







Security and Privacy Challenges and Solutions in Autonomous Driving Systems: A Comprehensive Review

Giuseppe Lippi¹ , Mahmoud Aljawarneh² , Qais Al-Na'amneh² , Rahaf Hazaymih³, Lachhman Das Dhomeja⁴ 

¹ Section of Clinical Biochemistry and School of Medicine, University of Verona, Verona, Italy

² Faculty of Information Technology, Applied Science Private University, Amman, Jordan

³ Dept. Computer Science, Jordan University of Science and Technology, Irbid, Jordan

⁴ Faculty of Engineering and Technology, Sindh University, Jamshoro, Pakistan

ARTICLE INFO

Article History

Received: 25-03-2025

Revised: 04-05-2025

Accepted: 05-05-2025

Published: 06-05-2025

Academic Editor:

Prof. Youakim Badr

Vol.2025, No.3

DOI:

<https://doi.org/10.63180/jcsra.thestap.2025.3.3>



ABSTRACT

The rapid advancement of autonomous driving technology has transformed modern transportation, offering enhanced safety, efficiency, and convenience. However, as these vehicles become increasingly connected and reliant on complex software and sensor-based systems, they also become prime targets for a wide range of cyber and privacy threats. This review paper comprehensively examines the current landscape of security and privacy in autonomous driving systems. We explore emerging attack vectors targeting key components such as sensor perception, vehicle-to-everything (V2X) communication, machine learning models, and internal control systems. Particular attention is given to adversarial machine learning, GPS spoofing, Controller Area Network (CAN) bus attacks, and data privacy breaches. In parallel, we evaluate existing defense mechanisms and mitigation strategies, including intrusion detection systems (IDS), secure communication protocols, hardware-based security modules, and privacy-preserving architectures. We also highlight key challenges in securing autonomous systems, identify gaps in current research, and propose directions for future work to build resilient and trustworthy autonomous vehicles. This review aims to provide researchers and practitioners with a consolidated foundation for understanding and advancing the security posture of next-generation autonomous driving technologies.

Keywords: Autonomous vehicles, cybersecurity, privacy, security attacks, defense mechanisms, sensor security, V2X security, machine learning security, CAN bus security, data privacy, adversarial machine learning, GPS spoofing, and intrusion detection systems.

How to cite the article

Lippi, G., Aljawarneh, M., Al-Na'amneh, Q., Hazaymih, R., & Dhomeja, L. D. (2025). Security and Privacy Challenges and Solutions in Autonomous Driving Systems: A Comprehensive Review. Journal of Cyber Security and Risk Auditing, 2025(3), 23–41. <https://doi.org/10.63180/jcsra.thestap.2025.3.3>

1. Introduction

The confluence of sophisticated sensing modalities, advanced computing architectures, and ubiquitous connectivity has ushered in an era heralding the widespread deployment of autonomous vehicles (AVs). These sophisticated machines promise revolutionary shifts in personal mobility, freight logistics, and urban planning, offering potential benefits encompassing enhanced road safety through elimination of human error, optimized traffic flow reducing congestion and fuel consumption, expanded accessibility for individuals with mobility limitations, and novel economic opportunities within emergent transportation models [1, 2]. The transition from driver-assisted features to fully autonomous operation necessitates a profound increase in computational complexity and reliance on interconnected systems operating seamlessly in dynamic environments [3] as shown in Fig. 1.

While foundational to achieving autonomous capabilities, this escalating complexity simultaneously expands the system's vulnerability surface, presenting a compelling target for malicious actors. As vehicles evolve from isolated mechanical devices into highly connected nodes within a broader transportation ecosystem, the traditional physical security concerns are compounded by a diverse spectrum of cyber and privacy threats. Compromises impacting autonomous functions—from perception and decision-making to vehicle control and external communication—can potentially affect safety, property, and human life [4, 5, 6, 7, 8]. Furthermore, the pervasive data collection inherent in autonomous operation raises significant privacy concerns, necessitating robust safeguards against unauthorized access, usage, or disclosure of sensitive information about vehicle occupants, locations, and driving behaviors [9].

