IEEE Open Journal of Vehicular Technology

Received 12 February 2023; accepted 3 April 2023. Date of publication 7 April 2023;
date of current version 27 April 2023. The review of this article was arranged by Editor Yongdong Wu.

Digital Object Identifier 10.1109/OJVT.2023.3265363

Cybersecurity of Autonomous Vehicles: A Systematic Literature Review of Adversarial Attacks and Defense Models

MANSI GIRDHAR [1] (Graduate Student Member, IEEE), JUNHO HONG [1] (Senior Member, IEEE), AND JOHN MOORE [2] (Member, IEEE)

[1]Department of Electrical and Computer Engineering, University of Michigan-Dearborn, Dearborn, MI 48128 USA
[2]Ford Motor Company, Dearborn, MI 48128 USA

CORRESPONDING AUTHOR: JUNHO HONG (e-mail: jhwr@umich.edu)

This work was supported by the Ford-UM Alliance Research Program.

ABSTRACT Autonomous driving (AD) has developed tremendously in parallel with the ongoing development and improvement of deep learning (DL) technology. However, the uptake of artificial intelligence (AI) in AD as the core enabling technology raises serious cybersecurity issues. An enhanced attack surface has been spurred on by the rising digitization of vehicles and the integration of AI features. The performance of the autonomous vehicle (AV)-based applications is constrained by the DL models' susceptibility to adversarial attacks despite their great potential. Hence, AI-enabled AVs face numerous security threats, which prevent the large-scale adoption of AVs. Therefore, it becomes crucial to evolve existing cybersecurity practices to deal with risks associated with the increased uptake of AI. Furthermore, putting defense models into practice against adversarial attacks has grown in importance as a field of study amongst researchers. Therefore, this study seeks to provide an overview of the most recent adversarial defensive and attack models developed in the domain of AD.

INDEX TERMS Autonomous vehicles, artificial intelligence, adversarial machine learning, computer vision, cyber-attacks, cybersecurity, deep learning, defense strategies, tensor perturbations.

I. INTRODUCTION

The revolutionary research on computer-controlled vehicles for automated and assisted driving was initially conducted by the Carnegie Mellon University (CMU) Navigation Laboratory (Navlab) group in 1984 [1]. Over the intervening years, it has attracted significant attention and become a prominent research trend in vehicular technology. Further, as machine learning (ML) and artificial intelligence (AI) have continued to evolve and improve, autonomous vehicles (AVs) have gained rapid advancements. The auto sector is witnessing a technological breakthrough as new generations of cars are exploiting the advances in AI to provide semi-autonomous and autonomous driving (AD) capabilities, which strongly impacts existing behaviors and practices [2]. There are many AD initiatives around different parts of the world. For instance, Google, one of the most extensive networks, developed and outfitted an autonomous car with lane keeping and lane changing applications in 2010 [3]. General Motors (GM) developed the internet of vehicles (IoV)-based ENV series of smart cars to achieve automatic driving and parking in 2017. In a similar vein, Toyota debuted the Lexus LS460 L in 2010, which had an advanced parking assist system [4]. Tesla, an American automotive company, launched the Autopilot 8.1 system, enhancing the performance of existing autonomous cars [5]. Additionally, it currently offers "full self-driving" to owners of private vehicles and provides "self-driving mode" in its automobiles. Hence, these events mark a remarkable landmark in AV development.

Moreover, because there are abundant high-quality datasets available and there are such strict performance requirements, the academic community favors DL models for ML-related tasks in AVs. Since Hinton published his deep belief network (DBN), a novel deep-structured learning architecture, significant advances have been made in DL [6]. Current AVs rely

heavily on DL algorithms, e.g., object detection (OD), image classification (IC), and semantic segmentation (SS) to perform. Traffic sign recognition (TSR) is an essential application of DL in AVs [7]. It uses DL algorithms to categorize the image of a traffic sign that was acquired by the camera sensor and then makes use of the intelligent control system to steer the car in accordance with the classification results.

The risk of driving when operating a fully AV still exists even though they are not subject to human intervention. Despite continuous advancement and significant improvement in the AVs, AD demands further attention from industry and academia due to its sensitive nature and key aspect in diminishing crash rates and saving lives. For instance, 6 million car accidents happen annually in the USA, and the primary reasons behind these crashes include speeding, distraction, alcohol, and reckless driving [8], although these crashes can be dramatically reduced by using AD technology as supporting tools for drivers or in full automation. Contrary to the claims, however, even AVs are not safe from external threats [9]. Several crash incidents have been reported due to AVs' erroneous or abnormal behavior in uncertain, complex, and unseen environments. There are some specific examples of notable crashes. For instance, a Tesla AV operating in "Autopilot" mode resulted in a death in Florida on May 7, 2016 [10]. Similarly, an Uber with a self-driving system collided with a pedestrian in Tempe, Arizona, on November 20, 2018 [11]. Also, Uber had been involved in 37 other crashes before the fatal accident in 2018.

Additionally, there have been a few instances of grey or white hat hackers identifying cybersecurity threats in advanced driver assistance features available in passenger cars. For instance, researchers at Keen Security Labs in China demonstrated a couple of exploits through a camera system in a Tesla Model S [12]. There have also been instances of researchers identifying exploits in perception algorithms used in AVs.

Hence, besides the fact that AVs provide numerous benefits for individuals and society (including increased energy savings, overall traffic flow efficiency, mobility for the disabled, improvements in social cohesion, and reduced traffic congestion and accidents [13]), there are longstanding challenges accompanying the applications of ML that have rendered them adversarial or safety-critical. For example, previous research has discovered that DL models exploited in AVs to mimic human cognitive capabilities are not entirely secure and are highly vulnerable to several attacks that might jeopardize the normal operation of AVs and provide unmodelled threats and unanticipated challenges to safety [14], [15], and [16]. It can be assumed that attackers could identify the existing vulnerabilities and hack the AI applications to initiate a car accident or steal confidential information. So, it is not wrong to assume that if defenders can utilize ML technology to protect the system, it will not be long before it is in the hands of an adversary to evade detection. In these applications, an adversary could be a hostile force intent on causing congestion or accidents or could even simulate peculiar circumstances that reveal weaknesses in a particular AI application. In other words, an attacker may design specific attacks to deceive the AI systems by disseminating carefully crafted patterns in the environment and thus induce unexpected behavior of the AV [17]. These deliberate patterns, often referred to as perturbations, are imperceptible to AV users but intense enough to deceive the AI model time and time again [18], [19], [20], and [21]. So, defensive tactics against adversarial attacks have also been the subject of extensive research [22]. In addition, the physical world itself serves as an adversarial sample generator and DL models are susceptible to perturbations beyond the training set, according to novel research, which shows that adopting defense techniques for man-made adversarial attacks is insufficient. This qualifier necessitates the introduction of general defense strategies for adversary samples from the physical world and man-made objects. It is to be noted that besides the advantages of ML in the AVs, there are some disadvantages. The DL models act as black boxes in the inference phase where the decision-making is not interpretable. In other words, they do not have model interpretability and explainability capabilities. For example, in the work [23], classical algorithms failed to identify an adversarial attack, while the reliable AI methodologies-based on eXplainable AI (logic learning machine) or support vector data description correctly detected a possible adversarial machine learning attack.

Many adversarial attacks have been proposed and demonstrated effectively on image classification models, e.g., [24] and [25]. Numerous methods, for instance, [26] and [27], have been developed to harden neural networks in order to defend adversarial attacks. But prior research has mostly concentrated on image categorization models. The effectiveness of these adversarial attacks and responses against regression models (e.g., autonomous driving models) is unknown. This ambiguity highlights potential security threats and expands research possibilities. Adversarial attackers might easily cause road accidents and endanger personal safety if they are successful in targeting AVs. As a result, it is essential to identify a novel defense mechanism appropriate for autonomous driving if existing defense techniques cannot be modified to defend against attacks on regression models. Although adversarial attacks have been studied in research laboratories and controlled environments, there have been limited adversarial attacks reported on commercial AVs. Cybersecurity experts are raising a concern that these attacks might evolve into a severe issue due to the adoption of ML in higher levels of automation in AVs, thereby putting human lives at peril. Hence, in order to effectively tackle new cybersecurity challenges related to AI or ML, it is crucial that the automotive sector strengthen its incident response capacities and raise its degree of preparedness. Given the challenges of mitigating these attacks, especially in making them inconspicuous to human sight, the serious safety ramifications should compel automakers to adopt defense strategies to minimize AI threats.

The primary contributions of this review article are:

1) presenting a systematic overview of the role of AI in AD,
2) outlining the possible vulnerabilities and limitations of AVs

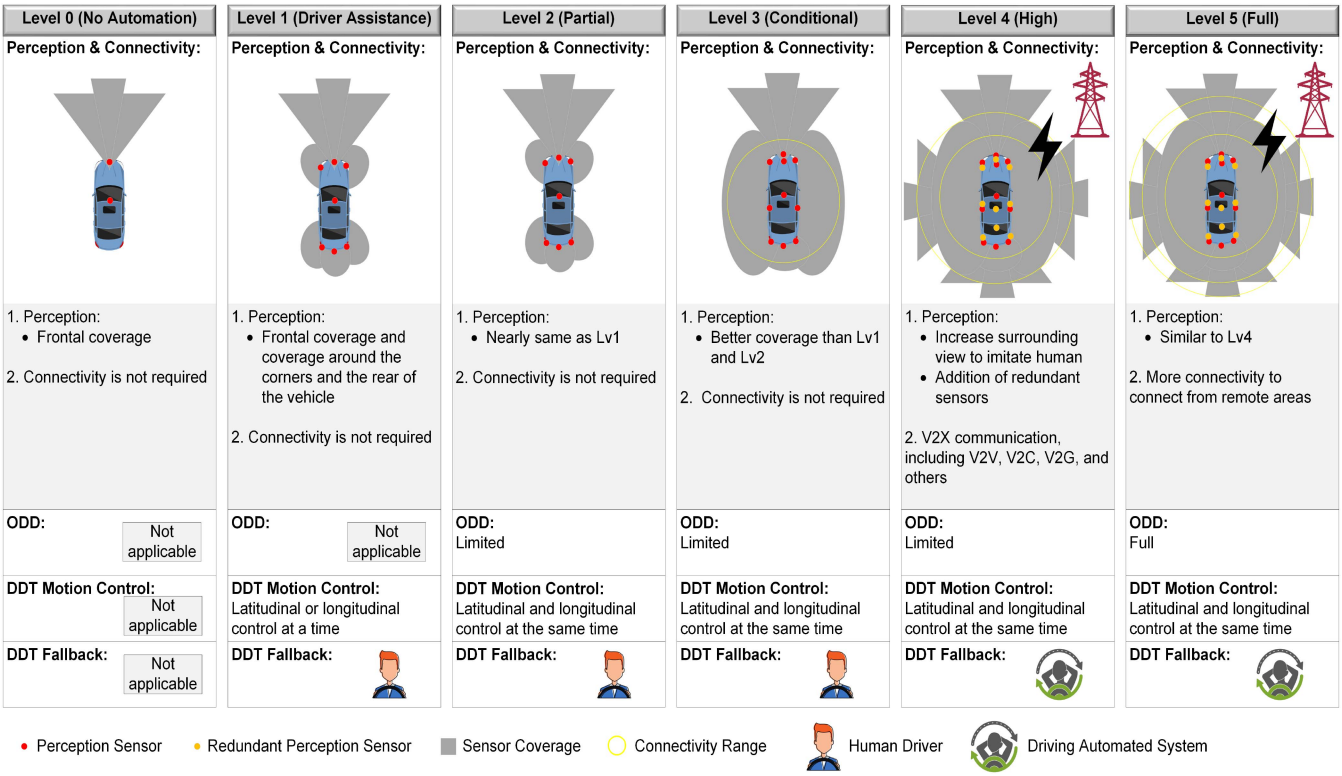

FIGURE 1. Driving automation levels as defined by the SAE J3016 standard.

in the cybersecurity threat landscape, 3) explaining cybersecurity challenges associated with AVs due to the uptake of AI, 4) defining adversarial ML, which renders the AI components in an AV open to be compromised, and 5) proposing suggestions to strengthen AI security in AVs and reduce potential risks and threats.

The remainder of the article is divided as follows:

Section II discusses the high-level overview of the six driving automation levels defined by the society of automotive engineers (SAE). Section III analyzes the engagement of different DL-based algorithms used in AVs. Further, diverse AI vulnerabilities that may jeopardize the safety and security of AVs, and associated elements are outlined in Section IV. Sections V and VI highlight the concept of adversarial ML and summarizes various adversarial ML attacks against AVs, respectively. Section VII analyzes the cybersecurity aspects of AVs, describes underlying standards, and overviews different countermeasures to defend adversarial ML attacks. Finally, Section VIII concludes the article along with the limitations and recommendations for future work.

II. SAE LEVELS OF DRIVING AUTOMATION

Since this work analyzes the effects of adversarial ML attacks on AVs, it is necessary to provide a brief description of how the levels of automation in cars are changing over time. Furthermore, it is critical to comprehend how the increased dependability of various driving applications on ML as a result of improved automation compromises the security and safety of AVs and associated entities.

AVs are typically defined as vehicles with the ability to move and take action without the aid of a conductor (driver) or teleoperation control. In 2014, SAE published the J3016 standard, which was updated significantly in collaboration with the ISO in 2021 [28]. Currently, the SAE J3016 standard of SAE International is the industry's most-cited reference concerning AV capabilities [29]. It is dedicated to advancing mobility engineering worldwide and presents a six-level taxonomy of driving automation [30], as depicted in Fig. 1. The regulatory organizations UNECE WP.29/GRVA [31], NHTSA, US DOT [32], and California DMV [33], as well as the major players in AV standardization like ISO/PAS 21448 (SOTIF) [34], ISO 34501 [35], ISO 34502 [36], ISO 34503 [37], UL4600 [38], IAMTS, and ASAM [39], have all endorsed this standard as a basis for the development of additional AV standards, laws, and regulations. A recent scientometric and bibliometric review article on AVs [40] claims that many name conventions have been employed in recent years for AVs, including self-driving cars, intelligent automobiles, driverless cars, fully automated systems, and others. However, to prevent several definitions with conflicting meanings, SAE advocates using the term "automated driving system (ADS)" to refer to cars with varying degrees of automation. The U.S. National Highway Traffic safety Administration (NHTSA) defines AVs as ADSs in which the vehicle performs the steering, acceleration, and braking

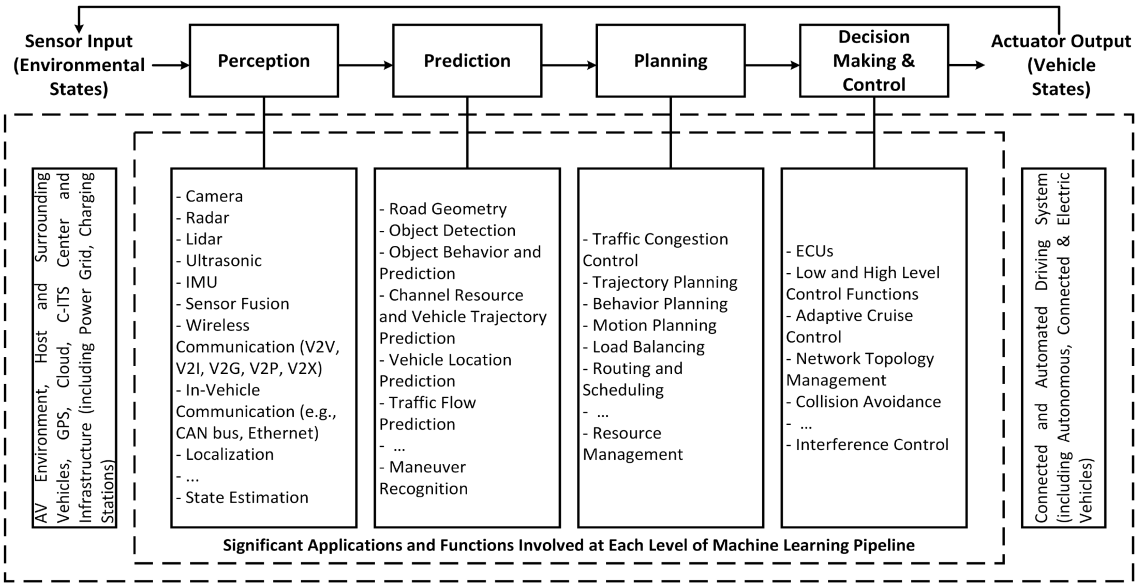

FIGURE 2. The machine learning pipeline of autonomous vehicles.

operations during their engagement. Further, these systems are intelligently designed to monitor roadway conditions (e.g., lane markings, traffic and road signs, pedestrians, cyclists, and potholes) without the driver's intervention.

