-time dynamic traffic and road information to the vehicles as well, which will help AVs to take decisions about its traffic path along with V2X communications both at short and long distance. Urban AVs will require accurate and automatic localisation in order to relive the human workload of driving a car and to provide a reliable position data source for future mobility services. Considering these, ADAS technologies provide sensors and vehicle operational control systems to advance the day-by-day autonomous driving.

3.1. Existing Access Control Mechanisms for AVs

The authors in [12] have proposed and mentioned the company about two others papers such as“An AI-based Advanced Driving Assistance System for Camera Images from Autonomous Vehicles” and “An Advanced Driving Assistance System-based On LiDAR and Camera Images from Autonomous Vehicles” where they consider that the modern car is already a computer on wheels, equipped with sensing, computation and actuation capabilities, which altogether make it a suitable candidate as a component for connected self-driving behavior in IoT networks. Already today advanced drivers assistance systems (ADAS) are commercially offered, representing the antecedent of self-driving capabilities. Automated driver assistance systems (ADAS), autonomously assisted, proactively actuating and fully autonomous systems are terms coming up as advanced increasingly in parallel with technology and legal topics. There are a wide arrange of different car parking and overtake systems commercially offered, augumented realitiy (AR) in-car information systems, automatic emergency braking, adaptive cruise control (ACC) and lane keeping assist (LKA), all of them using AI-techniques. Beside the ocular sensing systems being standard, sensor fusion technologies also encompass LiDAR and radar. The mentioned and AI-enhanced in-car info-tainment is seeing an increasingly transformative disruption. Virtual assistants become the new commute time must have beyond AC and comfort. Following market reports, 80% of kilometers traveled might be handled autonomously already in 2021, with the potential to significantly change the whole automotive ecosystem. The connected driving approach inequality is the collision avoidance system (i.e., emergency brake assist and adaptive cruise control) or the climate control system, which adopt automated learning sue to raise user satisfaction in a cost-effective manner. Automated functions are becoming ubiquitously available and increasingly expected and connected for infotainment. The sensors which impedance up the electricity used are unfitown human is in information also outputinting systems. Here, we have chosen an AI-based implementation of an end-to-end cocoon system for an automotive multi-camera setup to ensure the bestblind spot helping systems transportation and safety outcome AI-integrated driver-vehicle communication systems. The developed self-driving camera system COCOMI-PasS is an optical detecting computer vision syston to securely accelerate and brake an end-to-end car.

Much of the traditional research on autonomous vehicles (AVs) is on system-level defense, not the access control directly. As a result, the AVs still face challenges in many key security issues, such as data security and privacy protection, real-time processing power and processing delay, communications security, vehicle security, intelligent attack, and the coexistence of the vehicular network, etc. [3]. Fortunately, the researchers have produced some lightweight access control schemes for Fixed access Ubiquitous WLAN and ad hoc network, focusing on real-time decisions, safety augmentation, and device verification and authentication. The trade-off between security/privacy and performance has been analyzed carefully. Excepting those combinatorial security/privacy problems, there is more interdisciplinary researches on AI and AVs. Unlike the previous metaphor, these new schemes are presented when considering network architecture, vehicles' cooperative safety mechanisms, scene/environment work directions and understanding mixed reality.

3.2. AI Applications in Access Control

Another way of classifying AI systems based on level of automation is by their level of interpretability; it can be referred to as interpretable AI vs non-interpretable AI. Many AI algorithms such as neural networks (NN) are well known for being black-box systems which essentially means that they are good at prediction but horrible at explaining their predictions. Verification and validation of such systems is challenging partly because of this property. Many systems especially those working at levels 4 and 5 have to be sensitive to decisions made by the AI and therefore must have some degree of interpretability [2]. An attractive mechanism for interpretability is using rule-based systems. AI systems that have any kind of interpretation of learned objectives, for example self-explaining neural networks, fall in this category. Also, any machine learning system that utilizes a strong AI model to generate its rules would be considered in this group because it represents a way to interpret BB AI system.

[13] [14]Decision-making in autonomous vehicles combines various methodologies to solve complex scenarios. For example, to perform higher-level tactical decision-making, machine learning models designed and trained for driver prediction are utilized. Various parameters such as proximity of AV to the human-controlled vehicles and the level of confidence that the model has in predicting human vehicle movement are considered for this purpose. This level of decision-making will also utilize experience-based reinforcement learning methods for determining near off-road behaviors in presence of external traffic. Operational zone decision-making concentrates mostly on negotiating simple scenarios such as intersections or merging.