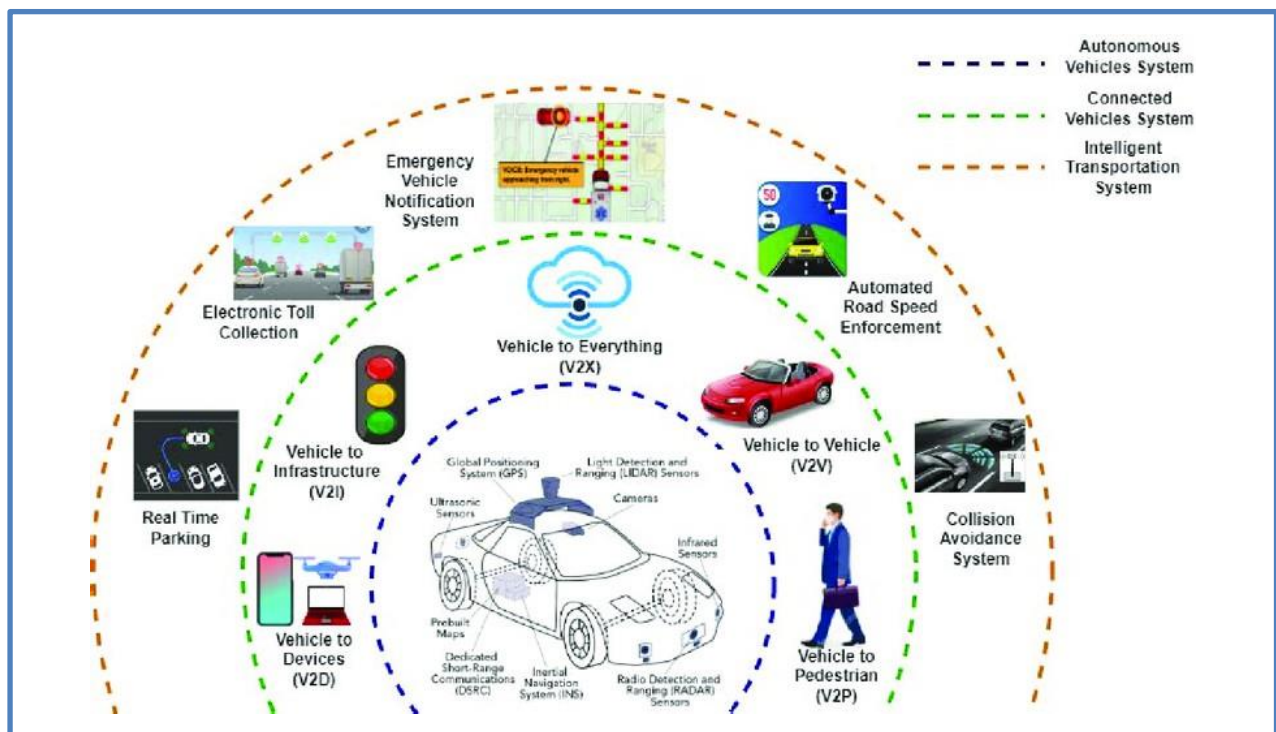


Figure 1. Overview of vehicle infrastructure.

Securing autonomous driving systems thus represents a paramount challenge, demanding proactive design and rigorous evaluation throughout the development lifecycle. The dynamic interplay between system components, the real-time demands of autonomous operation, and the continuously evolving nature of cyber threats necessitate a comprehensive understanding of potential attack [10, 11, 12, 13, 14, 15] vectors and corresponding defense strategies. This paper thoroughly reviews the security and privacy landscape pertinent to autonomous vehicles, dissecting key attack methodologies and evaluating current mitigation techniques. We examine vulnerabilities intrinsic to core AV subsystems: sensor perception, vehicle-to-everything (V2X) communication, underlying machine learning models, and the internal vehicle network infrastructure. Specific

attention is directed towards prevalent threats such as adversarial manipulations of sensor data, spoofing of global positioning signals, exploitation of the Controller Area Network (CAN) bus protocol, and breaches of occupant privacy. Counterbalancing this analysis, we survey a range of defense mechanisms, including advanced intrusion detection systems, secure communication protocols tailored for vehicular environments, hardware-anchored security primitives, and architectural approaches to preserve data privacy. Addressing key challenges impeding the deployment of truly secure autonomous systems, this review identifies critical gaps in current research efforts and delineates promising avenues for future investigation. The objective is to furnish researchers, engineers, and policymakers with a structured synthesis of existing knowledge, thereby fostering continued progress in building resilient and trustworthy autonomous driving technologies, as shown in Figure 2.



Figure 2. Autonomous Vehicle connected transportation systems.

2. Autonomous Vehicle Connected Transportation Systems

2.1 Autonomous Vehicle Connected Transportation Systems

A foundational understanding of autonomous vehicle architecture proves indispensable when analyzing potential security and privacy vulnerabilities. The design of these systems typically adheres to a layered abstraction, broadly segmented into perception, planning, and control modules [16]. Each layer relies on a complex interplay of heterogeneous hardware and sophisticated software, presenting distinct interfaces and internal processing points susceptible to compromise.