Six degrees of driving automation, together with the scope and applicability of associated key terminologies used in J3016, e.g., operational design domain (ODD), dynamic driving task (DDT), DDT fallback, and a few more, have been outlined in Fig. 1. According to SAE J3016, ODD is arguably the most critical parameter, as other parameters are highly dependent on it. It can be noticed that the definition of ODD in J3016 is very high level and does not give enough clarity on how ODD can be parameterized. To address this limitation, the European standard PAS 1883 [41] has created a taxonomy document that classifies ODD parameters into three main categories, 1) scenery, 2) environmental conditions, and 3) dynamic elements. SAE has recently started an initiative to create J3259 for ODD taxonomy and definition, but this standard is not yet available for use. In this article, ODD from a perception and connectivity perspective has been analyzed. To exemplify, for perception coverage in L0, only frontal coverage is required, but in L1 and L2, coverage is also required in the rear and four corners. Perception coverage for L3 should be augmented with a surround-view in the nearby vehicle zone, and for L4 and L5, the surround-view coverage needs to be extended like a human driver. Connectivity is recommended starting from L4 to communicate with vehicle-to-everything (V2X) technology, and for L5, the connectivity range needs to be extended to communicate with V2X from remote areas. For DDT, in L3 and above, the expectation is to have complete and continuous DDT by the system, whereas in L1 and L2, it is limited to a sustained basis. DDT fallback is a significant distinguishing factor between L3 and the levels above L3, as the driver is responsible for DDT fallback for L3 features. In contrast, the ADS on the vehicle must handle the DDT fallback for L4 and L5.

III. DEPLOYMENT OF MACHINE LEARNING IN AUTONOMOUS VEHICLES

The ML pipeline of an AV, as illustrated in Fig. 2, utilizes four primary interconnected modules, namely, 1) environmental perception, 2) prediction, 3) planning, and 4) decision-making and control, to link unprocessed sensory inputs and actuator control outputs [42]. These ML-based modules define the driving task elements of the AVs. They are in charge of reproducing complex data-processing and decision-making capabilities that combine to provide a feedback mechanism for supporting self-driving. In addition, the AI software components embedded in AVs facilitate autonomous real-time decisions (e.g., move, stop, and slow down) by exploiting insights (e.g., information on the dynamics of the cars, network topology, and their positions) from the diverse types of data gathered via the sensors. The remaining portions of this section will describe some of the most well-known applications of ML-based techniques to carry out these tasks.

A. MACHINE LEARNING APPLICATIONS FOR PERCEPTION TASKS IN AUTONOMOUS VEHICLES

The perception module gathers numerous streams of on-board and off-board sensory input and analyzes them to identify pertinent data about the area around the driving vehicle. In AVs, the perception process combines cutting-edge sensors, e.g., cameras, radar, LiDAR, ultrasonic, inertial measurement unit (IMU), and global navigation satellite system (GNSS) receivers, and communication technologies with state-of-the-art software systems to perceive the environment in real time. Additionally, they keep an eye on their physical characteristics (localization and state estimation) to aid decision-making.

For the perception task in extremely difficult settings, some academics and engineers have attempted to emulate the operating principles of bio-inspired visual systems to develop an innovative event-based neuromorphic vision sensor [43] that performs better than the most sophisticated artificial vision systems, such as high-quality frame-based cameras, and offers promising qualities, low power consumption, low latency, high dynamic range, and high temporal resolution [44]. The dynamic vision sensor (DVS), which was put forth by the Tobi Delbruck group, is the first event-based neuromorphic vision sensor that is based on a biological concept [45]. The two main techniques employed in the perception systems of AVs are SS and OD [46]. SS is an IC task at the pixel level, where each pixel is assigned to an image belonging to a particular labeled class (e.g., person, bicycle, or tree). Localizing and categorizing the objects of interest in the image are the fundamental goals of OD. This includes lane markings, traffic signs, traffic lights, lanes, and, more broadly, anything that might be of interest to a driver. Tracking people on foot, bicycles, cars, trucks, and other moving things is also included in perception. In addition, it keeps track of the vehicle localization (also called visual odometry), determining its location and orientation in relation to the road and other entities in the scene.

Several ML techniques have been widely adopted to develop the perception system of AVs based on image content analysis. Hashing algorithms, e.g., supervised deep hashing framework (SDHP) and SDHP+, are used in [47]. In [48], an AV is directly represented by a deep convolutional neural network (DCNN) model that can operate in a diverse set of virtual environments. In another work [49], a variant of a CNN is proposed for locating and detecting unexpected roadblocks or obstacles. The work of [50] proposes a complete perception fusion architecture to solve the problem of detecting and tracking moving objects (e.g., pedestrian, bike, car, and truck). A novel TSR algorithm called kernel extreme learning machine (KELM) is proposed using deep perceptual (DP) features in [51]. In another work [52], pothole and wetland OD is performed by using you only look once (YOLO) and CNN algorithms that are implemented on a Raspberry Pi4. Finally, the authors in [53] perform object recognition using more than 500 images of 10 objects (e.g., pedestrians, cars, traffic signs) using CNN models, including single-stage detection (SSD) Inception V2, faster regional CNN (faster R-CNN) Inception V2, and others. In another example, the research of [54] presents a CNN-based traffic-light recognition algorithm for varying illumination conditions.

B. MACHINE LEARNING APPLICATIONS FOR PREDICTION TASKS IN AUTONOMOUS VEHICLES

Also considered one of the two primary functions of the perception system, the prediction module analyzes the dynamics of the environment and forecasts the behavior of nearby objects (positions) [55]. Tracking systems, also called multiple object tracking (MOT), perform this capability by calculating the heading and velocity of the objects and using a motion model to estimate the trajectory.

Another key responsibility for AVs is the timely and accurate prediction of various events in driving scenarios, which is mostly carried out using various ML and DL algorithms. To substantiate, the work in [56] makes use of a deep neural network (DNN) to address the issues of 3D detection, tracking, and motion prediction for AVs. In vehicle behavior prediction, long short-term memory (LSTM) is by far the most prevalent deep model. Based on the states of the target vehicle (TV) and the expected target lane, one LSTM is used to forecast the target lane while a second LSTM is used to predict the trajectory in [57]. In another work [58], the authors use two groups of LSTM networks for modeling the TV's trajectory prediction; one group models the TV's trajectory along with the trajectories of nearby or surrounding vehicles (SVs), while the other group models the interactions between the TV and SVs. A six-layered CNN is employed to estimate the behavior of SVs by the authors in [59]. In [60], two backbone CNN modules are used to process the 3D point clouds produced by a LiDAR sensor and a rasterized map, respectively. In [61], the authors use a simplistic approach for vehicle behavior modeling by relying on only the current state of the AV. The parameters of a Gaussian mixture model (GMM), which simulates the multimodal trajectory of the AV in terms of arrival time and end location, are predicted using a multi-layer, fully linked network. A recurrent neural network (RNN) and a CNN are combined in the study in [62] to process the temporal and spatial characteristics of the input data. The temporal dynamics of the AV are extracted using an LSTM encoder, and a CNN is then used to learn the spatial relationships. The LSTM decoder predicts the future trajectory of the AV. A graph neural network (GNN) is used as a prediction model in [63] to predict the AV's behavior, where the vehicles and their interaction in a driving scenario represent the nodes and the edges of a graph, respectively. Similarly, the authors in [64] evaluate the effectiveness of two cutting-edge GNNs, 1) a graph convolutional network (GCN), and 2) a graph attention network (GAT), at predicting trajectory. Another prediction model in [65] estimates the future behavior of an AV's efficient and intelligent wireless communication networks. Further, in [66], a trajectory prediction model is presented that integrates semi-supervised and-or graph (AOG) and spatio-temporal LSTM (ST-LSTM) to solve several existing problems of maneuver-based trajectory prediction.

C. MACHINE LEARNING APPLICATIONS FOR PLANNING TASKS IN AUTONOMOUS VEHICLES

The fundamental goal of the planning module is to compute/determine the most feasible trajectory of the TV [67] and find the best or the quickest possible route to the destination, considering all the constraints, which include potential obstacles (e.g., stationary objects, moving vehicles, potholes and traffic congestion) that come along the entire path and compliance with driving rules. It makes use of offline maps that are incorporated into the AV and GNSS coordinates. It is in charge of performing vehicle actions autonomously, ranging from route planning (also called global planning) to

motion planning (also called local planning) in a given driving situation. It is also responsible for searching for the fastest maneuver of the TV while simultaneously predicting the paths of other cars and preventing collisions between vehicles [68].

With encouraging outcomes, a number of ML approaches have been used for planning in AVs. The authors in [69] offer an interactive motion predictor that uses a bidirectional LSTM (Bi-LSTM) module to infer the motives of cut-in vehicles. The suggested predictor has three modules, 1) interaction, 2) maneuver recognition, and 3) trajectory prediction. In another work [70], a hybrid solution is provided to model uncertainty in trajectory prediction for an AV by fusing DL models and the kernel density estimation (KDE) technique. In [71], for the spatiotemporal planning of an AV in a multi-vehicle traffic scenario taking into account a roundabout scenario and two complex takeover maneuvers with various moving obstacles, a support vector machine (SVM)-based solution is given. The authors in [72] execute an AV's local planning using a deep reinforcement learning (DRL) method in uncharted tough terrain. The research of [73] presents an SV motion-prediction algorithm for multilane turn intersections using an LSTM-based RNN. Also, a survey presented in [74] describes several DRL-based algorithms used for motion planning problems. In another study [75], a Gaussian process regression (GPR) method is used to present a probabilistic trajectory forecasting of cut-in vehicles that takes advantage of information from intervening vehicles. The authors in [76] propose an AV motion planning for illegally parked cars in no parking zones using SVM.

D. MACHINE LEARNING APPLICATIONS FOR DECISION-MAKING AND CONTROL IN AUTONOMOUS VEHICLES

The control module executes the trajectory or sequences of actions as estimated by the planning module by transmitting command signals to multiple AV actuators at the component level. A car's control motion can be roughly divided into two categories, 1) lateral, which is controlled by the steering wheel, and 2) longitudinal, which is controlled by the accelerator and brake pedals.

DL-based algorithms have been widely utilized in recent years to govern AVs. The work in [77] presents a CNN-based end-to-end learning architecture for self-driving automobiles that immediately converts unprocessed front-facing camera pixels into steering directions. With the least amount of training data from humans, the system effectively operated the vehicle on local roads, even without lane markers and on highways. Similarly, to determine the appropriate steering angle needed to keep the vehicle in its lane, CNN was trained for end-to-end learning in [78]. Recently, researchers have started utilizing DRL for performing actions and decision-making in driving conditions [79] and [80]. A generic approach in line with reinforcement learning (RL) is presented in [81] to manage the speed of AVs using the double Q-learning approach. The authors in [82] proposed a comprehensive framework for connected automobiles that relies on a DRL-based strategy. The work of [83] proposes a hierarchical RL approach for autonomous decision-making and motion planning in complex dynamic traffic scenarios, such as a left turn without traffic signals and multi-lane merging from side roads, by using a kernel-based least-squares policy iteration (KLSPI) algorithm and a dual heuristic programming (DHP) algorithm. The research of [84] proposes an end-to-end RNN algorithm to control the steering angle and to keep up with the autonomous cars in the lane. Another study [85] proposes a CNN-based learning framework to predict the steering angle of a self-driving car. A similar approach proposed by [86] also focused on the end-to-end approach of the self-driving AV to identify two distinct frameworks for performing steering angle prediction with the high feature using DL approaches, such as transfer learning (TL), 3D CNN, LSTM, and RNN. The researchers in [87] present automated ML (AutoML) for risk prediction and behavior assessment, which can be used in AVs' behavioral decision-making and motion trajectory planning. In [88], an RL technique is offered for autonomous decision-making of intelligent automobiles on roads, such as a multi-objective approximate policy iteration (MO-API) algorithm with value function approximation and feature learning. In another work [89], a DRL-based framework, deep deterministic policy gradient (DDPG), is adopted for decision-making in an emergency to solve the autonomous braking problem. The work in [90] uses double deep Q-network (Double DQN) to learn policies (control strategies) for both longitudinal speed and lane change decisions.

E. STATE-OF-THE-ART MACHINE LEARNING ALGORITHMS FOR ADAS APPLICATIONS IN AUTONOMOUS VEHICLES

Advanced driver assistance systems (ADASs) are technological features that are added to vehicles to assist drivers in driving and to enhance safety. Nowadays, ADAS applications use automated technology, such as sensors (radar, LiDAR, ultrasonic) and several external communication techniques, to monitor the vehicle's surroundings, detect driver errors, and respond accordingly. There have been numerous ML algorithms that various researchers in the literature have used for different ADAS applications in AVs.

The research of [91] and [92] uses CNN and R-CNN, respectively, for TSR. In another work [93], the authors suggest an SVM-based system for autonomous traffic sign detection and recognition. In [94], the authors develop a shape-based classification model using SVM. This effort concentrates on identifying five categories of speed limit signs and seven categories of traffic sign shapes. Similarly, in [95], [96], and [97], SVM is used to cope with the detection and recognition of traffic signs from visual sequences. The work of [98] utilizes moment invariants and SVM, an automated method for identifying and detecting traffic signs. In [99], a TSR algorithm based on SVM and CNN for the TSR of intelligent transportation and unmanned vehicles is proposed, while the authors in [100], [101], [102], and [103] use CNN for the application. However, an artificial neural network (ANN) has also been used by many researchers, as shown in [104], [105],

and [106]. Also, in [106], the authors assess ANN along with the application of SVM, decision tree (DT), ensemble learners (Adaboost), and K-nearest neighbor (K-NN) classifiers. In another work [107], a new traffic sign detection and recognition approach is presented using a fuzzy neural network (FNN). The research of [108] compares the application's performance based on the random forest (RF) algorithm, K-NN, and SVM. The authors of [109] compare K-NN, ANN, CNN, and YOLO algorithms for accurate traffic flow detection and building an intelligent transportation system (ITS). In another example, K-NN is employed for video frame recognition and tracking systems for traffic signs in [110]. The authors in [111] evaluate K-NN, SVM, Gaussian process (GP), multilayer perceptron, DT, AdaBoost, RF, Gaussian naive Bayes (GNB), and quadratic discriminant analysis (QDA) for automatic traffic sign detection. DT methodology is being widely used in the literature, e.g., [112], [113], and [114]. The work of [114] also uses RF and SVM for traffic sign classification.

Several research works, e.g., [115] and [116], implemented an SVM algorithm as the classifier for lane departure warning (LDW), while the authors of [117] opted for DNN for the application. In [115], SVM-based prediction of the trajectory of lane-changing vehicles is performed using actual Next Generation Simulation (NGSIM) field data. Also, SVMs outperformed the preceding models and demonstrated particular success in the early detection of lane changes made by drivers. In another work [118], ANN and SVM are used for vehicle trajectory and lane-change prediction. Moreover, the suggested trajectory prediction algorithms can anticipate lane change actions up to three seconds in advance and are 30% more accurate than the vehicle motion model in a time range of four seconds. Similarly, in [119], mask region CNN (mask R-CNN) is used for an LDW system. Some other works, e.g., [120], [121], [122], [123], [124], and [125], exploit CNN for the lane detection function. The researchers in [126] used a K-NN and SVM-based lane detection system. The authors of [127] and [128] implemented K-NN for an LDW ADAS application. For ANN, [129] and [130] are two prestigious works on LDW.