4. AI Algorithms for Adaptive Access Control

The array of sophisticated technologies powering autonomous vehicles are evolving rapidly. Features like lane-keeping, adaptive cruise control, self-parking, and traffic jam assist (TJA) were the highlights of advanced driver-assistance systems (ADAS) until balked by low-road penetration among the public. Now, the industry is embracing fully autonomous driving and it is presumed that in the next decade, fully autonomous vehicles will realize a production viability [15]. The traffic congestion on road networks is a plausible precursor of Autonomous Vehicle (AV) misuse scenarios. For instance, the adversarial angles could abuse AVs to snarl traffic conditions, and hence a community position for verifying AV accessibility privacy is warranted. Valuable insights rooted on user accessibility motives within AVs confirm the critical reliance on solving various privacy, security, and safety issues [5]. AI algorithms are highlighted addressing robustness, effectiveness, efficiency, and resource-aware implementation in AV systems. AI algorithms for scene understanding, actor identification and tracking, motion planning, and controller design are recurrent in the context. By highlighting the limitations in the AI-driven AV system, the community envisions to establish a smart ecosystem to human infrastructure, critical stakeholders, and testing domains, thus accelerating economic, social, and environmental benefits to the users [2].

4.1. Machine Learning Algorithms

Machine Learning (ML) is widely used in ADAS functions. One popular algorithm used in function like Automatic Emergency Braking (AEB), Adaptive Cruise Control (ACC) and Lane Keeping Assist (LKA), is the Support Vector Machine (SVM). Optimization is the task of finding an input for a given function that results in the maximum or minimum of the function. MLP was trained and validated with data from full vehicle system simulations, providing detailed predictions of passenger vehicle speeds, even at larger lead distances. Research developed the concept of risk zones that are calculated from the prediction and interpreted as polygon "footprints‟ around the ego vehicle. This risk zone calculation demonstrates a new method for distributing driving responsibility within the overall control system: When the ego vehicle is in the center of the risk zone there are no warnings created by the vehicle, even though there might be tasks on the todo list of the driver, meaning all foreseeable collision scenarios can still be avoided using vehicle systems, if necessary [16].

The vehicular industry majors made numerous efforts brought significant progress in advancements like electrification, autonomy, and connectivity, which establishes attractive market dynamics to sustenance mobility ecosystem stakeholders. The advent of electrification, contribute towards sustainability, and the contextualization of auto-Mobiles further connect the millennials' ecosystem owing to its sustainability-centric visions. The effective validation and verification of software solutions, in the context of thresholds for deploying software, integrative to a vehicle system, are substantial issues. The two methods chosen: Model-Integrated Computing and Machine Learning, bring advancements and the relevance of using trust, to handle attacks and applicable scenarios, realte around using control-theoretic solutions [17]. Further novelty proposed and evaluated through a set of illustrative simulations, are the handling of delicate influences related to intrinsic model-theoretic communications and all responses showcased significant improvements in trends that could have been negligibly addressed either focusing on robustness and fairness alone.

4.2. Deep Learning Algorithms

We propose a scalable and provably polynomial iteration-complexity algorithm, l1-Doubly-Regularized ADMM for Asynchronous Parallel Inference, which provides an alternative to heuristics like the hard-thresholding proximal updates [18]. We also use the Stability Aproximation in order to have a sample complexity theorem proving that the extra regularization scales better, from a statistical standpoint that depends critically on the number of non-zero elementary signals in the aggregated signal. We use the Mixed Noise Results to prove power-law reductions (in the number of thresholded measurements) for Bayesian Probabilistic Inference if the noise variance in the measurements is super-Gaussian [19].

Bayes Loss is threshold-independent and proper in the sense that it estimates the error in the same probability space of the data. We develop a new, scalable ADMM (Alternating Direction Method of Multipliers) algorithm that uses the soft thresholding operator for variational optimization over a mixture of linear regression. For both Bayesian Probabilistic and this Variational ADMM, we prove that the relaxed iterates converge almost surely to their minimizers, a result deeply connected to the variational theory of gradient flows (Semi-Algebraic Schemes, Keller-Segel Systems) [15].

5. Design and Implementation of Adaptive Access Control System

The presented A3-A3 concept enables the development of a cloud-based, Adaptive, Access Control Management System significantly to reduce the processing application response time in the Butterware system. The Owner Resource has the control point in the different entity resources. As an experimental setup model, the laboratory is established using Raspberry Pi 3 B+, NUC 5i5 Docker microservers, and 4G LTE and the experimental environment setup is explained in [20]. The Arbitrary edge data is set up to generate heterogenous dataset using IoT SENSORS and for training CNN. The ACLs are a group of IPv4 address strings that represent the policy decision set by creating rules to allow or deny communication requests in and out of the Raspberry Pi [6].