At the base layer resides the Perception System, which interprets the vehicle's surroundings. This relies heavily on an array of diverse sensors. Cameras provide rich visual information for tasks such as object detection, recognition, lane keeping, and traffic sign reading [17]. LiDAR (Light Detection and Ranging) sensors emit laser pulses to create precise 3D maps of the environment, excelling in distance measurement and object shape determination, particularly under varying lighting conditions [18]. Radar utilizes radio waves to detect objects and measure their velocity and distance, operating robustly in adverse weather where visual or LiDAR data may be degraded. Ultrasonic sensors assist with short-range detection and

are commonly used for parking and low-speed maneuvering. Global Navigation Satellite Systems (GNSS), predominantly GPS, provide global positioning data, often augmented by Inertial Measurement Units (IMUs), which track orientation and acceleration, enabling dead reckoning when GNSS signals are weak or unavailable. The raw data streams originating from these disparate sensors undergo significant processing, often involving complex algorithms and machine learning models to extract meaningful information, such as object classification, tracking, and scene semantic segmentation [19, 20].

The processed perception data feeds into the Planning System. This layer is responsible for predicting the behavior of other road users and dynamic elements in the environment, making high-level decisions regarding route selection, trajectory generation, and tactical maneuvers like lane changes or merging. This involves sophisticated algorithms for behavioral prediction, path optimization, and decision-making under uncertainty [21]. The output of the planning system is a specific, executable trajectory or sequence of actions for the vehicle to follow. The Control System executes the planned trajectory by sending commands to the vehicle's actuators. This involves low-level control loops managing steering, acceleration, and braking [22]. These commands are relayed through various Electronic Control Units (ECUs)—specialized embedded computers controlling specific vehicle functions. Modern vehicles feature dozens, sometimes over a hundred, interconnected ECUs managing everything from engine performance and braking systems (ABS, ESC) to airbags, infotainment, connectivity, and domain-specific controllers for autonomous driving functions [23]. Communication between these ECUs occurs over In-Vehicle Networks. The historical and still prevalent network is the Controller Area Network (CAN bus), known for its simplicity, robustness in noisy environments, and cost-effectiveness.

However, CAN's design inherently lacks built-in security features like message authentication or encryption, as it was conceived in an era predating significant cyber threats [24]. Newer, higher-bandwidth networks like Automotive Ethernet and FlexRay offer improved performance and capabilities, including support for IP-based protocols, presenting both new opportunities and different security challenges [25]. LIN (Local Interconnect Network) handles less critical, lower-bandwidth communications, often acting as a sub-bus as shown Figure 3.