For both lane keep assist (LKA) and lane change assist (LCA), the authors of [131] and [132] applied SVM, and the work of [133] used DNN. The work of [134] develops an autonomous lane-change decision-making model by adopting an SVM algorithm with Bayesian parameters optimization that performs better than the rule-based lane change model. Moreover, the decision model's efficacy was tested by the authors using a real automotive experiment. The work in [135] introduces a lane-changing prediction model based on a hybrid SVM/ANN technique at highway lane drops. The authors in [136] proposed an SVM-based anomaly detection model to identify potential abnormalities that may lead to various hazards during a lane change. It aimed at locating latent hazards posed by SVs that might cause potentially risky maneuvers on roads. In [137], [138], [139], and [140], a DCNN was used to construct an autonomous lane keeping system (LKS) based on a road lane model. Some works, e.g., [141], [142], [143], [144], and [145], implement K-NN for the LKA function. Moreover, the authors in [145] also performed a comparison between the LKSs based on K-NN and LSTM. There is also some literature on RF-based LKSs, including [146] and [147]. ANN-based systems for this ADAS function cited in the literature are [148] and [149].

Likewise, for a forward collision-avoidance assistance (FCAA) or forward collision warning (FCW) system, some research works, including [150], [151], and [152], focused on an RF algorithm, while works [153], [154], and [155] emphasized SVM. In another study, [156], the authors simplified trajectory planning by solving a convex optimization problem formulated as an SVM, resulting in a trajectory planner-friendly, obstacle-free corridor. The works of [157] and [158] used CNN to develop a forward collision alert system. The authors opted for SVM for FCW and LDW functions in [159]. Similarly, the work of [160] implemented SVM for a unique camera-based FCW and LDW system, which provides additional flexibility at a lower cost and has several advantages over the conventional radar/laser-based warning systems.

With the advancement in ADAS applications, automakers are eager to include a smart parking system in AVs that will give drivers access to real-time information regarding parking space availability and location. The research of [161] offers an SVM-based method for determining unoccupied defined parking spaces in lots where the limits of each parking lot are known in advance. In another work [162], a new parking lot system built on SVM and ZigBee technologies is created. Similarly, the authors in [163] proposed a novel method for parking space detection using an SVM classifier. Researchers in [164], [165], and [166] implemented an RF classifier for locating vacant parking slots, while researchers of [167], [168], [169], and [170] chose CNN for parking occupancy detection. Other works, e.g., [171] and [172], used K-NN for this application.

OD's difficulty is in locating and separating an obstacle from a complex background. The literature identified several computer vision algorithms to handle this problem. Authors in [173], [174], and [175] used SVM for vehicle and pedestrian detection, while researchers in [176], [177], and [178] focused on a CNN classifier to design their systems. In other works, [179], [180], and [181], the authors used RF to recognize and steer clear of any obstacles on the path.

An overview of contemporary ML methods for ADAS applications in AVs is shown in Tables 1 and 2. These tables are an effort to turn the reader's attention toward some of the prominent ML algorithms that have been utilized in ADAS applications.

Current systems are already achieving tremendous performance in various conditions, but extreme complexity and uncertainty in the AV ecosystem limits their capacity to perform. For AV researchers, developing the right ML system remains a major issue because it is possible to run into unanticipated situations that are not related to training or data distribution. In that case, proper handling of edge cases for the ML systems becomes a tedious task. Hence, it is a long haul to

TABLE 1. State-of-the-art machine learning algorithms for the ADAS applications in AVs

Machine Learning Algorithms for ADAS Applications				
ADAS Application	**Machine Learning Algorithm**	**Authors**	**Year**	**Reference**
Traffic Sign Detection and Recognition	SVM	Maldonado-Bascon et al.	2007	[93]
		Min et al.	2008	[94]
		Kiran et al.	2009	[95]
		Boi et al.	2011	[97]
		Gomez et al.	2014	[96]
		Agrawal et al.	2017	[98]
		Abedin et al.	2017	[106]
		Narayana et al.	2022	[108]
	CNN	Wei et al.	2018	[91]
		Vennelakanti et al.	2019	[102]
		He et al.	2020	[103]
		Kapoor et al.	2021	[100]
		Pavani et al.	2022	[109]
		Li et al.	2022	[92]
	ANN	Abedin et al.	2017	[106]
		Rezgui et al.	2019	[104]
		Kerim et al.	2021	[105]
		Pavani et al.	2022	[109]
	K-NN	Abedin et al.	2017	[106]
		Reddy et al.	2019	[110]
		Santos et al.	2019	[111]
		Narayana et al.	2022	[108]
		Pavani et al.	2022	[109]
	RF	Zaklouta et al.	2012	[114]
		Santos et al.	2019	[111]
		Narayana et al.	2022	[108]
	Decision Tree	Meuter et al.	2010	[113]
		Song et al.	2012	[112]
		Zaklouta et al.	2012	[114]
		Santos et al.	2019	[111]
Lane Departure Warning	SVM	Tomar et al.	2011	[115]
		Albousefi et al.	2014	[116]
		Izquierdo et al.	2017	[118]
		Narayana et al.	2022	[126]
	CNN	Huang et al.	2015	[117]
		Olanrewaju et al.	2019	[124]
		Chao et al.	2019	[125]
		Qiao et al.	2020	[121]
		Islam et al.	2021	[122]
		Chung et al.	2021	[123]
		Undit et al.	2021	[119]
	ANN	Izquierdo et al.	2017	[118]
		Ambarak et al.	2017	[129]
		Wei et al.	2019	[130]
	K-NN	Hammami et al.	2013	[128]
		Yang et al.	2019	[127]
		Narayana et al.	2022	[126]

TABLE 2. State-of-the-art machine learning algorithms for the ADAS applications in AVs

Machine Learning Algorithms for ADAS Applications				
ADAS Application	**Machine Learning Algorithm**	**Authors**	**Year**	**Reference**
Lane Keep Assist or Lane Change Assist	SVM	Mandalia et al.	2005	[132]
		Dou et al.	2016	[135]
		Ramyar et al.	2016	[136]
		Liu et al.	2019	[134]
		Karthikeyan et al.	2020	[131]
	CNN	Yang et al.	2019	[137]
		Liu et al.	2019	[138]
		Chen et al.	2019	[140]
		Wang et al.	2020	[133]
		Choi et al.	2020	[139]
	ANN	Dou et al.	2016	[135]
		Kruger et al	2019	[148]
		Bian et al.	2020	[149]
	K-NN	Li et al.	2015	[141]
		Zheng et al.	2017	[142]
		Huang et al.	2021	[143]
		Khelfa et al.	2022	[144]
		Long et al.	2022	[145]
	RF	Bai et al.	2019	[147]
		Deng et al.	2020	[146]
Forward Collision Avoidance or Warning	SVM	Lin et al.	2008	[159]
		Salari et al.	2013	[160]
		Iranmanesh et al.	2018	[154]
		Lim et al.	2018	[155]
		Morsali et al.	2019	[156]
		Puspaningrum et al.	2019	[153]
	CNN	Pyo et al.	2016	[158]
		Kumar et al.	2020	[157]
	RF	Lee et al.	2002	[150]
		Wang et al.	2018	[151]
		Teimouri et al.	2018	[152]
Smart Parking (Automatic Slot Detection)	SVM	Wu et al.	2007	[163]
		Zhang et al.	2017	[162]
		Varghese et al.	2020	[161]
	K-NN	Muntean et al.	2019	[172]
		Suheryadi et al.	2021	[171]
	RF	Cho et al.	2018	[166]
		Raj et al.	2019	[164]
		Deb et al.	2022	[165]
Obstacle Detection	SVM	Chen et al.	2013	[173]
		Nguyen et al.	2017	[174]
		Sasaki et al.	2021	[175]
	CNN	Hong et al.	2013	[176]
		Robinson et al.	2020	[177]
		Rajendran et al.	2022	[178]
	RF	Zhang et al.	2020	[179]
		Ahmed Mahdi	2020	[180]
		A.M. Abdulkadium	2020	[181]

certify that an AI-based system will produce accurate findings in unexpected situations, resulting in potentially dangerous events.

IV. AI VULNERABILITIES IN AUTONOMOUS DRIVING

Investigating the security issues and AV flaws of AI that may jeopardize the safety of users, pedestrians, other vehicles, and associated infrastructures is a critical issue. Additionally, AI-related security flaws are allowing exploitation of ML system-specific vulnerabilities as well as software and hardware flaws in digital systems, expanding the attack surface and raising the possibility of physical attacks and cyber-attacks on an AV. Typical threats associated with AI are broadly classified into two main categories, 1) intentional and 2) unintentional.

Intentional threats occur when bad actors maliciously take advantage of the shortcomings and weaknesses of AI techniques with the goal of interfering with the AI system and impairing safety-critical operations. Such attacks include painting the road to confuse drivers or placing stickers on a stop sign to obscure the view [182], [183], [184], [185], [186], and [187]. These modifications may cause the AI system to misclassify objects, which may therefore cause the AV to act in a potentially hazardous manner. Hence, these attacks jeopardize both the integrity and accessibility of AVs. The forthcoming sections elaborate more on this type of attack.

Unintentional risks include unforeseen/sudden malfunctions or failures brought on by biased algorithms, bad design, and internal quirks of AI and ML techniques. For example, an AV's AI systems are always at work to identify traffic signs and road markings, find moving objects and determine their speed, and plan the path. The decision-making process may be opaque due to complex model structures and mathematical operations that escape an easy straightforward interpretation. It also could be unsafe due to critical scenarios inadequately represented and outside of the training data that are fed to the model during the design phase or challenging reproducibility and verification that can convey a misleading message, among other things. These problems have an impact on the methods' dependability in real-world applications. A typical AV [188] is illustrated in Fig. 3.

The following paragraphs give an in-depth analysis of some of the security issues and vulnerabilities associated with the sensors, controls, and connection mechanisms in an AV.

1) Sensor Jamming or Spoofing Attacks: One could jam or blind AV sensors [189]. Hence, the attacker may tamper with the AI model, feed erroneous data into the algorithm, or purposefully give inadequate data, reducing the efficacy of automated decision-making. For instance, by directly reflecting light back at the scanner unit that has the same frequency as the laser reflecting on the target, one may show how the LiDAR sensor could be interfered with [190]. A similar attack is performed in [191], where a LiDAR sensor is compromised. Additionally, the vehicle's control unit is misled into thinking a big item is in front of the car, which makes it halt. Further, recent works have demonstrated the possibility of saturating LiDAR sensors [192]. In [193], the authors spoofed LiDAR sensors and their underlying ML-based perception method. An adversarial ML attack is demonstrated in Fig. 4, where spoofing is executed. In this adversarial ML attack, camera signals are re-transmitted to provide false information to the camera, thereby misleading it in target detection and, as a result, confusing the detection of the actual target and increasing the risk of collision.

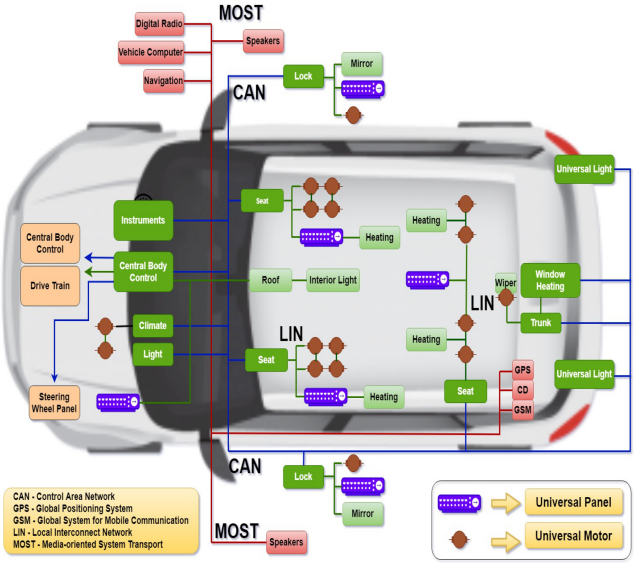

FIGURE 3. A simple structure of a typical autonomous vehicle.

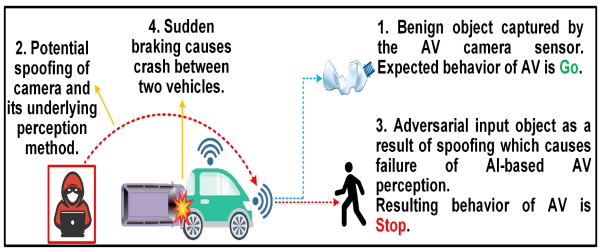

FIGURE 4. Illustration of a road scenario where the victim's camera is interfered with by a spoofing attack.

2) Denial of Service (DoS)/Distributed DoS (DDoS) Attacks: DoS attacks involve flooding a host with an enormous amount of information to overload it, effectively preventing it from receiving or processing information coming in from legitimate users. A variety of communication routes are available to AVs, all of which are intended to receive and transmit the data required for safe navigation and motoring. Vehicle-to-satellite, vehicle-to-vehicle (V2V), vehicle-to-internet, and other communication technologies are among them. Additionally, there is internal communication through the controller area network (CAN). Any of these communication channels can be broken, which can impair the car's ability to function properly and effectively render it blind to its surroundings. This adversely affects its

accessibility and impedes necessary operations for AD. DDoS attacks attempt to block these lines of communication. The authors of [194] studied DoS attacks against a platoon of intelligent vehicles. Another work [195] shows a GNSS DoS attack on an AV. Attackers can obstruct the camera's ability to recognize objects, roads, and warning signs by using DoS attacks. DoS attacks can potentially negatively impact the braking system, resulting in the automobile stopping abruptly or being unable to stop.

3) Manipulating Vehicle Communications: Hijacking and manipulating communication channels can affect AD operations. This enables an attacker to alter sent sensor readings or incorrectly decipher messages from the road infrastructure. As a result, a vehicle may act differently from what was planned or designed for it. The hacker might inject malicious messages and manipulate the communication between the two entities. This way, they might get unauthorized access to vehicle electronic control units (ECUs) or the roadside unit (RSU).
4) Information Disclosure: Given the large amount of private and sensitive data saved and used by vehicles for AD, including vital information on the AI components, a specific incentive emerges for prospective adversaries to obtain this kind of data and trigger a data breach.

V. ADVERSARIAL MACHINE LEARNING

The majority of the time, ML models are computer algorithms that are made to discover patterns in data. Algorithms, also referred to as "classifiers," can be taught how to react to various inputs with the assistance of people who provide "training data." Through repeated exposure to training data, these models are intended to make judgments that are ever more accurate over time. As of late, ML models have achieved human and even above-human accuracy in many computer vision tasks. The increasing accuracy of ML systems has led to their deployment in a veritable flood of real-world applications. However, ML models may be susceptible to manipulation, despite their many potential advantages.

An ML system may classify information using different parameters from those that a human can grasp intuitively, giving the impression that it is a "black box." Also, minor data adjustments through deliberate adversarial attacks can force a trained model to produce incorrect outputs and can have an outsized impact on the algorithm's decision. Cybersecurity researchers refer to this risk as "adversarial machine learning" as attackers can deceive AI-based systems into making incorrect predictions or assessments.

The term "adversary," which refers to the people or machines attempting to intrude on or corrupt a computer network illegally, is customary in computer science. Emerging in 2004 to deal with the robustness of anti-spam filters, adversarial ML has evolved to challenge the security of ML models.

Adversaries can use distinguished attack methods to disrupt an AI model, 1) during the training phase ("poisoning" or "contamination") or 2) after the classifier is trained ("evasion"). The first form of attack corrupts an ML model with false or misleading data (intentional feature perturbations) while training. On the other hand, evasion attacks try to trick an already trained model into making mistakes by feeding it deliberately created data. Further, the current adversarial attacks are mainly researched on IC tasks.

Formally, for a given ML classifier *(f)* and an initial categorized input image sample *(x)* with its class *(c)*, an adversary introduces a carefully crafted minor disturbance or perturbation *(ξ)* into the actual input image that results in an adversarial sample $(x^* = x + \xi)$ and makes the target model classify *(x*)* as *(c*)*, which is different from the targeted class *(c)* [196]. Mathematically, it can be formulated as shown in (1). Hence, the integrity of the ML/DL model is compromised by adding a little perturbation to the actual input [197].

$$x^* = x + argmin\{\| \xi \|: f(x+\xi) = c\}. \tag{1}$$

An attacker uses manipulated training samples or wrongly labeled data to launch a poisoning attack on a classifier. As a result, the ML-based system will now make decisions that are oblique or incorrect. An adversary must have some degree of influence over training data in order to conduct poisoning attacks. There are multiple ways to manipulate the target model using a poisoning attack, such as logic corruption, data manipulation, data injection, or transfer learning.