An adaptive access control system based on the designed methods for generating an Access Control Policy Module is integrated into the Butterware System. The Adaptive Access Control module chooses the minimum association key permission while sending results. When edge data generation runs on the Raspberry Pi, the Adaptive Access Control checks for the keys generated at the edge data module before sending the access control request to the Policy Decision Point, resulting in enhancing the speed of action. An entity resource is set containing the public keys of the other devices in the system. Notification one can get the corresponding entity resource from the IoT Registry to get all the public keys of the IoT infrastructure and Butterware system. An Integration Server is then deployed parallel to the Butterware system, which will receive the collected assuming data. In the Butterware system, a method is generated for developing the adaptive and inquisitive bucketing techniques based on the predefined security priority rules.

6. Case Studies and Use Cases

In summary, intelligent access control mechanisms are a promising option to boost the traffic efficiency of congested networks, be they motorway, urban, or highway junction ones, by relaxing frustrating artificial car placement maintenance constraints enforcing stop-and-go travel. Moreover, a cognitive subsystem based one such adaptive access control mechanism is a useful tool of the SocioVeh framework further facilitating the microscopic simulation of architectures ground on artificial reasoning. This means that the excellent performance in terms of speed and accuracy of the automotive robotic system (Cooperative Collision Avoidance) can be sustained efficiently. Due to AI I-wide functional and conceptual backgrounds, and DE's unimportance in regulator design, xml-based input/output models can effectively support pragramatic control board level. An automotive case study from previous ADAC seems to support this. A clear tear-splitting strategy appears as certain encoderless can nan. Multiple process models for the same continuous time one have been identified just as non-can input-output parameter relationship. The switched-output stabilizability, as a special heuristic feature in the template area of kernel function, has been conveniently extended to safety, and more recently to reoptimization in the switched sen MegaDVCMAADM based SD-RIROMAFAs dead verdade-free syndrome test. The biomimetic implementation of such research can possibly clone, code approve LAMIKltra, and activate all similar reputation chips [parad transformations].

In such cases, a controller shall maintain a state of being in control in face of ego vehicle actuation errors. The true longitudinal safety limit is estimated by means of an artificial neural network. If, in autonomous or heavily automated driving, the distance to the micro-attractor stroke is valuable small, the reentry motion starts under access conditions for which the car still remains within the ego scenario's margin of safety [Safety of autonomous vehicles: A survey on Model-based vs. AI-based approaches]. The control state system is sample behavior capable. In CarMaker, this database is built by systematically disturbing parameter levels (that pull together those of the real ego scenario) within their limits and allows, hence synergetic simulations of the worst case sliding car at realistic μz values only in longitude, at constant steering angle. While perfect standard simulation of the ADAS system is allowed by CarMaker, secure standard simulation of the combined ADAS + car interaction cannot be claimed since disruptive ADAS effect parameters in the first interval may lead to atypical ego scenario states. By contrast, the standard simulation of the combined ADAS + car behavior using the unified vehicle model/ADAS-interface requires also the rewriting and adaption of adapted access control initialization tables in each hierarchical vehicle representation.

To further present the utility of AI-driven adaptive access control mechanisms for autonomous driving systems, let us consider a few relevant case studies and use cases of the model explained above. These case studies allow a better understanding of the applicability, adaptability, and fault tolerance of the adaptive access control mechanism currently discussed in the paper [Advancing autonomy through lifelong learning: a survey of autonomous intelligent systems]. Consider the well-known example of an adaptive cruise control (ACC) system that leverages networked resources to update safety recommendations based on a decentralized runtime learning algorithm. It has been shown that the adaptive system can make various recommendations for the same scenario at different points in time. For instance, the first recommendation could be "keep current average speed", a subsequent recommendation could be "slow down to average speed by 176 m", and so on. Such a system can configure its runtime algorithm to predict the benefits of the recommended strategy. The current runtime prediction will significantly contribute to a situation-aware context that is adapted over time by invoking the feedback-loop adaptive learning mechanism. This helps to avoid unwanted behaviour as, for instance, false-positive, self-induced hard braking interventions [An overview of VANET vehicular networks]. Similarly, the predictive vehicle-specific dangers do not only depend on epoxy road surface roughness attributes, but also, on attitudinal factors of the car driver. In adverse cases, i.e., for instance, when the driver has got no driving experience offers VW-based longitudinal safety limits that are beyond the radix wheel tire grip ($\mu x = 1$) even on dry roads.

6.1. Urban Mobility Systems

Further, the availability to make vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication promises improved traffic flow and safety. The authors use a modular learning framework by MORGAN et al. consisting of a mixture of control learning and planning modules. The learning modules control agent behavior through various ways such as supervised learning, reinforcement learning and especially through human-in-the-loop studies. The task distribution among learning and planning modules can be adapted dynamically based on road geometry, congestion level, intersection demand and pedestrian presence. We demonstrate that our approach can outperform a wide range of state-of-the-art baseline policies ranging from classical Traffic-Dependent Routing algorithms over model-predictive control policies to reinforcement learning algorithms in various experiment setups, validating the concept of a modular learning-based mixed-autonomy control framework. We emphasize how our employed modular learning framework can improve the adaptability of mixed-autonomy traffic by re-learning from diverse, synthesized road scenarios and rewarding rare behaviors. It caters to a curious desire to make vehicles move less predictably and adapt to the unexpected behavior of vulnerable road users. The latter aspect is heavily underrepresented in state-of-the-art benchmarks for autonomous driving. Therefore, we wish that our benchmarks will serve as a reference for future research or influence reward function design [21].

A traffic management system must be designed to address the concerns of stakeholders. To introduce highly-automated vehicles (HAVs) into urban traffic, a firm cooperation between HAVs, other road users, the road infrastructure, and the traffic control center is necessary. In this work, intersection control algorithms that assign optimized driving instructions to all detected agents, such that they reach their destinations while obeying traffic rules, are designed [22]. These instruction include stopping, acceleration, steering, and communicating intentions, and are issued by traffic control centers. All driving instructions are scheduled such that they are communicated and executed by the time they are needed. The driving instructions are first determined to be physically feasible and safe to execute. The goal of this author is to connect autonomous driving to other relevant AI safety topics and to show how the AI safety analysis of HAVs should differ from a standard discussion found in the literature. The authors have developed the paper story starting from threats at the driving-relevant decision level to cyber-physical level and could not go more into HW level or human/morals issues, but it is in our intention for the final submission. Here are a few challenges related to demonstrating that a driving system is sufficiently safe: We cannot behave optimally in human Society, rigid implementation of the safe set concept is unfeasible in dynamic environments, and Failure due to noise, communications and mechanical failure [23].

6.2. Fleet Management Systems

The decision-making of our vehicle fleet management occurs on a fully automated electronic commerce route, including different destinations. The associated route decisions are made charted and perfected by AI models, controllers, and simulation elements. Here, AI vehicles take the users over the road and make all decisions in a tandem quest. This adaptation to particular route topologies and learning. These own initializations are further aided by evolved driver assistance systems and cooperative sensor and ICT modules, which work to collect, act, learn, and then even imitate (mirror) consumptive and profitable human motives. This eventually becomes considerable as a systems access mechanism leveraging increasing vehicle digitalization [21].

With an increasing number of connected and semi- or fully automated vehicles on the roads, vehicles, individuals and groups comprising a networked fleet, and agencies will become more comfortable, confident and effective if decision-making over established, selected and learned routes, destinations, and driver assistance zones can be shifted increasingly over to AI-driven systems. This chapter starts with a focus on an autonomous vehicle fleet [24], but illustrates the strong potential for also leveraging driver assistance systems for individual effects within, through, or into fleets. Using multiple enabling technologies, which can be categorized as artificial intelligence (AI) acts, our method illustrates navigation planning and (adaptive) access control planning over learned or designed (adaptive) routes and zones for multiple fleets or career path coordinations of a herd of (semi-)autonomous vehicles.

7. Evaluation Metrics

The performance of the proposed MDP based adaptive access control system has been evaluated using the Q-Learning algorithm. The metrics reported in Section is obtained by considering 10% poison rates [25]. A poison rate equal to 30% resulted in an invalid exploration of the state-action space and learning failed, this was also observed by Sahin et al.. The Learning rate is kept to 0.5 for all the environments. It is interesting to observe that more challenging environments require a larger exploration rate to refine the policy. Indeed, low exploration rates reduce the quality of actions chosen while low learning rates lead to a slow convergence in some curves. For example, in the more challenging environments Initialization and EVP, the learning rate will be lowered to 0.5 and the exploration rate will go up to 0.9 meaning different policy evaluations must be considered. Despite this, it is still possible to reason on metric marginal improvements after retrainings.