A. REVIEW OF EXISTING ADVERSARIAL ML ATTACKS

Using a spoofing attack to submit a bogus biometric feature to a biometric authentication system (BAS) is a paradigmatic example of an attack against the ML systems used for pattern recognition in cybersecurity [198] and [199]. In [200], network packets from malicious traffic are altered to avoid detection by intrusion detection systems, and in [201], spam emails' content is altered (e.g., by distorting widely used spam words) to make it through spam filters. Similarly, malware manipulation is used to get around malware detection based on ML, and face recognition systems are deceived in [202] and [203]. Additionally, research is being done on how to defend against attacks on supervised learning models, such as those that target regression techniques [204] and SVM [202]. Moreover, the weaknesses of unsupervised learning models have been investigated, looking at potential clustering method attacks.

This research topic has gained a lot of attention recently due to the increased incorporation of DL approaches in many important applications. The authors of [205] first demonstrated that existing DNNs are susceptible to malicious perturbations. The suggested method was a gradient-based attack where adversarial instances with the lowest distance were created to deceive the image classifiers. In [206], the researchers used pictures collected by a cell phone camera for the development of adversarial examples and demonstrated how vulnerable ML/DL systems are in practical situations. Similar research found that 10 cutting-edge DNNs were susceptible to basic geometric transformations like translation, rotation, and blurring. The work of [207] proposes a neural network trojan attack that alters the neurons of the trained model rather than

interfering with the training procedure. Recently, RL models have been probed concerning vulnerabilities because of their dependency on DL models. The research community is always coming up with new attacks, such as those that target real-time video classification systems or RNNs. Similarly, some adversarial attack examples have been explored for computer vision techniques that distinguish white-box attacks, black-box attacks, and grey-box attacks. A perturbation makes the model misclassify the resulting perturbed image in these attacks.

The techniques proposed most to perform adversarial attacks include projected gradient descent (PGD), fast gradient sign method (FGSM), iterative targeted FGSM [196], basic iteration method (BIM), Jacobian-based saliency map (JSM), Carlini & Wagner (C&W) attacks, DeepFool attack, one pixel attack, Houdini attack, and zeroth order optimization (ZOO) attack. Likewise, different attack strategies have been found to produce adversarial cases for data produced by the sensors prevalent in AVs. These include attacks on 3D point clouds outputted by LiDARs, radars, or ultrasonic sensors. These attacks involve the attacker's ability to update the inputs. However, the perturbations or the poisoned data may be too subtle or imperceptible for humans. Further, by modifying or fabricating things with particular properties that are misclassified by an ML model trained to detect them after being acquired by a camera, these attacks could be applied to the real world. Due to the lack of sensitivity of adversarial perturbations when they are subject to minute changes in the physical environment, generating successful physical adversarial attacks is incredibly challenging. One example of physical attack techniques is the expectation-over-transformation (EOT) attack.

VI. AI-BASED ADVERSARIAL ATTACKS AGAINST AUTONOMOUS VEHICLES

In addition to playing a crucial role in vehicle-to-infrastructure (V2I), V2V, vehicle-to-grid (V2G), vehicle-to-cloud (V2C), and V2X communications, ML and DL algorithms also act as core elements for performing many critical tasks in AVs. For instance, they provide deeply ingrained information for the decision-making process within the vehicle's components. The currently available AVs are not resistant to unforeseen hostile circumstances. There have been a few cases of documented life-threatening injuries or fatalities brought on by AI-based AV system faults or malfunctions when DNNs running the AV mistakenly produced adversarial samples. To substantiate, an AV crashed during the Hyundai competition in 2014 because of the sensors' failure to detect road signs, lane markers, and pedestrians due to rain [208]. Another accident was reported in 2016, when one of the pioneers in the US market, Tesla Autopilot, failed to handle the image contrast, causing a severe crash and the driver's death [209]. Also, due to a DNN-based system fault in 2018, an accident involving Uber's self-driving vehicle claimed the life of a pedestrian.

The literature on adversarial attacks on AI in semi-autonomous cars has grown significantly in recent years. The authors of [210] employed FGSM and JSM attack techniques to create false traffic signs in order to defeat DNN-based traffic sign detection systems and to draw attention to the issue of false examples in AD. The work of [211] developed a real-world adversarial ML strategy that modifies traffic signs and logos using adversarial perturbations while preserving the signs' visual appearance. The researchers of [212] targeted the ML-based TSR functionalities of an AV by performing an evasion attack, which deceived an image classifier corresponding to a front-facing camera. Further, a lenticular printing (LP) attack was also implemented, where the camera height is exploited to deceive the AV's sign recognition system by fabricating the appearance of fake traffic signs in the real world. With the capacity to create perturbations specifically targeted to speed-limit traffic signs, this application is enhanced to deceive a commercial car perception system in real-world driving situations in [222]. The TSR system of the car moving around the track noticed that the attack had caused fake and real signs to be placed all around it. Results demonstrated that the misclassification of the altered indicators led to certain unanticipated actions in the car. In a different study [213] that focused on the well-known Mobileye external ADAS, researchers used drone projections of fake traffic signals to determine how environmental changes—such as those related to projection speed, diameter, color, and ambient light—affected the success of an attack.

In another example, the authors demonstrated adversarial evasion attacks on an AV's steering angle predicting systems, adapting the C&W attack method [214]. The auto wipers of a Tesla car were activated by a research team from Tencent Keen Security Lab by projecting noise onto an electronic display that was placed in front of the car [223]. This tricked the system's visual sensor. Additionally, they looked at whether the perception system might miss a traffic lane after applying an intensive blur to it and whether false lanes could be created by applying certain stickers to the road. Another hack tricked Tesla cars into accelerating much beyond the posted speed limit [224]. The system anticipated a speed limit of 85 mph (about 137 km/h) by significantly extending with black tape the middle line in the number three on a 35 mph (about 56 km/h) speed sign. Modern DNN-based schemes like Mask R-CNN [225] and YOLO [226] are employed in OD, another crucial component of AVs' perception modules. By simulating how a simulator would cover a car in camouflage, the authors in [227] presented a camouflaged physical world adversarial assault. Next, it used a local search for the best camouflage to minimize the approximate detection score. Image-based OD systems were effectively tricked by the proposed adversarial approach. The research of [228] developed a different physical world adversarial example generation approach for OD, keeping a disturbed "Stop" sign hidden from cutting-edge object detectors like Mask R-CNN and YOLO. The authors of [229] presented DeepBillboard, a methodical approach for creating hostile billboard advertisements that would cause the AV's steering angle to malfunction. The intended adversarial billboard caused a 26.44° error in the average steering angle. Other works include overflow and class

TABLE 3. Distribution of adversarial attacks on autonomous driving

Distribution of Adversarial Attacks against Autonomous Driving				
Attack Category	**Authors**	**Year**	**AI-Based Attack Approach and Explanation**	**Reference**
Road Sign Recognition	Aung et al.	2017	CNN-based fast gradient sign and Jacobian-based saliency map methods are used to successfully generate a black-box attack on the road signs	[210]
Traffic Sign Detection	Sitawarin et al.	2018	A novel CNN-based sign embedding attack is introduced to modify innocuous signs, e.g., ad signs, drawings, graffiti, logos and custom road signs	[211]
Traffic Sign Recognition	Sitawarin et al.	2018	Out-of-distribution and lenticular printing attacks are launched to create toxic signs and fool the sign recognition system of the AV	[212]
Traffic Sign Recognition	Dudi et al.	2019	Drone-projected deceptive traffic signs are injected onto Mobileye, which controls the targeted AV	[213]
Steering Angle Prediction	Chernikova et al.	2019	C&W evasion attack is used to spoof the images sent by a camera, which are misclassified by the DNN-based steering angle controller	[214]
Traffic Sign Recognition	Wenbo et al.	2020	Particle optimization-based evasion and poisoning attacks are launched to CNN-based TSR system	[215]
Object Detection	Tong et al.	2020	Mosaic-like adversarial textures are drawn on other vehicles using an enlarged-and-repeated process and a discrete searching method to attack the vehicle detection models	[216]
Traffic Sign Recognition	Li et al.	2021	Adaptive square attack is used to generate perturbations for traffic sign images	[184]
Road Sign Recognition	Yang et al.	2021	Targeted attention attack is launched to intrude a DNN-based road sign recognition system images	[217]
Traffic Sign Recognition	Ye et al.	2021	Patch-based attack is conducted on three DNN-based traffic sign classifiers	[218]
Image Recognition	Ghosh et al.	2022	A differential evolution-based algorithm called DEceit is used to construct effective universal pixel-restricted perturbations for CNN-based image recognition models	[219]
Image Recognition	Patel et al.	2022	An adversarial attack is performed by installing a billboard that displays videos on the roadside to incoming DNN controlled vehicles so that the vehicle tracks an adversary customized trajectory	[220]
Traffic Sign Recognition	Chi et al.	2023	Multiple dual or triple attention patterns of white-box models are collected to generate adversarial perturbations for public attention attacks on traffic sign recognition system	[221]

spoofing adversarial attacks, which are implemented on the YOLOv5 frameworkto perform TSR. In an overflow attack, the TSR system detects more than 100 indicators in contrast to the two signs in the scene because of the magnified intensity of the disturbance introduced to each image pixel, while the sticker-like disturbance on the sign causes the model to misclassify the "Keep Right" sign as "Priority Road" during the class spoofing attack. By developing a black-box adversarial attack on images of traffic signs, the work of [20] exposes the weaknesses of an AV. Also, the authors suggested a "multi-gradient" attack on a DNN model for the perception of traffic scenes. A compilation of recent adversarial attacks on AVs is shown in Table 3.

VII. CYBERSECURITY OF AUTOMOTIVE VEHICLES

An increase in electronic components in a vehicle corresponds to a growth in the number of attack vectors through which an attacker might endeavor to get access to the vehicle's information and data or even modify its operations. Automobile manufacturers strive to produce AVs that follow a security cycle of design and development, which involves planning, manufacturing, and monitoring software and hardware throughout the vehicle's lifespan to mitigate cybersecurity threats. Certain automakers' mechanisms to deal with cybersecurity issues are diverse and numerous, including assessing threat data, sharing them with external partners, and designing and pushing out security upgrades to vehicles. Comprehensive cybersecurity techniques are required to deal with an increasingly complex cyber-threat scenario (e.g., interference related to driving securely, manipulation, and fraud), which is becoming more prevalent.

AV safety is highly influenced by the integrity of signal transmissions, which implies that signals from vehicles usually are acted upon only if they are authentic and transmitted and received correctly. The availability of secure vehicle functionality is the primary aim of safety, which frequently necessitates the design of a system that is both efficient and fail-safe (i.e., redundant). Therefore, an emphasis on the confidentiality, integrity, and availability (CIA) of a system or information is essential for cybersecurity efforts. As a result, cybersecurity evaluates whether a system may be controlled in a way that compromises these features. Overall, technology has evolved to the point where vehicles cannot maintain a safe condition unless they also operate correctly in a secure way. Hence, cybersecurity concepts and practices are necessary during the production development processes to guarantee

that attackers do not obtain arbitrary control over a vehicle's driving systems [230].

A. AUTOMOTIVE CYBERSECURITY STANDARDS AND REGULATIONS

Since various data and AI drive the decision-making processes of an AV, system malfunction and cybersecurity have turned out to be the most critical aspects of determining safety and security. AV cybersecurity comprises functional security and driving automation system (DAS) security. Although international standards ISO 26262, SAE J3061, and ISO 21434 provide guidelines for the functional safety and functional security of conventional road vehicles (onboard electrical and electronic systems), respectively [231], these standards are not created for AV-specific functionalities. For DAS safety, some recent standards, e.g., UL4600 [38] and SOTIF [34], have been developed. Although there are yet no AV-specific cybersecurity regulations, the UNECE WP.29 cybersecurity and cybersecurity management systems (CSMS) regulation [232] requires vehicle approval authority to ensure a holistic analysis encompassing ISO 26262-2018, ISO/PAS 21448, and ISO/SAE 21434 to make sure that every stage of the automotive supply chain is centered on cybersecurity. This standard aims to increase ingrained cybersecurity measures from vehicle original equipment manufacturers (OEMs), component and software suppliers, and mobility services. It puts the onus of cybersecurity on OEMs to incorporate the best cybersecurity practices into the design of vehicles. Alternatively said, OEMs must have a comprehensive strategy in place to efficiently monitor, detect, and react to cyber breaches and security vulnerabilities. Companies must be obliged to disclose recurring reports on cyber threats and attacks that have been discovered. It was formally adopted in the United Nations on June 25, 2020, and 50 OEMs worldwide are meant to adhere to this regulation and implement changes within their cybersecurity processes. The WP.29 CSMS legislation stands out for its pragmatic approach to vehicular cybersecurity, which includes specific examples of threats and mitigations, as well as its comprehensive approach, which considers process and governance, IT, and product and OT perspectives. However, this law makes sure that the risk of a cyber-attack is kept to a minimum but does not guarantee that automobiles cannot be compromised. Also, it fails to list all possible risks and mitigations.

B. ADVERSARIAL DEFENSE STRATEGIES

As stated above, ML approaches, notwithstanding their excellent performance, display marked susceptibility to carefully crafted adversarial cases. The overall vision is to develop defense techniques capable of making AVs more resilient to adversarial attacks and therefore to satisfy more stringent system safety and performance requirements. In this section, a synopsis of approaches for developing robust ML solutions to enhance vehicle performance and improve the security and reliability of AVs is drafted.

Many methodologies have been demonstrated in the past to defend against adversarial attacks, roughly categorized as proactive and reactive defenses. Proactive defenses attempt to strengthen a neural network's resistance toward adversarial examples in advance of an attack. In contrast, reactive defenses aim at detecting adversarial input observations or examples after the neural network models are trained. Alternatively, these techniques can also be broadly categorized into three groups, 1) manipulating data, 2) introducing auxiliary models, and 3) altering models.

The techniques that take advantage of proactive defenses mostly involve modifying either the test data or the training data. Widely used approaches that utilize such methods are adversarial re-training, defensive distillation, classifier robustifying, features masking, and gradient regularization.

In some of the works, the target model is either re-trained using the dataset with adversarial examples [234] or added to with regularization components [248]. In terms of making DNNs resistant to adversarial attacks, [234] and [249] originally suggested training with adversarial examples. By including more adversarial instances in the training set, they improved the model's learning. Additionally, it was demonstrated [234] that adversarial training could offer DNNs improved regularization. Furthermore, the authors in [26] introduced defensive distillation when training DNNs. It increases the magnitude of input features to create adversarial samples to harden a network. In another work [250], adversarial pixel masking (APM), a type of feature masking, is used to remove adversarial patches in images so that the distribution shift can be mitigated in pixel space. The most delicate input features, which are more vulnerable to adversarial perturbations, have to be hidden by the masking layer. Input gradient regularization was employed as a defensive tactic in the work found in [238]. The authors suppressed the variance in the output caused by fluctuations in the input by using differentiable DNN models. Because of this, adversarial instances with minor changes were unlikely to change the response of deep models, but doing so doubles the complexity of training the models.