In this section we introduce the metrics used to evaluate the behavior of ASS and to comprehensively assess the performance of the A2RM [26]. Autonomous Security Systems (ASS), presented in [27], combine adaptive access control mechanisms with resources to ensure that the system operates correctly and securely. ASS are complex, encapsulating complex control strategies, uncertain environments, and a broad set of input characteristics for access control policies. Evaluating and validating the security of ASS profoundly differs from evaluating other classical systems where input-output mappings need to be assessed. Assessing operational security of ASS essentially requires considering the interaction of the different agents impacting the operational security targets. This chapter proposes evaluating metrics considering regular security vulnerabilities and if required reflecting the specific constraints of autonomous and constraint that AV may access the security policies of the AS as resources. This allows us to reason directly on policy mismatches and their potential security consequences instead of reasoning about individual security vulnerabilities like we typically do in cyber security.

7.1. Performance Metrics

We deployed a tailored internet-wide scanning campaign to analyze the evolution of three automotive file-related remote command attribute holders, which—significantly—increased from 15.1k active instances in August 2018 to 27.8k in December 2018: an increase of 85.1%. Our analysis focuses on four separate automotive data breaches tied to the automotive dossier application three of which were major—running from the 31st of December 2016. to the 31st of October 2020.ätze Sarah Ann-Marie Antos, Chutian Alex Xiang Armerding and P. Gabriel Jime?nez Daniel Güttler and Cem Ismail Caglar Abstract The automotive industry is experiencing an unprecedented transformation, its first large-scale digitalization processes in history. Information security in autonomous vehicle systems is of significant interest and has received attention from the automotive industry and academia in recent years. Specifically, academic and non-academic automotive security researchers primarily focus on the following four broad security research areas: lightweight cryptographic protocol algorithms, data processing algorithms, access control/check mechanisms and secure communication algorithms [3, 7, 8].

[28], [27]A range of potential performance metrics covering network security and automotive safety are described in. Each controller is capable of issuing numerous requests to access separate parts of the database using the 'TOY' cross-domain benchmark. The third-level administrative controller is the only mechanism that is able to pose a request for any file blocks of the automotive dossier from the second-level administrative controller, which manages the content of the database. Curiously (14) does not compare its measurements to a reference and its calibration and measurement methodology to any other similar works. However, we have tested our setup for vertical offset by bringing our precision gauge block (δz ≈ 0.9181 mm) in contact with the AFM tip surface.

7.2. Security Metrics

The security risks posed by connected vehicle communication systems have attracted the attention of researchers and inspired the development of security systems that use authenticated encryption and digital signature schemes to provide secure and authenticated communication modes [29]. The international community has been promoting the development of Internet of vehicles (IoV) technology for communication networks; however, security has remained a priority in the protection of the information exchange mode since the adoption of the technology. The secure evaluation of SA is essential to contribute to and accelerate the industrial application of preventive management algorithms. Nevertheless, the basic requirements of secure sensor devices and the demand for efficient intrusion protection mechanisms have not been effectively addressed. From the perspective of practicality and safety, this paper highlights an attention model and applies the model to the deep learning-based space information forecasting framework.

Recent trends indicate that more vehicles are being connected in various communication techniques to exchange information (e.g., speed and location) for active safety-related applications. The safety and comfort features integrated into vehicles can be enhanced via this exchange of information [30]. This concept of vehicles collaborating with each other to minimize accidents has stimulated the development of smart vehicles and smart cities. Different forms of vehicles such as buses, motorcycles, and cars all share the roads together and have to maintain a proper distance from one another to ensure safety. Providing a controlled vehicle-to-vehicle (V2V) distance can have a dramatic impact on accident reduction rates. Thus, the problem of selecting a safe-following distance in cooperative automated vehicle platooning (CAVP) has caught the attention of many researchers and experts in the field [31].

8. Challenges and Future Directions

1. Considering adversarial environments: Autonomous vehicles, even those integrated into a centralized system, are likely to face cybersecurity threats. To adapt conventional AdAC approaches that cannot handle complex social/operational constraints to such security threats, blockchain-based SDRU will be useful. Unlike the NGS, security requirements cannot be dynamically adapted into operational requirements. Thus, studying the compromise between them, and building a robust, game-theory-driven approach that adversarially handles the trade-off between them is required [9]. 2. Integrating SUs in AdAC: Advising users, such as pedestrians, about an autonomous vehicle system, improved security. Competition between SUs and PUs can be interpreted as an intelligent interpersonal behaviour. Accordingly, a Q-learning-based SDRU-A and game-theoretic IAS models will be worth researching. On the other hand, the iso-parent research is valuable to investigate the security-fairness trade-off between users and pedestrians. Each of the above-mentioned scenarios can also be modelled as a sequential decision process whose solution involves optimizing for a balance of each of the objectives jointly. Developing such an AdAC mechanism or linking the operational phase with the social phase can be a crucial contribution for autonomous vehicle systems.

Developing a comprehensive and efficient adaptive access control (AdAC) mechanism for autonomous vehicles in different operational and social contexts, while considering the privacy and interference constraints of competing users, is a complex challenge. Although AdAC mechanisms have been primarily designed to improve security in vehicular networks (VNs) and connected vehicles [20], this chapter has identified major limitations in recent works conducted on this subject within the domain of autonomous vehicle systems. These limitations were identified after considering several factors such as: privacy issues, suitability of operational contexts, application of NGS and SUs in autonomous vehicle systems, both communication and access control in a single control loop, and the motivation for developing interdependent models considering both operational constraints and social or safety context constraints. Future research works can focus on overcoming these limitations, and should research could model other relevant contexts and constraints to improve upon the approach proposed in this chapter. Some future research directions are proposed as follows:

8.1. Ethical Considerations

Even though it is determined that highly autonomous and fully autonomous vehicles do not carry any safety risk in terms of ethical dilemmas, the legal orders are insufficient to get rid of these obstacles. The system also knows the autonomous automobile failure and predicts possible human reactions. As a result, pre-accident assessment and autonomous vehicle impacts are among the other legal problems [32]. In order to solve the challenges of autonomous vehicles, legal regulations must be followed first. It is possible to develop legal regulations towards autonomous vehicles, ethical and moral problems can be solved through education and awareness raising, and young people should pay attention to the traffic problems in schools. For example, man-machine team and ethical dilemmas related to the man-machine relationship should be studied. The aim of this study was to review the literature most recently published in a single platform and to contribute to the legal problems arised by highly and fully autonomous vehicles. The article discusses the relationship between autonomous vehicles and legal regulations and the basic concepts particular to autonomous vehicles in the ethical field. It is aimed that the article will be beneficial for those who have responsibilities in the field of law, research or ethical issues associated with the field of artificial intelligence. On the other hand, considerations and wishes about “autonomy” and “automation” can be shaped by the law or law has an impact on formulating considerations and desires.

Various moral and legal challenged exist in the concept of self-driving cars. For example, what happens when the car has to make a decision from which two opponents are involved, for example those who are in danger while breaking by a human driver. With this human reaction and the situation, this decision may vary. The level of autonomy is different between no more automatic and fully automatic vehicles [33]. For the higher levels it is difficult to define the "driver". For this reason, possible ethical dilemmas need to be resolved in autonomous vehicles. The legal status of autonomous vehicles and related ethical challenge ares reviewed from a legal perspective. Dilemmas and ethical problems are looked at in a legal context. In the context of highly and fully autonomous vehicles, it is not possible for issues such as the video part and the concept of trust between the user and the system. While watching movies without the stress of driving, it is seen that trust in television is decreasing. In autonomous vehicles, the trust level can be observed as a stress or driving experience tool. For all this, ethical issues must be resolved first.

8.2. Interoperability Challenges

In recent decades, we have seen various studies aiming to provide technical and software solutions or architecture designs in order to have self-driving cars from different vehicle makers be able to be interoperable to each other and also with other CAV on the road. The real challenge could be the management of the security aspects at all phases from the level of vehicles, supplier chain and connection with the external infrastructures (such as Communication Networks, Clean Energy Systems. etc.) to the data collection, disposal phase, in a reliable and timely manner. An open question is whether the literature's single vehicle-based techniques and architectures could address the new scenario coming from the bulk introduction of that kind of autonomous vehicle. To overcome these challenges, a set of the best practice solution should inspire and pave the way for powerful standards facilitating the safe and effective CAV communication and control.

To promote the widespread and safe adoption of autonomous vehicles, standards need to be established. This includes standards regarding safety, security, privacy, system, and component interoperability. While formal verification techniques can be used to prove system resilience against internal and external cyberattacks, efficient security assessment tools still need to be developed. These tools should be able to evaluate a system's level of cyber protection. The cybersecurity mechanisms should be able to minimize the service impact while fitting various vehicular hardware resource constraints for secure autonomous deployment. However, any tools and mechanisms cannot stay valid without a framework to ensure its interoperability compatibility.