Widely used approaches that utilize reactive defense methods include input reconstruction, network verification, adversarial detection, network distillation, and others. The idea of input reconstruction is to discard the inconsistent data samples and change them into legitimate equivalents. This transformation is done so that there are no hostile samples to influence the predictions of the DNN models. The authors in [233] developed a technique named deep contractive autoencoder (DCA) for robustifying the DNN model. A denoising autoencoder was programmed to effectively eliminate malicious adversarial perturbations. In addition, the procedure adopted to defend against adversarial attacks was network distillation. The authors in [235] introduced another reactive technique, feature squeezing, to harden DNN models. It shrinks the search space available to an adversary by combining samples. This study looked into two aspects of feature compression, 1) smoothing the spatial domain and, 2) lowering the color bit depth of each pixel. Last but not least, the network verification approach authenticates the DNN's attributes if an input sample conforms with or infringes on a specific trait

TABLE 4. State-of-the-art adversarial defense strategies

Summary of State-of-the-Art Adversarial Defense Approaches				
Adversarial Defense Strategy	**Authors**	**Year**	**Adversarial Perturbations**	**Reference**
Adversarial examples cleaning using denoising autoencoders (DAES)	Gu et al.	2014	Local perturbations, for instance, additive Gaussian noise	[233]
Augmented adversarial examples into the training set	Goodfellow et al.	2014	Fast Gradient Sign Method (FGSM)	[234]
Reduced the feature space available to an adversary	Xu et al.	2017	Evaluated different state-of-the-art perturbation generation methods	[235]
Proposed DeepCloak that removes unnecessary features in the model	Gao et al.	2017	Perturbations are generated using FGSM	[236]
Proposed PixelDefend to clean adversarial examples by moving them back to the manifold of original training data	Song et al.	2017	Used five state-of-the-art adversarial attacks	[237]
Trained the model with input gradient regularization for defending adversarial attacks	Ross et al.	2017	Evaluated three famous attacks, i.e., FGSM, TGSM, and JSMA	[238]
Constructed adversarially robust features using spectral property of the dataset	Garg et al.	2018	L2 Perturbations	[239]
Used wavelet-based denoising method to clean natural and adversarial noise	Prakash et al.	2018	Generated perturbations using pixel deflection	[240]
Formulated a robust optimization problem using convex outer approximation for detection of adversarial examples	Wong et al.	2018	FGSM and gradient descent-based methods	[241]
Used generative modelling using variational autoencoder (VAE)	Schott et al.	2019	Applied score-based, decision-based, transfer-based, and gradient-based attacks	[242]
Devised a stereo-regularizer to guide the model to learn the implicit relationship between the left and right images of the stereo-vision system	Sun et al.	2020	Evaluated FGSM and PGD attacks	[243]
Developed a GAN-based defense algorithm to determine the reconstructed images	Laykaviriyakul et al.	2022	Generated adversarial images using FGSM, iFGSM, PGD, and CW attacks	[244]
Designed mitigation strategies, e.g., data augmentation, train-time trajectory smoothing, and test-time detection and trajectory smoothing	Zhang et al.	2022	Generated adversarial trajectories using PGD and PSO-based attacks	[245]
Used a combination of compressive sensing with generative neural networks	Wang et al.	2022	Generated adversarial examples using CW-L2, FGSM, and sticker attacks	[246]
Proposed generative modelling using autoencoder and compressive memory module	Shibly et al.	2023	Evaluated FGSM and AdvGAN-based attacks	[247]

or characteristic since that might block new, unanticipated adversarial disruptions. This technique is exploited in [251] to handle the rectified linear unit (ReLU) activation function, which is a crucial element in many modern neural networks. In adversarial detection strategy [252] and [253], the authors trained a binary classifier to ascertain if an input is valid or hostile. To instantiate, in [252], a SafetyNet architecture is used for the SceneProof application, which can detect whether the captured image is a picture of a benign object or of an adversarial one. SceneProof is applied to images captured with depth maps (RGBD images), checking if a pair of image and depth maps is consistent. In a related study [254], scientists trained a DNN model while integrating an outlier class; the model subsequently recognized adversarial cases by categorizing them as outliers.

Table 4 presents an overview of existing adversarial defense strategies used in the literature.

Although the majority of the defenses have tested their effectiveness only on IC tasks, their insights can be applied to other AD tasks when taking into account similar methods for enhancing model robustness or pre-processing model inputs that are not limited just to IC.

VIII. CONCLUSION

In order to help human drivers in specific situations, such as preventing lane drift or assisting the driver in coming to a complete halt in time to avoid a potential AV crash, the thriving automated vehicles currently come equipped with ADAS safety capabilities. The future L4 and L5 vehicles, on the other hand, will be equipped with advanced ADS functionality, which relies solely on sophisticated AI/ML algorithms for sensor processing, sensor fusion, scene creation, and motion planning, hence allowing the vehicle to sense its environment and make informed decisions. This article has therefore outlined the importance of ML and DL technologies in AVs in, for instance, object classification and detection, SS, etc. However, recent investigations and groundwork on adversarial attacks elicit suspicions about AVs' security and potency. It

is inferred that the uptake of these advanced AI technologies has introduced a range of vulnerabilities in the AVs featuring them. This article presented a detailed investigation of adversarial attacks on the automated driving ecosystem. In addition, a survey of adversarial defense models for improving resistance against adversarial attacks on ML components in AVs has been discussed. In order to strengthen resilience and secure the ML and training data for AVs, the authors have especially addressed the significance of generic defense techniques. Finally, the authors expect that the academic community will use this study to help discover any loopholes and withholdings in the existing studies on adversarial attacks and defense strategies for ADSs.

REFERENCES

[1] S. Shafer, A. Stentz, and C. Thorpe, "An architecture for sensor fusion in a mobile robot," in *Proc. IEEE Int. Conf. Robot. Automat.*, 1986, vol. 3, pp. 2002–2011.

[2] M. Girdhar, J. Hong, H. Lee, and T.-J. Song, "Hidden Markov models-based anomaly correlations for the cyber-physical security of EV charging stations," *IEEE Trans. Smart Grid*, vol. 13, no. 5, pp. 3903–3914, Sep. 2022.

[3] Q. Memon, M. Ahmed, S. Ali, A. R. Memon, and W. Shah, "Self-driving and driver relaxing vehicle," in *Proc. IEEE 2nd Int. Conf. Robot. Artif. Intell.*, 2016, pp. 170–174.

[4] S. Ma, H. Jiang, M. Han, J. Xie, and C. Li, "Research on automatic parking systems based on parking scene recognition," *IEEE Access*, vol. 5, pp. 21901–21917, 2017.

[5] M. Dikmen and C. Burns, "Trust in autonomous vehicles: The case of Tesla Autopilot and Summon," in *Proc. IEEE Int. Conf. Syst., Man, Cybern.*, 2017, pp. 1093–1098.

[6] P. M. Baggenstoss, "New restricted Boltzmann machines and deep belief networks for audio classification," in *Proc. IEEE 14th ITG Conf. Speech Commun.*, 2021, pp. 1–5.

[7] Y. Zhu and W. Q. Yan, "Traffic sign recognition based on deep learning," *Multimedia Tools Appl.*, vol. 81, pp. 17779–17791, 2022.

[8] K. Muhammad, A. Ullah, J. Lloret, J. D. Ser, and V. H. C. de Albuquerque, "Deep learning for safe autonomous driving: Current challenges and future directions," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 7, pp. 4316–4336, Jul. 2021.

[9] J. Raiyn, "Data and cyber security in autonomous vehicle networks," *Transport Telecommun.*, vol. 19, no. 4, pp. 325–334, 2018.

[10] M. Uzair, "Who is liable when a driverless car crashes?," *World Electric Veh. J.*, vol. 12, no. 2, 2021, Art. no. 62. [Online]. Available: https://www.mdpi.com/2032-6653/12/2/62

[11] P. Penmetsa, P. Sheinidashtegol, A. Musaev, E. K. Adanu, and M. Hudnall, "Effects of the autonomous vehicle crashes on public perception of the technology," *IATSS Res.*, vol. 45, no. 4, pp. 485–492, 2021. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0386111221000224

[12] G. Costantino and I. Matteucci, "Reversing Kia motors head unit to discover and exploit software vulnerabilities," *J. Comput. Virol. Hacking Techn.*,vol. 19, pp. 33–49, 2022.

[13] I. Nastjuk, B. Herrenkind, M. Marrone, A. B. Brendel, and L. M. Kolbe, "What drives the acceptance of autonomous driving? An investigation of acceptance factors from an end-user's perspective," *Technological Forecasting Social Change*, vol. 161, 2020, Art. no. 120319. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0040162520311458

[14] K. Ren, T. Zheng, Z. Qin, and X. Liu, "Adversarial attacks and defenses in deep learning," *Engineering*, vol. 6, no. 3, pp. 346–360, 2020. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S209580991930503X

[15] A. Kloukiniotis, A. Papandreou, A. Lalos, P. Kapsalas, D.-V. Nguyen, and K. Moustakas, "Countering adversarial attacks on autonomous vehicles using denoising techniques: A review," *IEEE Open J. Intell. Transp. Syst.*, vol. 3, pp. 61–80, 2022.

[16] A. Qayyum, M. Usama, J. Qadir, and A. Al-Fuqaha, "Securing connected & autonomous vehicles: Challenges posed by adversarial machine learning and the way forward," *IEEE Commun. Surv. Tut.*, vol. 22, no. 2, pp. 998–1026, 2020.

[17] Y. Xiao, C.-M. Pun, and B. Liu, "Fooling deep neural detection networks with adaptive object-oriented adversarial perturbation," *Pattern Recognit.*, vol. 115, 2021, Art. no. 107903. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S003132032100090X

[18] P. Sharma, D. Austin, and H. Liu, "Attacks on machine learning: Adversarial examples in connected and autonomous vehicles," in *Proc. IEEE Int. Symp. Technol. Homeland Secur.*, 2019, pp. 1–7.

[19] Z. Xiong, H. Xu, W. Li, and Z. Cai, "Multi-source adversarial sample attack on autonomous vehicles," *IEEE Trans. Veh. Technol.*, vol. 70, no. 3, pp. 2822–2835, Mar. 2021.

[20] K. N. Kumar, C. Vishnu, R. Mitra, and C. K. Mohan, "Black-box adversarial attacks in autonomous vehicle technology," in *Proc. IEEE Appl. Imagery Pattern Recognit. Workshop*, 2020, pp. 1–7.

[21] J. Zhang, Y. Lou, J. Wang, K. Wu, K. Lu, and X. Jia, "Evaluating adversarial attacks on driving safety in vision-based autonomous vehicles," *IEEE Internet Things J.*, vol. 9, no. 5, pp. 3443–3456, Mar. 2022.

[22] X. Yuan, P. He, Q. Zhu, and X. Li, "Adversarial examples: Attacks and defenses for deep learning," *IEEE Trans. Neural Netw. Learn. Syst.*, vol. 30, no. 9, pp. 2805–2824, Sep. 2019.

[23] I. Vaccari, A. Carlevaro, S. Narteni, E. Cambiaso, and M. Mongelli, "explainable and reliable against adversarial machine learning in data analytics," *IEEE Access*, vol. 10, pp. 83949–83970, 2022.

[24] O. Poursaeed, I. Katsman, B. Gao, and S. Belongie, "Generative adversarial perturbations," in *Proc. IEEE/CVF Conf. Comput. Vis. Pattern Recognit.*, 2018, pp. 4422–4431.

[25] S.-M. Moosavi-Dezfooli, A. Fawzi, and P. Frossard, "Deepfool: A simple and accurate method to fool deep neural networks," in *Proc. IEEE Conf. Comput. Vis. Pattern Recognit.*, 2016, pp. 2574–2582.

[26] N. Papernot, P. McDaniel, X. Wu, S. Jha, and A. Swami, "Distillation as a defense to adversarial perturbations against deep neural networks," in *Proc. IEEE Symp. Secur. Privacy*, 2016, pp. 582–597.

[27] X. Chen, J. Weng, X. Deng, W. Luo, Y. Lan, and Q. Tian, "Feature distillation in deep attention network against adversarial examples," *IEEE Trans. Neural Netw. Learn. Syst.*, to be published, doi: 10.1109/TNNLS.2021.3113342.

[28] J. Shuttleworth, "SAE and ISO refine the levels of driving automation," *SAE Int.*, 2021.

[29] "SAE j3016 taxonomy and definitions for terms related to driving automation systems for on-road motor vehicles," SAE, Geneva, Carouge, Switzerland, Tech. Rep., Apr. 2021, doi: 10.4271/J3016_202104.

[30] M. Girdhar, Y. You, T.-J. Song, S. Ghosh, and J. Hong, "Post-accident cyberattack event analysis for connected and automated vehicles," *IEEE Access*, vol. 10, pp. 83176–83194, 2022.

[31] United Nations Economic Commission for Europe (UNECE), "All you need to know about automated vehicles," UNECE, Geneva, Switzerland, Tech. Rep., 2021. [Online]. Available: https://unece.org/sites/default/files/2022-01/Brochure%20Automated%20Vehicles.pdf

[32] National Highway Traffic Safety Administration (NHTSA) and US Department of Transportation (DOT), "Framework for automated driving system safety," Tech. Rep., 2020.

[33] California Department of Motor Vehicle, "Californial autonomous driving system safety," Tech. Rep., 2020.

[34] "ISO/PAS 21448:2019, road vehicles – safety of the intended functionality," Int. Org. Standardization, Geneva, CH, Tech. Rep., Jan. 2019.

[35] "ISO/DIS 34501, road vehicles – terms and definitions of test scenarios for automated driving systems," Int. Org. Standardization, Geneva, CH, Tech. Rep.

[36] "ISO/DIS 34502, road vehicles – scenario-based safety evaluation framework for automated driving systems," Int. Org. Standardization, Geneva, CH, Tech. Rep.

[37] "ISO/DIS 34503, road vehicles – taxonomy for operational design domain for automated driving systems," Int. Org. Standardization, Geneva, CH, Tech. Rep.

[38] "UL4600, evaluation of autonomous products," Underwriters Lab. (UL) Standards, Geneva, CH, Tech. Rep.

[39] D. Basserman, "ASAM publishes concept for a new autonomous vehicle safety standard enabling testing for road readiness," *Assoc. Standardization Automat. Measuring Syst.*, 2022.

[40] R. M. Gandia et al., "Autonomous vehicles: Scientometric and bibliometric review," *Transport Rev.*, vol. 39, no. 1, pp. 9–28, 2019. [Online]. Available: https://doi.org/10.1080/01441647.2018.1518937

[41] A. Hamoud, "Understanding operational design domain to create informed safety in autonomous vehicles deployment," Claytex Tech. Blog, 2021.

[42] R. McAllister et al., "Concrete problems for autonomous vehicle safety: Advantages of Bayesian deep learning," in *Proc. 26th Int. Joint Conf. Artif. Intell.*, 2017, pp. 4745–4753.

[43] G. Chen, H. Cao, J. Conradt, H. Tang, F. Rohrbein, and A. Knoll, "Event-based neuromorphic vision for autonomous driving: A paradigm shift for bio-inspired visual sensing and perception," *IEEE Signal Process. Mag.*, vol. 37, no. 4, pp. 34–49, Jul. 2020.

[44] S.-C. Liu, B. Rueckauer, E. Ceolini, A. Huber, and T. Delbruck, "Event-driven sensing for efficient perception: Vision and audition algorithms," *IEEE Signal Process. Mag.*, vol. 36, no. 6, pp. 29–37, Nov. 2019.

[45] T. Serrano-Gotarredona and B. Linares-Barranco, "A 128 × 128 1.5% contrast sensitivity 0.9% fpn 3 μs latency 4 mW asynchronous frame-free dynamic vision sensor using transimpedance preamplifiers," *IEEE J. Solid-State Circuits*, vol. 48, no. 3, pp. 827–838, Mar. 2013.

[46] H.-H. Jebamikyous and R. Kashef, "Autonomous vehicles perception (AVP) using deep learning: Modeling, assessment, and challenges," *IEEE Access*, vol. 10, pp. 10523–10535, 2022.

[47] C. Yan, H. Xie, D. Yang, J. Yin, Y. Zhang, and Q. Dai, "Supervised hash coding with deep neural network for environment perception of intelligent vehicles," *IEEE Trans. Intell. Transp. Syst.*, vol. 19, no. 1, pp. 284–295, Jan. 2018.

[48] C. Chen, A. Seff, A. Kornhauser, and J. Xiao, "Deepdriving: Learning affordance for direct perception in autonomous driving," in *Proc. IEEE Int. Conf. Comput. Vis.*, 2015, pp. 2722–2730.

[49] S. Ramos, S. Gehrig, P. Pinggera, U. Franke, and C. Rother, "Detecting unexpected obstacles for self-driving cars: Fusing deep learning and geometric modeling," in *Proc. IEEE Intell. Veh. Symp.*, 2017, pp. 1025–1032.

[50] R. O. Chavez-Garcia and O. Aycard, "Multiple sensor fusion and classification for moving object detection and tracking," *IEEE Trans. Intell. Transp. Syst.*, vol. 17, no. 2, pp. 525–534, Feb. 2016.

[51] Y. Zeng, X. Xu, D. Shen, Y. Fang, and Z. Xiao, "Traffic sign recognition using kernel extreme learning machines with deep perceptual features," *IEEE Trans. Intell. Transp. Syst.*, vol. 18, no. 6, pp. 1647–1653, Jun. 2017.

[52] R. Kavitha and S. Nivetha, "Pothole and object detection for an autonomous vehicle using yolo," in *Proc. IEEE 5th Int. Conf. Intell. Comput. Control Syst.*, 2021, pp. 1585–1589.