Interoperability Challenges [34] [19]

9. Conclusion and Recommendations

[35] We have presented a comprehensive review of Adaptive Access Control Mechanisms (AACMs) utilizing AI in reference to security of Connected and Autonomous Vehicles (CAVs). Different types of access control are critically analyzed, and better options coherent with contemporary CAV security requirements are proposed. These include AI-driven Context- and Risk-based Access Control Mechanism (CRBC) and a concept of Malicious Behavior based Access Control Mechanism (MBBC). The study bolsters the concept of advanced Risk-Based Access Control Mechanism (RBACM) equipped with contextual information processing and Malicious Behavior Detection (MBD). In this endeavor, remarkable emphasis is given to the relevant provision of resources and permission allocation to entities on the basis of their reputation and a set of attributes and operations, respectively.[36] The CAVs have taken shape of cyber-physical systems. In consideration of its dynamic change in ownership, onboard components, environment, and adaption speed to accomplish roadmap driving, it is essential to have all-inclusive measures to apprehend unauthorized entities and possible events. It is an ongoing matter of focus for scholars to envision different security solutions for such autonomous CAVs capable to exhibit context-aware decisions. Proposed model is crucial due to the fact that, current vehicle intrusion protection systems mostly consider low-level attack events. Moreover, the envisaged cumulative reputation value for any principal/agent is based on its behavior captured at multiple levels. The higher level of risk posed is primarily vocal for mitigation strategies. Hence, in our proposed mechanism, RBACM+CRBC can provide value as an advanced decision system by integrating decision agents from multiple abstraction levels. Using the conceptual model of CAV environments, we have identified resource allocation elements mostly as single abstract entities. Moreover, we defined these entities hierarchically under agent and principal entities. Although notable progress is seen in establishing physical and communicational mechanisms to apprehend intruders, little is done to address the security of logical vehicle mechanisms. AI-driven techniques can exploit the benefit of the context-rich system status to provide security decisions as per the requirements on a case-by-case basis.

10. References

1. [1] D. Iberraken and L. Adouane, "Safety of autonomous vehicles: A survey on Model-based vs. AI-based approaches," 2023. [PDF]
2. [2] C. Englund, E. Erdal Aksoy, F. Alonso-Fernandez, M. Daniel Cooney et al., "AI perspectives in Smart Cities and Communities to enable road vehicle automation and smart traffic control," 2021. [PDF]
3. [3] H. Cao, W. Zou, Y. Wang, T. Song et al., "Emerging Threats in Deep Learning-Based Autonomous Driving: A Comprehensive Survey," 2022. [PDF]
4. [4] D. Zhu, Q. Bu, Z. Zhu, Y. Zhang et al., "Advancing autonomy through lifelong learning: a survey of autonomous intelligent systems," 2024. ncbi.nlm.nih.gov
5. [5] A. Jafar Md Muzahid, S. Fauzi Kamarulzaman, M. Arafatur Rahman, S. Akbar Murad et al., "Multiple vehicle cooperation and collision avoidance in automated vehicles: survey and an AI-enabled conceptual framework," 2023. ncbi.nlm.nih.gov
6. [6] A. Ashutosh, A. Gerl, S. Wagner, L. Brunie et al., "XACML for Mobility (XACML4M)—An Access Control Framework for Connected Vehicles," 2023. ncbi.nlm.nih.gov
7. [7] M. Masud Rana and K. Hossain, "Connected and Autonomous Vehicles and Infrastructures: A Literature Review," 2023. ncbi.nlm.nih.gov
8. Tatineni, Sumanth. "Customer Authentication in Mobile Banking-MLOps Practices and AI-Driven Biometric Authentication Systems." *Journal of Economics & Management Research. SRC/JESMR-266. DOI: doi. org/10.47363/JESMR/2022 (3)* 201 (2022): 2-5.
9. Vemori, Vamsi. "Evolutionary Landscape of Battery Technology and its Impact on Smart Traffic Management Systems for Electric Vehicles in Urban Environments: A Critical Analysis." *Advances in Deep Learning Techniques* 1.1 (2021): 23-57.
10. Shaik, Mahammad, Srinivasan Venkataramanan, and Ashok Kumar Reddy Sadhu. "Fortifying the Expanding Internet of Things Landscape: A Zero Trust Network Architecture Approach for Enhanced Security and Mitigating Resource Constraints." *Journal of Science & Technology* 1.1 (2020): 170-192.
11. [11] S. Paiva, M. Abdul Ahad, G. Tripathi, N. Feroz et al., "Enabling Technologies for Urban Smart Mobility: Recent Trends, Opportunities and Challenges," 2021. ncbi.nlm.nih.gov