[53] G. Öztürk, R. Köker, O. Eldoğan, and D. Karayel, "Recognition of vehicles, pedestrians and traffic signs using convolutional neural networks," in *Proc. IEEE 4th Int. Symp. Multidisciplinary Stud. Innov. Technol.*, 2020, pp. 1–8.

[54] V. John, K. Yoneda, B. Qi, Z. Liu, and S. Mita, "Traffic light recognition in varying illumination using deep learning and saliency map," in *Proc. IEEE 17th Int. Conf. Intell. Transp. Syst.*, 2014, pp. 2286–2291.

[55] S. Mozaffari, O. Y. Al-Jarrahand, M. Dianati, P. Jennings, and A. Mouzakitis, "Deep learning-based vehicle behaviour prediction for autonomous driving applications: A review," *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 1, pp. 33–47, Jan. 2022, doi: 10.1109/TITS.2020.3012034.

[56] W. Luo, B. Yang, and R. Urtasun, "Fast and furious: Real time end-to-end 3 d detection, tracking and motion forecasting with a single convolutional net," in *Proc. IEEE/CVF Conf. Comput. Vis. Pattern Recognit.*, 2018, pp. 3569–3577.

[57] L. Xin, P. Wang, C. Chan, J. Chen, S. E. Li, and B. Cheng, "Intention-aware long horizon trajectory prediction of surrounding vehicles using dual LSTM networks," in *Proc. IEEE 21st Int. Conf. Intell. Transp. Syst.*, 2018, pp. 1441–1446.

[58] S. Dai, L. Li, and Z. Li, "Modeling vehicle interactions via modified LSTM models for trajectory prediction," *IEEE Access*, vol. 7, pp. 38287–38296, 2019.

[59] D. Lee, Y. P. Kwon, S. McMains, and J. K. Hedrick, "Convolution neural network-based lane change intention prediction of surrounding vehicles for ACC," in *Proc. IEEE 20th Int. Conf. Intell. Transp. Syst.*, 2017, pp. 1–6.

[60] R. U. S. Casas and W. Luo, "Intentnet: Learning to predict intention from raw sensor data," *Proc. Mach, Learn. Res.*, vol. 87, pp. 947–956, 2018.

[61] Y. Hu, W. Zhan, and M. Tomizuka, "Probabilistic prediction of vehicle semantic intention and motion," in *Proc. IEEE Intell. Veh. Symp.*, 2018, pp. 307–313.

[62] N. Deo and M. M. Trivedi, "Convolutional social pooling for vehicle trajectory prediction," in *Proc. IEEE/CVF Conf. Comput. Vis. Pattern Recognit. Workshops*, 2018, pp. 1549–15498.

[63] F. Scarselli, M. Gori, A. C. Tsoi, M. Hagenbuchner, and G. Monfardini, "The graph neural network model," *IEEE Trans. Neural Netw.*, vol. 20, no. 1, pp. 61–80, Jan. 2009.

[64] F. Diehl, T. Brunner, M. T. Le, and A. Knoll, "Graph neural networks for modelling traffic participant interaction," in *Proc. IEEE Intell. Veh. Symp.*, 2019, pp. 695–701.

[65] Q. Mao, F. Hu, and Q. Hao, "Deep learning for intelligent wireless networks: A comprehensive survey," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 4, pp. 2595–2621, Fourthquarter 2018.

[66] S. Dai, Z. Li, L. Li, N. Zheng, and S. Wang, "A flexible and explainable vehicle motion prediction and inference framework combining semi-supervised AOG and ST-LSTM," *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 2, pp. 840–860, Feb. 2022.

[67] C. Katrakazas, M. Quddus, W. H. Chen, and L. Deka, "Real-time motion planning methods for autonomous on-road driving: State-of-the-art and future research directions," *Transp. Res. Part C: Emerg. Technol.*, vol. 60, pp. 416–442, 2015.

[68] A. Houenou, P. Bonnifait, V. Cherfaoui, and W. Yao, "Vehicle trajectory prediction based on motion model and maneuver recognition," in *Proc. IEEE/RSJ Int. Conf. Intell. Robots Syst.*, 2013, pp. 4363–4369.

[69] Y. Jeong and K. Yi, "Bidirectional long shot-term memory-based interactive motion prediction of cut-in vehicles in urban environments," *IEEE Access*, vol. 8, pp. 106183–106197, 2020.

[70] T. Li, "Modeling uncertainty in vehicle trajectory prediction in a mixed connected and autonomous vehicle environment using deep learning and kernel density estimation," in *Proc. 4th Annu. Symp. Transp. Informat.*, 2018.

[71] M. Morsali, E. Frisk, and J. Åslund, "Spatio-temporal planning in multi-vehicle scenarios for autonomous vehicle using support vector machines," *IEEE Trans. Intell. Veh.*, vol. 6, no. 4, pp. 611–621, Dec. 2021.

[72] S. Josef and A. Degani, "Deep reinforcement learning for safe local planning of a ground vehicle in unknown rough terrain," *IEEE Robot. Automat. Lett.*, vol. 5, no. 4, pp. 6748–6755, Oct. 2020.

[73] Y. Jeong, S. Kim, and K. Yi, "Surround vehicle motion prediction using LSTM-RNN for motion planning of autonomous vehicles at multi-lane turn intersections," *IEEE Open J. Intell. Transp. Syst.*, vol. 1, pp. 2–14, 2020.

[74] S. Aradi, "Survey of deep reinforcement learning for motion planning of autonomous vehicles," *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 2, pp. 740–759, Feb. 2022.

[75] Y. Yoon, C. Kim, J. Lee, and K. Yi, "Interaction-aware probabilistic trajectory prediction of cut-in vehicles using Gaussian process for proactive control of autonomous vehicles," *IEEE Access*, vol. 9, pp. 63440–63455, 2021.

[76] T.-M. Hsu, C.-H. Wang, H.-C. Hsu, C.-H. Chiang, and Y.-R. Chen, "Motion planning of autonomous vehicle for illegal parked vehicles at no parking area," in *Proc. IEEE Int. Autom. Control Conf.*, 2021, pp. 1–5.

[77] M. Bojarski et al., "End to end learning for self-driving cars," 2016.

[78] Z. Chen and X. Huang, "End-to-end learning for lane keeping of self-driving cars," in *Proc. IEEE Intell. Veh. Symp.*, 2017, pp. 1856–1860.

[79] S. Xiao, J. Huang, L. Xiao, Y. Jiao, Z. Wang, and X. Wang, "Research on driving decision of smart vehicles based on reinforcement learning," in *Proc. IEEE 4th Adv. Inf. Manage., Communicates, Electron. Automat. Control Conf.*, 2021, vol. 4, pp. 1466–1469.

[80] J. Liu, P. Hou, L. Mu, Y. Yu, and C. Huang, "Elements of effective deep reinforcement learning towards tactical driving decision making," 2018.

[81] Y. Zhang, P. Sun, Y. Yin, L. Lin, and X. Wang, "Human-like autonomous vehicle speed control by deep reinforcement learning with double Q-learning," in *Proc. IEEE Intell. Veh. Symp.*, 2018, pp. 1251–1256.

[82] Y. He, N. Zhao, and H. Yin, "Integrated networking, caching, and computing for connected vehicles: A deep reinforcement learning approach," *IEEE Trans. Veh. Technol.*, vol. 67, no. 1, pp. 44–55, Jan. 2018.

[83] Y. Lu, X. Xu, X. Zhang, L. Qian, and X. Zhou, "Hierarchical reinforcement learning for autonomous decision making and motion planning of intelligent vehicles," *IEEE Access*, vol. 8, pp. 209776–209789, 2020.

[84] A. Khanum, C.-Y. Lee, and C.-S. Yang, "End-to-end deep learning model for steering angle control of autonomous vehicles," in *Proc. IEEE Int. Symp. Comput., Consum. Control*, 2020, pp. 189–192.

[85] M. Smolyakov, A. Frolov, V. Volkov, and I. Stelmashchuk, "Self-driving car steering angle prediction based on deep neural network an example of carnd udacity simulator," in *Proc. IEEE 12th Int. Conf. Appl. Inf. Commun. Technol.*, 2018, pp. 1–5.
[86] S. Du, H. Guo, and A. Simpson, "Self-driving car steering angle prediction based on image recognition," 2019.
[87] X. Shi, Y. D. Wong, C. Chai, and M. Z.-F. Li, "An automated machine learning (AutoML) method of risk prediction for decision-making of autonomous vehicles," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 11, pp. 7145–7154, Nov. 2021.
[88] X. Xu, L. Zuo, X. Li, L. Qian, J. Ren, and Z. Sun, "A reinforcement learning approach to autonomous decision making of intelligent vehicles on highways," *IEEE Trans. Syst., Man, Cybern. Syst.*, vol. 50, no. 10, pp. 3884–3897, Oct. 2020.
[89] Y. Fu, C. Li, F. R. Yu, T. H. Luan, and Y. Zhang, "A decision-making strategy for vehicle autonomous braking in emergency via deep reinforcement learning," *IEEE Trans. Veh. Technol.*, vol. 69, no. 6, pp. 5876–5888, Jun. 2020.
[90] S. Mo, X. Pei, and Z. Chen, "Decision-making for oncoming traffic overtaking scenario using double DQN," in *Proc. IEEE 3rd Conf. Veh. Control Intell.*, 2019, pp. 1–4.
[91] L. Wei, L. Runge, and L. Xiaolei, "Traffic sign detection and recognition via transfer learning," in *Proc. IEEE Chin. Control Decis. Conf.*, 2018, pp. 5884–5887.
[92] X. Li, Z. Xie, X. Deng, Y. Wu, and Y. Pi, "Traffic sign detection based on improved faster R-CNN for autonomous driving," *J. Supercomputing*, vol. 78, pp. 7982–8002, 2022.
[93] S. Maldonado-Bascon, S. Lafuente-Arroyo, P. Gil-Jimenez, H. Gomez-Moreno, and F. Lopez-Ferreras, "Road-sign detection and recognition based on support vector machines," *IEEE Trans. Intell. Transp. Syst.*, vol. 8, no. 2, pp. 264–278, Jun. 2007.
[94] M. Shi, H. Wu, and H. Fleyeh, "Support vector machines for traffic signs recognition," in *Proc. IEEE Int. Joint Conf. Neural Netw. (IEEE World Congr. Comput. Intell.)*, 2008, pp. 3820–3827.
[95] C. G. Kiran, L. V. Prabhu, and K. Rajeev, "Traffic sign detection and pattern recognition using support vector machine," in *Proc. IEEE 7th Int. Conf. Adv. Pattern Recognit.*, 2009, pp. 87–90.
[96] J. A. Gómez and S. Bromberg, "Design and evaluation of a traffic sign recognition system based on support vector machines," in *Proc. IEEE 19th Symp. Image, Signal Process. Artif. Vis.*, 2014, pp. 1–5.
[97] F. Boi and L. Gagliardini, "A support vector machines network for traffic sign recognition," in *Proc. IEEE Int. Joint Conf. Neural Netw.*, 2011, pp. 2210–2216.
[98] S. Agrawal and R. K. Chaurasiya, "Automatic traffic sign detection and recognition using moment invariants and support vector machine," in *Proc. IEEE Int. Conf. Recent Innov. Signal Process. Embedded Syst.*, 2017, pp. 289–295.
[99] T. Guofeng, C. Huairong, L. Yong, and Z. Kai, "Traffic sign recognition based on SVM and convolutional neural network," in *Proc. IEEE 12th Conf. Ind. Electron. Appl.*, 2017, pp. 2066–2071.
[100] A. Kapoor, N. Nehra, and D. Deshwal, "Traffic signs recognition using CNN," in *Proc. IEEE Int. Conf. Ind. Electron. Res. Appl.*, 2021, pp. 1–4.
[101] R. Qian, Y. Yue, F. Coenen, and B. Zhang, "Traffic sign recognition with convolutional neural network based on max pooling positions," in *Proc. IEEE 12th Int. Conf. Natural Comput., Fuzzy Syst. Knowl. Discov.*, 2016, pp. 578–582.
[102] A. Vennelakanti, S. Shreya, R. Rajendran, D. Sarkar, D. Muddegowda, and P. Hanagal, "Traffic sign detection and recognition using a CNN ensemble," in *Proc. IEEE Int. Conf. Consum. Electron.*, 2019, pp. 1–4.
[103] Z. He, Z. Xiao, and Z. Yan, "Traffic sign recognition based on convolutional neural network model," in *Proc. IEEE Chin. Automat. Congr.*, 2020, pp. 155–158.
[104] J. Rezgui, A. Hbaieb, L. Chaari, and J. Maryland, "Traffic sign recognition using neural networks useful for autonomous vehicles," in *Proc. IEEE Int. Conf. Smart Appl., Commun. Netw.*, 2019, pp. 1–6.
[105] A. Kerim and M. Efe, "Recognition of traffic signs with artificial neural networks: A novel dataset and algorithm," in *Proc. IEEE Int. Conf. Artif. Intell. Inf. Commun.*, 2021, pp. 171–176.
[106] Z. Abedin, P. Dhar, M. K. Hossenand, and K. Deb, "Traffic sign detection and recognition using fuzzy segmentation approach and artificial neural network classifier respectively," in *Proc. IEEE Int. Conf. Elect., Comput. Commun. Eng.*, 2017, pp. 518–523.
[107] A. S. Alturki, "Traffic sign detection and recognition using adaptive threshold segmentation with fuzzy neural network classification," in *Proc. IEEE Int. Symp. Netw., Comput. Commun.*, 2018, pp. 1–7.
[108] M. Narayana and N. P. G. Bhavani, "Detection of traffic signs under various conditions using random forest algorithm comparison with KNN and SVM," in *Proc. IEEE Int. Conf. Bus. Anal. Technol. Secur.*, 2022, pp. 1–6.
[109] K. Pavani and P. Sriramya, "Comparison of KNN, ANN, CNN and YOLO algorithms for detecting the accurate traffic flow and build an intelligent transportation system," in *Proc. IEEE 2nd Int. Conf. Innov. Pract. Technol. Manage.*, 2022, vol. 2, pp. 628–633.
[110] D. S. Reddy and C. Joseph, "A access traffic sign detection tracking and recognition system for video frames using KNN algorithms," *Int. J. Innov. Technol. Exploring Eng.*, vol. 8, pp. 56–61, 2019.
[111] A. Santos, P. A. Abu, C. Oppus, and R. Reyes, "Traffic sign detection and recognition for assistive driving," in *Proc. IEEE Int. Symp. Multimedia Commun. Technol.*, 2019, pp. 1–6.
[112] L. Song and Z. Liu, "Color-based traffic sign detection," in *Proc. IEEE Int. Conf. Qual., Rel., Risk, Maintenance, Saf. Eng.*, 2012, pp. 353–357.
[113] M. Meuter, S. Müller-Schneiders, C. Nunny, S. Holdy, S. Goermery, and A. Kummerty, "Decision fusion and reasoning for traffic sign recognition," in *Proc. IEEE 13th Int. Conf. Intell. Transp. Syst.*, 2010, pp. 324–329.
[114] F. Zaklouta and B. Stanciulescu, "Real-time traffic-sign recognition using tree classifiers," *IEEE Trans. Intell. Transp. Syst.*, vol. 13, no. 4, pp. 1507–1514, Dec. 2012.
[115] R. S. Tomar, S. Verma, and G. S. Tomar, "SVM based trajectory predictions of lane changing vehicles," in *Proc. IEEE Int. Conf. Comput. Intell. Commun. Netw.*, 2011, pp. 716–721.
[116] A. A. Albousefi et al., "A support vector machine approach to unintentional vehicle lane departure prediction," in *Proc. IEEE Intell. Veh. Symp. Proc.*, 2014, pp. 299–303.
[117] Z. Huang, Y. Wu, and J. Liu, "Research on effects of pattern, amplitude and frequency of pulse steering torque warnings for lane departure," *Transp. Res. Part F: Traffic Psychol. Behav.*, vol. 31, pp. 67–76, 2015.
[118] R. Izquierdo, I. Parra, J. Muñoz-Bulnes, D. Fernández-Llorca, and M. A. Sotelo, "Vehicle trajectory and lane change prediction using ANN and SVM classifiers," in *Proc. IEEE 20th Int. Conf. Intell. Transp. Syst.*, 2017, pp. 1–6.
[119] H. J. A. Undit, M. F. A. Hassan, and Z. M. Zin, "Vision-based unmarked road detection with semantic segmentation using mask R-CNN for lane departure warning system," in *Proc. IEEE 4th Int. Symp. Agents, Multi-Agent Syst. Robot.*, 2021, pp. 1–6.
[120] H. Aravind, P. S, and K. I. Ramachandran, "Design and optimization of CNN for lane detection," in *Proc. IEEE 11th Int. Conf. Comput., Commun. Netw. Technol.*, 2020, pp. 1–6.
[121] D. Qiao, X. Wu, and T. Wang, "A lane recognition based on line-CNN network," in *Proc. IEEE Asia-Pacific Conf. Image Process., Electron. Comput.*, 2020, pp. 96–100.
[122] M. R. Islam, T. A. Siddique, M. I. H. Sakib, and S. Hossain, "A convolutional neural network for end to end structural prediction and lane detection for autonomous vehicle," in *Proc. IEEE 5th Int. Conf. Elect. Eng. Inf. Commun. Technol.*, 2021, pp. 1–6.
[123] S. H. Chung, D. J. Kim, J. S. Kim, and C. C. Chung, "Collision detection system for lane change on multi-lanes using convolution neural network," in *Proc. IEEE Intell. Veh. Symp.*, 2021, pp. 690–696.
[124] R. F. Olanrewaju, A. S. A. Fakhri, M. L. Sanni, and M. T. Ajala, "Robust, fast and accurate lane departure warning system using deep learning and mobilenets," in *Proc. IEEE 7th Int. Conf. Mechatronics Eng.*, 2019, pp. 1–6.
[125] F. Chao, S. Yu-Pei, and J. Ya-Jie, "Multi-lane detection based on deep convolutional neural network," *IEEE Access*, vol. 7, pp. 150833–150841, 2019.
[126] M. Narayana and N. P. G. Bhavani, "A lane detection system to assistant drivers for better driving using gradient decent algorithm comparison with KNN and SVM," in *Proc. IEEE Int. Conf. Bus. Anal. Technol. Secur.*, 2022, pp. 1–6.
[127] S. Yang, W. Wang, C. Lu, J. Gong, and J. Xi, "A time-efficient approach for decision-making style recognition in lane-changing behavior," *IEEE Trans. Human-Mach. Syst.*, vol. 49, no. 6, pp. 579–588, Dec. 2019.

[128] M. Hammami, N. B. Romdhane, and H. Ben-Abdallah, "An improved lane detection and tracking method for lane departure warning systems," *Int. J. Comput. Vis. Image Process.*, vol. 3, pp. 1–15, 2013.

[129] J. M. Ambarak, H. Ying, F. Syed, and D. Filev, "A neural network for predicting unintentional lane departures," in *Proc. IEEE Int. Conf. Ind. Technol.*, 2017, pp. 492–497.

[130] Z. Wei, C. Wang, P. Hao, and M. J. Barth, "Vision-based lane-changing behavior detection using deep residual neural network," in *Proc. IEEE Intell. Transp. Syst. Conf.*, 2019, pp. 3108–3113.

[131] M. Karthikeyan, S. Sathiamoorthy, and V. Muruganandam, "Lane keep assist system for an autonomous vehicle using support vector machine learning algorithm," in *Proc. Int. Conf. Innov. Data Commun. Technol. Appl.*, Berlin, Germany, 2020, pp. 101–108.

[132] H. Mandalia and D. Salvucci, "Using support vector machines for lane-change detection," in *Proc. Hum. Factors Ergonom. Soc. Annu. Meeting*, 2005, vol. 49, pp. 1965–1969.

[133] Q. Wang, W. Zhuang, L. Wang, and F. Ju, "Lane keeping assist for an autonomous vehicle based on deep reinforcement learning," *SAE Tech. Paper*, p. 7, 2020.

[134] Y. Liu, X. Wang, L. Li, S. Cheng, and Z. Chen, "A novel lane change decision-making model of autonomous vehicle based on support vector machine," *IEEE Access*, vol. 7, pp. 26543–26550, 2019.

[135] Y. Dou, F. Yan, and D. Feng, "Lane changing prediction at highway lane drops using support vector machine and artificial neural network classifiers," in *Proc. IEEE Int. Conf. Adv. Intell. Mechatronics*, 2016, pp. 901–906.

[136] S. Ramyar, A. Homaifar, A. Karimoddini, and E. Tunstel, "Identification of anomalies in lane change behavior using one-class SVM," in *Proc. IEEE Int. Conf. Syst., Man, Cybern.*, 2016, pp. 004405–004410.

[137] J. H. Yang, W. Y. Choi, S.-H. Lee, and C. C. Chung, "Autonomous lane keeping control system based on road lane model using deep convolutional neural networks," in *Proc. IEEE Intell. Transp. Syst. Conf.*, 2019, pp. 3393–3398.

[138] X. Liu, J. Liang, and B. Xu, "A deep learning method for lane changing situation assessment and decision making," *IEEE Access*, vol. 7, pp. 133749–133759, 2019.

[139] J. Y. Choi, J. S. Kim, and C. C. Chung, "Radar-based lane estimation with deep neural network for lane-keeping system of autonomous highway driving," in *Proc. IEEE 23rd Int. Conf. Intell. Transp. Syst.*, 2020, pp. 1–6.

[140] Z. Chen, Q. Liu, and C. Lian, "Pointlanenet: Efficient end-to-end CNNs for accurate real-time lane detection," in *Proc. IEEE Intell. Veh. Symp.*, 2019, pp. 2563–2568.

[141] G. Li, S. E. Li, Y. Liao, W. Wang, B. Cheng, and F. Chen, "Lane change maneuver recognition via vehicle state and driver operation signals – results from naturalistic driving data," in *Proc. IEEE Intell. Veh. Symp.*, 2015, pp. 865–870.

[142] Y. Zheng and J. H. L. Hansen, "Lane-change detection from steering signal using spectral segmentation and learning-based classification," *IEEE Trans. Intell. Veh.*, vol. 2, no. 1, pp. 14–24, Mar. 2017.

[143] J. Huang, Y. Long, and X. Zhao, "Driver glance behavior modeling based on semi-supervised clustering and piecewise aggregate representation," *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 7, pp. 8396–8411, Jul. 2022.

[144] B. Khelfa, I. Ba, and A. Tordeux, "Predicting highway lane-changing maneuvers: A benchmark analysis of machine and ensemble learning algorithms," *Physica A: Statist. Mech. Appl.*, vol. 612, p. 128471, 2023.

[145] Y. Long, J. Huang, X. Zhao, and Z. Li, "Does LSTM outperform 4DDTW-KNN in lane change identification based on eye gaze data?," *Transp. Res. Part C: Emerg. Technol.*, vol. 137, 2022, Art. no. 103583. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0968090X22000298

[146] Q. Deng, M. Saleh, F. Tanshi, and D. Söffker, "Online intention recognition applied to real simulated driving maneuvers," in *Proc. IEEE Conf. Cogn. Comput. Aspects Situation Manage.*, 2020, pp. 1–6.

[147] Q. Bai, Z. Qu, X. Song, and S. Xiong, "A simulation-based approach to determine the location of dedicated transit lane," *IEEE Access*, vol. 7, pp. 50962–50970, 2019.

[148] M. Krüger, A. S. Novo, T. Nattermann, and T. Bertram, "Probabilistic lane change prediction using Gaussian process neural networks," in *Proc. IEEE Intell. Transp. Syst. Conf.*, 2019, pp. 3651–3656.

[149] Y. Bian, J. Ding, M. Hu, Q. Xu, J. Wang, and K. Li, "An advanced lane-keeping assistance system with switchable assistance modes," *IEEE Trans. Intell. Transp. Syst.*, vol. 21, no. 1, pp. 385–396, Jan. 2020.

[150] J. Lee, D. McGehee, T. Brown, and M. Reyes, "Collision warning timing, driver distraction, and driver response to imminent rear-end collisions in a high-fidelity driving simulator," *Hum. Factors*, vol. 44, pp. 314–334, 2002.

[151] L.-W. Wang, X.-F. Yang, and W.-C. Siu, "Learning approach with random forests on vehicle detection," in *Proc. IEEE 23rd Int. Conf. Digit. Signal Process.*, 2018, pp. 1–5.

[152] F. Teimouri and M. Ghatee, "A real-time warning system for rear-end collision based on random forest classifier," *J. Soft Comput. Civil Eng.*, vol. 4, pp. 49–71, 2018.

[153] A. Puspaningrum, A. Suheryadi, and A. Sumarudin, "Pre-collision warning and recommendation system for assistant driver using least square support vector machine and fuzzy logic," in *Proc. IEEE Int. Seminar Intell. Technol. Appl.*, 2019, pp. 371–375.

[154] S. M. Iranmanesh, H. N. Mahjoub, H. Kazemi, and Y. P. Fallah, "An adaptive forward collision warning framework design based on driver distraction," *IEEE Trans. Intell. Transp. Syst.*, vol. 19, no. 12, pp. 3925–3934, Dec. 2018.

[155] Q. Lim, Y. He, and U.-X. Tan, "Real-time forward collision warning system using nested Kalman filter for monocular camera," in *Proc. IEEE Int. Conf. Robot. Biomimetics*, 2018, pp. 868–873.

[156] M. Morsali, J. Åslund, and E. Frisk, "Trajectory planning in traffic scenarios using support vector machines," *IFAC-PapersOnLine*, vol. 52, pp. 91–96, 2019.

[157] S. Kumar, V. Shaw, J. Maitra, and R. Karmakar, "FCW: A forward collision warning system using convolutional neural network," in *Proc. IEEE Int. Conf. Elect. Electron. Eng.*, 2020, pp. 1–5.

[158] J. Pyo, J. Bang, and Y. Jeong, "Front collision warning based on vehicle detection using CNN," in *Proc. IEEE Int. SoC Des. Conf.*, 2016, pp. 163–164.

[159] C.-C. Lin, C.-W. Lin, D.-C. Huang, and Y.-H. Chen, "Design a support vector machine-based intelligent system for vehicle driving safety warning," in *Proc. IEEE 11th Int. Conf. Intell. Transp. Syst.*, 2008, pp. 938–943.

[160] E. Salari and D. Ouyang, "Camera-based forward collision and lane departure warning systems using SVM," in *Proc. IEEE 56th Int. Midwest Symp. Circuits Syst.*, 2013, pp. 1278–1281.

[161] A. Varghese and G. Sreelekha, "An efficient algorithm for detection of vacant spaces in delimited and non-delimited parking lots," *IEEE Trans. Intell. Transp. Syst.*, vol. 21, no. 10, pp. 4052–4062, Oct. 2020.

[162] Y. Zhang, Y. Du, A. Zhen, C. Li, and X. Hu, "The intelligent parking lot based on ZigBee technology and SVM," in *Proc. IEEE 14th Annu. Consum. Commun. Netw. Conf.*, 2017, pp. 620–621.

[163] Q. Wu, C. Huang, S.-Y. Wang, W.-C. Chiu, and T. Chen, "Robust parking space detection considering inter-space correlation," in *Proc. IEEE Int. Conf. Multimedia Expo*, 2007, pp. 659–662.

[164] S. U. Raj, M. V. Manikanta, P. S. S. Harsitha, and M. J. Leo, "Vacant parking lot detection system using random forest classification," in *Proc. IEEE 3rd Int. Conf. Comput. Methodol. Commun.*, 2019, pp. 454–458.

[165] S. Deb, A. K. Goswami, R. L. Chetri, and R. Roy, "Bayesian optimization based random forest method for state-of charge prediction for congestion management in distribution system considering charging coordination of plug-in electric vehicle," in *Proc. IEEE Int. Conf. Power Electron., Smart Grid, Renewable Energy*, 2022, pp. 1–6.

[166] W. Cho et al., "Robust parking occupancy monitoring system using random forests," in *Proc. IEEE Int. Conf. Electron., Inf., Commun.*, 2018, pp. 1–4.

[167] S. Rahman, M. Ramli, F. Arnia, A. Sembiring, and R. Muharar, "Convolutional neural network customization for parking occupancy detection," in *Proc. IEEE Int. Conf. Elect. Eng. Informat.*, 2020, pp. 1–6.

[168] J. Martinez, D. Zoeke, and M. Vossiek, "A convolutional neural network approach to parking monitoring in urban radar sensing," in *Proc. IEEE Eur. Radar Conf.*, 2017, pp. 86–89.

[169] T. Fukusaki, H. Tsutsui, and T. Ohgane, "An evaluation of a CNN-based parking detection system with Webcams," in *Proc. IEEE Asia-Pacific Signal Inf. Process. Assoc. Annu. Summit Conf.*, 2020, pp. 1–4.

[170] J. Nyambal and R. Klein, "Automated parking space detection using convolutional neural networks," in *Proc. IEEE Pattern Recognit. Assoc. South Afr. Robot. Mechatron.*, 2017, pp. 1–6.

[171] A. Suheryadi, W. P. Putra, M. A. A. Hilmi, and K. A. Cahyanto, "Vehicles position tracking in parking lots using K-nearest neighbor and fingerprinting based on RSSI bluetooth," in *Proc. IEEE 6th Int. Conf. Informat. Comput.*, 2021, pp. 1–6.