12. [12] M. Abdou and H. Ahmed Kamal, "SDC-Net: End-to-End Multitask Self-Driving Car Camera Cocoon IoT-Based System," 2022. ncbi.nlm.nih.gov
13. [13] S. Malik, M. Ahmed Khan, H. El-Sayed, J. Khan et al., "How Do Autonomous Vehicles Decide?," 2022. ncbi.nlm.nih.gov
14. [14] E. Ejichukwu, L. Tong, G. Hazime, and B. Jia, "Enhancing Autonomous Vehicle Design and Testing: A Comprehensive Review of AR and VR Integration," 2024. [PDF]
15. [15] D. Garikapati and S. Sudhir Shetiya, "Autonomous Vehicles: Evolution of Artificial Intelligence and Learning Algorithms," 2024. [PDF]
16. [16] H. Delseny, C. Gabreau, A. Gauffriau, B. Beaudouin et al., "White Paper Machine Learning in Certified Systems," 2021. [PDF]
17. [17] S. Arbabi, S. Dixit, Z. Zheng, D. Oxtoby et al., "Lane-Change Initiation and Planning Approach for Highly Automated Driving on Freeways," 2020. [PDF]
18. [18] M. Moghadam and G. Hugh Elkaim, "A Hierarchical Architecture for Sequential Decision-Making in Autonomous Driving using Deep Reinforcement Learning," 2019. [PDF]
19. [19] D. Haileselassie Hagos and D. B. Rawat, "Recent Advances in Artificial Intelligence and Tactical Autonomy: Current Status, Challenges, and Perspectives," 2022. ncbi.nlm.nih.gov
20. [20] M. Gupta, J. Benson, F. Patwa, and R. Sandhu, "Secure Cloud Assisted Smart Cars Using Dynamic Groups and Attribute Based Access Control," 2019. [PDF]
21. [21] C. Wu, A. Kreidieh, K. Parvate, E. Vinitsky et al., "Flow: A Modular Learning Framework for Mixed Autonomy Traffic," 2017. [PDF]
22. [22] A. Abbas-Turki, Y. Mualla, N. Gaud, D. Calvaresi et al., "Autonomous Intersection Management: Optimal Trajectories and Efficient Scheduling," 2023. ncbi.nlm.nih.gov
23. [23] M. Wäschle, F. Thaler, A. Berres, F. Pölzlbauer et al., "A review on AI Safety in highly automated driving," 2022. ncbi.nlm.nih.gov
24. [24] F. Knoefel, B. Wallace, R. Goubran, I. Sabra et al., "Semi-Autonomous Vehicles as a Cognitive Assistive Device for Older Adults," 2019. ncbi.nlm.nih.gov
25. [25] V. Dubljević, G. F. List, J. Milojevich, N. Ajmeri et al., "Toward a Rational and Ethical Sociotechnical System of Autonomous Vehicles: A Novel Application of Multi-Criteria Decision Analysis," 2021. [PDF]
26. [26] M. Zipfl, B. Schütt, J. Marius Zöllner, and E. Sax, "Fingerprint of a Traffic Scene: an Approach for a Generic and Independent Scene Assessment," 2022. [PDF]

27. [27] X. Chen, H. Wang, A. Razi, B. Russo et al., "Network-level Safety Metrics for Overall Traffic Safety Assessment: A Case Study," 2022. [PDF]
28. [28] M. Arief, Z. Cen, Z. Liu, Z. Huang et al., "Test Against High-Dimensional Uncertainties: Accelerated Evaluation of Autonomous Vehicles with Deep Importance Sampling," 2022. [PDF]
29. [29] H. Singh, B. Weng, S. J. Rao, and D. Elsasser, "A Diversity Analysis of Safety Metrics Comparing Vehicle Performance in the Lead-Vehicle Interaction Regime," 2023. [PDF]
30. [30] J. Felipe González-Saavedra, M. Figueroa, S. Céspedes, and S. Montejo-Sánchez, "Survey of Cooperative Advanced Driver Assistance Systems: From a Holistic and Systemic Vision," 2022. ncbi.nlm.nih.gov
31. [31] S. Tro, I. Grooms, and K. Julien, "Parameterized Ekman boundary layers on the tilted f-plane," 2024. [PDF]
32. [32] A. Biswas and H. C. Wang, "Autonomous Vehicles Enabled by the Integration of IoT, Edge Intelligence, 5G, and Blockchain," 2023. ncbi.nlm.nih.gov
33. [33] A. Kriebitz, R. Max, and C. Lütge, "The German Act on Autonomous Driving: Why Ethics Still Matters," 2022. ncbi.nlm.nih.gov
34. [34] S. A. Abdel Hakeem, H. H. Hussein, and H. W. Kim, "Security Requirements and Challenges of 6G Technologies and Applications," 2022. ncbi.nlm.nih.gov
35. [35] A. Shah, "Adversary ML Resilience in Autonomous Driving Through Human Centered Perception Mechanisms," 2023. [PDF]
36. [36] H. Muslim and M. Itoh, "Long-Term Evaluation of Drivers' Behavioral Adaptation to an Adaptive Collision Avoidance System," 2021. ncbi.nlm.nih.gov