[172] M. V. Muntean, "Car park occupancy rates forecasting based on cluster analysis and KNN in smart cities," in *Proc. IEEE 11th Int. Conf. Electron., Comput. Artif. Intell.*, 2019, pp. 1–4.
[173] Z. Chen, K. Chen, and J. Chen, "Vehicle and pedestrian detection using support vector machine and histogram of oriented gradients features," in *Proc. IEEE Int. Conf. Comput. Sci. Appl.*, 2013, pp. 365–368.
[174] M. T.-T. Nguyen, V. D. Nguyen, and J. W. Jeon, "Real-time pedestrian detection using a support vector machine and stixel information," in *Proc. IEEE 17th Int. Conf. Control, Automat. Syst.*, 2017, pp. 1350–1355.
[175] Y. Sasaki, T. Emaru, and A. A. Ravankar, "SVM based pedestrian detection system for sidewalk snow removing machines," in *Proc. IEEE/SICE Int. Symp. Syst. Integration*, 2021, pp. 700–701.
[176] H. Yu, R. Hong, X. Huang, and Z. Wang, "Obstacle detection with deep convolutional neural network," in *Proc. IEEE 6th Int. Symp. Comput. Intell. Des.*, 2013, vol. 1, pp. 265–268.
[177] J. O. Pinzón-Arenas and R. Jiménez-Moreno, "Obstacle detection using faster R-CNN oriented to an autonomous feeding assistance system," in *Proc. IEEE 3rd Int. Conf. Inf. Comput. Technol.*, 2020, pp. 137–142.
[178] T. Rajendran, M. I. N, J. K, and A. K. D, "Road obstacles detection using convolution neural network and report using IoT," in *Proc. IEEE 4th Int. Conf. Smart Syst. Inventive Technol.*, 2022, pp. 22–26.
[179] P. Zhang, Y. Xiao, X. Wang, and B. Duan, "Semantic segmentation of point clouds of field obstacle-crossing terrain for multi-legged rescue equipment based on random forest," in *Proc. IEEE Int. Conf. Artif. Intell. Electromech. Automat.*, 2020, pp. 147–153.
[180] A. Mahdi, "A robot obstacle avoidance method based on random forest HTM cortical learning algorithm," *Webology*, vol. 17, pp. 788–803, 2020.
[181] A. M. Abdulkadium, "A robot obstacle avoidance method based on random forest HTM cortical learning algorithm," *Webology*, vol. 17, no. 2, pp. 788–803, 2020.
[182] Y. Bayzidi et al., "Traffic sign classifiers under physical world realistic sticker occlusions: A cross analysis study," in *Proc. IEEE Intell. Veh. Symp.*, 2022, pp. 644–650.
[183] A. Morgulis, A. Kreines, S. Mendelowitz, and Y. Weisglass, "Fooling a real car with adversarial traffic signs," 2019.
[184] Y. Li, X. Xu, J. Xiao, S. Li, and H. T. Shen, "Adaptive square attack: Fooling autonomous cars with adversarial traffic signs," *IEEE Internet Things J.*, vol. 8, no. 8, pp. 6337–6347, Apr. 2021.
[185] T. Gu, K. Liu, B. Dolan-Gavitt, and S. Garg, "Badnets: Evaluating backdooring attacks on deep neural networks," *IEEE Access*, vol. 7, pp. 47230–47244, 2019.
[186] A. Boloor, X. He, C. Gill, Y. Vorobeychik, and X. Zhang, "Simple physical adversarial examples against end-to-end autonomous driving models," in *Proc. IEEE Int. Conf. Embedded Softw. Syst.*, 2019, pp. 1–7.
[187] K. Eykholt et al., "Robust physical-world attacks on deep learning visual classification," in *Proc. IEEE/CVF Conf. Comput. Vis. Pattern Recognit.*, 2018, pp. 1625–1634.
[188] A. A. Elkhail, R. U. D. Refat, R. Habre, A. Hafeez, A. Bacha, and H. Malik, "Vehicle security: A survey of security issues and vulnerabilities, malware attacks and defenses," *IEEE Access*, vol. 9, pp. 162401–162437, 2021.
[189] S. Parkinson, P. Ward, K. Wilson, and J. Miller, "Cyber threats facing autonomous and connected vehicles: Future challenges," *IEEE Trans. Intell. Transp. Syst.*, vol. 18, no. 11, pp. 2898–2915, Nov. 2017.
[190] B. G. Stottelaar, "Practical cyber-attacks on autonomous vehicles," Master's Thesis, Univ. Twente, Netherlands, 2015.
[191] M. Harris, "Researcher hacks self-driving car sensors," *IEEE Spectr.*, 2015.
[192] H. Shin, D. Kim, Y. Kwon, and Y. Kim, "Illusion and dazzle: Adversarial optical channel exploits against lidars for automotive applications," in *Int. Conf. Cryptographic Hardware Embedded Syst.*, 2017, pp. 445–467.
[193] Y. Cao et al., "Adversarial sensor attack on lidar-based perception in autonomous driving," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, New York, NY, USA, 2019, pp. 2267–2281.
[194] S. Malik, P. Bandi, and W. Sun, "An experimental study of denial of service attack against platoon of smart vehicles," in *Proc. IEEE 4th Int. Conf. Connected Auton. Driving*, 2021, pp. 23–30.
[195] N. Flysher, R. Yozevitch, and B. Ben-Moshe, "GNSS denial of service and the preparation for tomorrow's threats," in *Proc. IEEE Int. Conf. Sci. Elect. Eng.*, 2016, pp. 1–5.
[196] Y. Deng, X. Zheng, T. Zhang, C. Chen, and M. Kim, "An analysis of adversarial attacks and defenses on autonomous driving models," in *Proc. IEEE Int. Conf. Pervasive Comput. Commun.*, 2020, pp. 1–10.
[197] A. Qayyum, M. Usama, J. Qadir, and A. Al-Fuqaha, "Securing connected amp; autonomous vehicles: Challenges posed by adversarial machine learning and the way forward," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 2, pp. 998–1026, Secondquarter 2020.
[198] P. A. Johnson, B. Tan, and S. Schuckers, "Multimodal fusion vulnerability to non-zero effort (spoof) imposters," in *Proc. IEEE Int. Workshop Inf. Forensics Secur.*, 2010, pp. 1–5.
[199] A. Adler, "Vulnerabilities in biometric encryption systems," in *Int. Conf. Ausio Video-Based Biometric Person Authentication*, Berlin, Heidelberg, Germany, 2005, pp. 1100–1109.
[200] P. Fogla, M. Sharif, R. Perdisci, O. Kolesnikov, and W. Lee, "Polymorphic blending attacks," in *Proc. USENIX Secur. Symp.*, 2006, Art. no. 16.
[201] D. Lowd, "Good word attacks on statistical spam filters," in *Proc. 2nd Conf. Email Anti-Spam*, 2005.
[202] B. Biggio, B. Nelson, and P. Laskov, "Poisoning attacks against support vector machines," in *Proc. 29th Int. Conf. Mach. Learn.*, 2012, pp. 1467–1474.
[203] M. Sharif, S. Bhagavatula, L. Bauer, and M. K. Reiter, "A general framework for adversarial examples with objectives," *ACM Trans. Privacy Secur.*, vol. 22, no. 3, pp. 16:1–16:30, 2019.
[204] C. Liu, B. Li, Y. Vorobeychik, and A. Oprea, "Robust linear regression against training data poisoning," in *Proc. 10th ACM Workshop Artif. Intell. Secur.*, New York, NY, USA, 2017, pp. 91–102.
[205] C. Szegedy et al., "Intriguing properties of neural networks," 2014.
[206] A. Kurakin, I. J. Goodfellow, and S. Bengio, "Adversarial examples in the physical world," in *Artificial Intelligence Safety and Security*, San Rafael, CA, USA: CRC Press, 2018, pp. 99–112. [Online]. Available: https://www.taylorfrancis.com/chapters/edit/10.1201/9781351251389-8/adversarial-examples-physical-world-alexey-kurakin-ian-goodfellow-samy-bengio
[207] Y. Liu et al., "Trojaning attack on neural networks," *Purdue Univ.*, Tech. Rep. 17-002, 2018.
[208] E. Yurtsever, J. Lambert, A. Carballo, and K. Takeda, "A survey of autonomous driving: Common practices and emerging technologies," *IEEE Access*, vol. 8, pp. 58443–58469, 2020.
[209] S. Wang and Z. Li, "Exploring the mechanism of crashes with automated vehicles using statistical modeling approaches," *PLoS One*, vol. 14, no. 3, 2019, Art. no. e0214550.
[210] A. M. Aung, Y. Fadila, R. Gondokaryono, and L. Gonzalez, "Building robust deep neural networks for road sign detection," 2017.
[211] C. Sitawarin, A. N. Bhagoji, A. Mosenia, P. Mittal, and M. Chiang, "Rogue signs: Deceiving traffic sign recognition with malicious ads and logos," 2018.
[212] C. Sitawarin, A. N. Bhagoji, A. Mosenia, M. Chiang, and P. Mittal, "Darts: Deceiving autonomous cars with toxic signs," 2018.
[213] D. Nassi, R. Ben-Netanel, Y. Elovici, and B. Nassi, "Mobilbye: Attacking ADAS with camera spoofing," 2019.
[214] A. Chernikova, A. Oprea, C. Nita-Rotaru, and B. Kim, "Are self-driving cars secure? evasion attacks against deep neural networks for steering angle prediction," in *Proc. IEEE Secur. Privacy Workshops*, 2019, pp. 132–137.
[215] W. Jiang, H. Li, S. Liu, X. Luo, and R. Lu, "Poisoning and evasion attacks against deep learning algorithms in autonomous vehicles," *IEEE Trans. Veh. Technol.*, vol. 69, no. 4, pp. 4439–4449, Apr. 2020.
[216] T. Wu, X. Ning, W. Li, R. Huang, H. Yang, and Y. Wang, "Physical adversarial attack on vehicle detector in the Carla simulator," 2020.
[217] X. Yang, W. Liu, S. Zhang, W. Liu, and D. Tao, "Targeted attention attack on deep learning models in road sign recognition," *IEEE Internet Things J.*, vol. 8, no. 6, pp. 4980–4990, Mar. 2021.
[218] B. Ye, H. Yin, J. Yan, and W. Ge, "Patch-based attack on traffic sign recognition," in *Proc. IEEE Int. Intell. Transp. Syst. Conf.*, 2021, pp. 164–171.
[219] A. Ghosh, S. S. Mullick, S. Datta, S. Das, A. K. Das, and R. Mallipeddi, "A black-box adversarial attack strategy with adjustable sparsity and generalizability for deep image classifiers," *Pattern Recognit.*, vol. 122, 2022, Art. no. 108279.

[220] N. Patel, P. Krishnamurthy, S. Garg, and F. Khorrami, "Overriding autonomous driving systems using adaptive adversarial billboards," *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 8, pp. 11386–11396, Aug. 2022.

[221] L. Chi, M. Msahli, G. Memmi, and H. Qiu, "Public-attention-based adversarial attack on traffic sign recognition," in *Proc. IEEE 20th Consum. Commun. Netw. Conf.*, 2023, pp. 740–745.

[222] N. Morgulis, A. Kreines, S. Mendelowitz, and Y. Weisglass, "Fooling a real car with adversarial traffic signs," 2019.

[223] "Experimental security research of tesla autopilot," Tencent Keen Security Lab, White Paper, 2019.

[224] S. Povolny and S. Trivedi, "Model hacking ADAS to pave safer roads for autonomous vehicles," *McAfee Blogs*, 2020.

[225] K. He, G. Gkioxari, P. Dollár, and R. Girshick, "Mask R-CNN," in *Proc. IEEE Int. Conf. Comput. Vis.*, 2017, pp. 2980–2988.

[226] J. Redmon and A. Farhadi, "Yolov3: An incremental improvement," 2018, *arXiv:1804.02767*.

[227] Y. Zhang, H. Foroosh, P. David, and B. Gong, "CAMOU: Learning physical vehicle camouflages to adversarially attack detectors in the wild," in *Proc. Int. Conf. Learn. Representations*, 2018, pp. 1–20.

[228] K. Eykholt et al., "Physical adversarial examples for object detectors," in *Proc. 12th USENIX Workshop On Offensive Technol.*, 2018, Art. no. 1.

[229] H. Zhou et al., "Deepbillboard: Systematic physical-world testing of autonomous driving systems," 2018, *arXiv:1812.10812*.

[230] B. Group, "Safety assessment report, sae level 3 automated driving system," BMW Group, Munich, Germany, Tech. Rep., 2020. [Online]. Available: https://usermanual.wiki/m/4bc317041f2a935a1043a71c6f17e878c4b17dddbbf798f19c27a4e0be22bfbb.pdf

[231] J. Cui, G. Sabaliauskaite, L. S. Liew, F. Zhou, and B. Zhang, "Collaborative analysis framework of safety and security for autonomous vehicles," *IEEE Access*, vol. 7, pp. 148672–148683, 2019.

[232] "An oem and automotive supplier's guide to the unece wp.29 cybersecurity regulation," Upsream Security Limited, White Paper, 2020.

[233] S. Gu and L. Rigazio, "Towards deep neural network architectures robust to adversarial examples," 2015, *arXiv:1412.5068*.

[234] I. J. Goodfellow, J. Shlens, and C. Szegedy, "Explaining and harnessing adversarial examples," 2014, *arXiv:1412.6572*.

[235] W. Xu, D. Evans, and Y. Qi, "Feature squeezing: Detecting adversarial examples in deep neural networks," in *Proc. 2018 Netw. Distrib. Syst. Secur. Symp.*, 2018.

[236] J. Gao, B. Wang, Z. Lin, W. Xu, and Y. Qi, "Deepcloak: Masking deep neural network models for robustness against adversarial samples," 2017, *arXiv:1702.06763*.

[237] Y. Song, T. Kim, S. Nowozin, S. Ermon, and N. Kushman, "Pixeldefend: Leveraging generative models to understand and defend against adversarial examples," 2018, *arXiv:1710.10766*.

[238] A. S. Ross and F. Doshi-Velez, "Improving the adversarial robustness and interpretability of deep neural networks by regularizing their input gradients," 2017, *arXiv:1711.09404*.

[239] S. Garg, V. Sharan, B. Zhang, and G. Valiant, "A spectral view of adversarially robust features," 2018, *arXiv:1811.06609*.

[240] A. Prakash, N. Moran, S. Garber, A. DiLillo, and J. Storer, "Deflecting adversarial attacks with pixel deflection," in *Proc. IEEE/CVF Conf. Comput. Vis. Pattern Recognit.*, 2018, pp. 8571–8580.

[241] E. Wong and J. Z. Kolter, "Provable defenses against adversarial examples via the convex outer adversarial polytope," 2018, *arXiv:1711.00851*.

[242] L. Schott, J. Rauber, M. Bethge, and W. Brendel, "Towards the first adversarially robust neural network model on MNIST," 2018, *arXiv:1805.09190*.

[243] Q. Sun, A. A. Rao, X. Yao, B. Yu, and S. Hu, "Counteracting adversarial attacks in autonomous driving," in *Proc. IEEE/ACM Int. Conf. Comput. Aided Des.*, 2020, pp. 1–7.

[244] P. Laykaviriyakul and E. Phaisangittisagul, "Initialization of random vectors to enhance defense-GAN for image classification," in *Proc. IEEE Int. Elect. Eng. Congr.*, 2022, pp. 1–4.

[245] Q. Zhang, S. Hu, J. Sun, Q. A. Chen, and Z. M. Mao, "On adversarial robustness of trajectory prediction for autonomous vehicles," in *Proc. IEEE/CVF Conf. Comput. Vis. Pattern Recognit.*, 2022, pp. 15138–15147.

[246] J. Wang, W. Su, C. Luo, J. Chen, H. Song, and J. Li, "CSG: Classifier-aware defense strategy based on compressive sensing and generative networks for visual recognition in autonomous vehicle systems," *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 7, pp. 9543–9553, Jul. 2022.

[247] K. H. Shibly, M. D. Hossain, H. Inoue, Y. Taenaka, and Y. Kadobayashia, "Towards autonomous driving model resistant to adversarial attack," *Internation J. Appl. Artif. Intell.*, vol. 37, no. 1, 2023, Art. no. 2193461.

[248] Z. Yan, Y. Guo, and C. Zhang, "Deep defense: Training DNNs with improved adversarial robustness," 2018, *arXiv:1803.00404*.

[249] R. Huang, B. Xu, D. Schuurmans, and C. Szepesvari, "Learning with a strong adversary," 2016, *arXiv:1511.03034*.

[250] P.-H. Chiang, C.-S. Chan, and S.-H. Wu, "Adversarial pixel masking: A defense against physical attacks for pre-trained object detectors," in *Proc. 29th ACM Int. Conf. Multimedia*, 2021, pp. 1856–1865.

[251] G. Katz, C. Barrett, D. Dill, K. Julian, and M. Kochenderfer, "Reluplex: An efficient SMT solver for verifying deep neural networks," 2017, *arXiv:1702.01135*.

[252] J. Lu, T. Issaranon, and D. Forsyth, "Safetynet: Detecting and rejecting adversarial examples robustly," in *Proc. IEEE Int. Conf. Comput. Vis.*, 2017, pp. 446–454.

[253] D. Gopinath, G. Katz, C. S. Pasareanu, and C. Barrett, "Deepsafe: A data-driven approach for checking adversarial robustness in neural networks," 2020, *arXiv:1710.00486*.

[254] G. Katz, C. Barrett, D. Dill, K. Julian, and M. Kochenderfer, "Towards proving the adversarial robustness of deep neural networks," *Electron. Proc. Theor. Comput. Sci.*, vol. 257, pp. 19–26, 2017.

MANSI GIRDHAR (Graduate Student Member, IEEE) received the Bachelor of Technology and Master of Technology degrees in electronics and communication engineering from India in 2014 and 2017, respectively. She is currently working toward the Ph.D. degree in electrical and computer engineering with the University of Michigan-Dearborn, Dearborn, MI, USA. Her research interests include cybersecurity of power systems, electric vehicle charging stations (EVCSs), and connected and automated vehicles (CAVs).

JUNHO HONG (Senior Member, IEEE) received the Ph.D. degree in electrical engineering from the Cybersecurity of Substation Automation System, Washington State University, Pullman, WA, USA, in 2014. He is currently an Assistant Professor with the Department of Electrical and Computer Engineering, University of Michigan–Dearborn, Dearborn, MI, USA. During 2014–2019, he was with ABB, where he provided technical project leadership and supported strategic corporate technology development/productization in areas related to cyber-physical security for substations, power grids control and protection, renewable integration, and utility communications. He has been working on cybersecurity of energy delivery systems with the Department of Energy (DOE) as Principal Investigator (PI) and Co-PI in the areas of substation, microgrids, HVDC, FACTS, and high-power EV chargers. He is with the CIGRE WG D2.50 Electric power utilities cybersecurity for contingency operations.

JOHN MOORE (Member, IEEE) received the Bachelor of General Studies (BGS) degree from the University of Michigan-Ann Arbor, Ann Arbor, MI, USA, and the Master of Computer and Information Science (CIS) degree from the University of Michigan-Dearborn, Dearborn, MI. He works for the Ford Motor Company as Vehicle Cybersecurity Technical Specialist for Advanced Engineering and Research within Product Development. He holds a CISSP. Hisresearch interests include advance computation, sensing, platform trust, cyber resiliency and AI security architectures within the vehicle ecosystem.