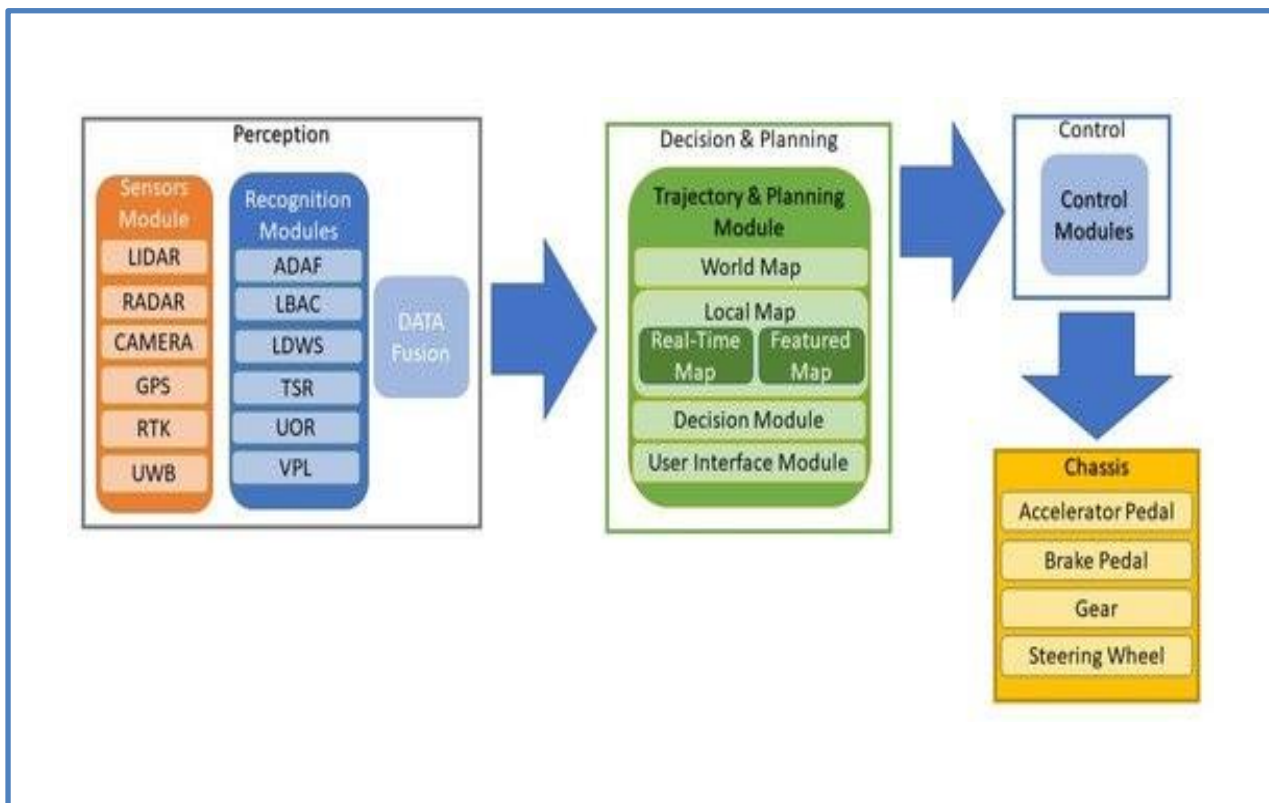


Figure 3. Architectural vehicle Autonomous.

Processing the immense data flow and executing complex algorithms, particularly those involving machine learning, requires substantial computational power. Compute Platforms utilizing high-performance processors, GPUs (Graphics

Processing Units), and specialized AI accelerators like TPUs (Tensor Processing Units) are central to modern AV designs [26]. These platforms host sophisticated software stacks implementing perception algorithms, planning logic, and control strategies.

External interaction and communication are handled by Connectivity Modules. Vehicle-to-Everything (V2X) communication, encompassing V2V (Vehicle-to-Vehicle), V2I (Vehicle-to-Infrastructure), V2N (Vehicle-to-Network), and V2P (Vehicle-to-Pedestrian), allows AVs to exchange information with other road entities and the surrounding environment [27]. Technologies like Dedicated Short-Range Communications (DSRC) and Cellular V2X (C-V2X) provide protocols for broadcasting safety messages, traffic information, and coordinating maneuvers [28, 29]. Standard cellular (LTE, 5G), Wi-Fi, and Bluetooth modules also facilitate communication for data updates, remote diagnostics, infotainment services, and user interaction.

Finally, the system interfaces with the physical world through Actuators controlling critical functions such as steering, braking, and throttle. Compromising the control commands sent to these actuators can directly lead to dangerous vehicle behavior [30]. Understanding the flow of information and command signals across these diverse components is crucial for identifying where vulnerabilities might reside and how attacks could propagate through the system.

3. Threat Landscape: Attack Vector and Vulnerabilities

Autonomous vehicles, by virtue of their intricate architecture, reliance on extensive software, and pervasive connectivity, expose a multifaceted threat landscape. Attackers, possessing varying levels of sophistication and motivations, could target different system components with objectives ranging from disrupting operations and causing accidents to stealing data or holding the vehicle for ransom. A systematic exploration of these attack vectors reveals the significant security challenges inherent in deploying trustworthy autonomous transportation.

3.1 Attacks on Sensor Perception Systems

The perception system, responsible for interpreting the physical environment, represents a critical yet potentially vulnerable component. Attacks targeting sensors aim to deceive the vehicle into misinterpreting its surroundings, leading to incorrect decisions by the planning and control systems. Different sensor modalities exhibit distinct vulnerabilities.

Camera-based perception often relies on complex deep learning models for object detection, classification, and segmentation. These models are known to be susceptible to adversarial machine learning (AML) attacks. An attacker can craft subtle perturbations to input data—in this case, visual scenes—that are imperceptible to humans but cause the machine learning model to misclassify objects with high confidence [31]. Physical AML attacks are particularly concerning for AVs, where modifications applied to real-world objects or the environment trick the perception system. For instance, researchers have demonstrated that applying specifically designed adversarial stickers or patches to stop signs can cause the vehicle's camera system to misclassify them as speed limit signs or even ignore them entirely [32]. These patches exploit the specific feature extraction patterns learned by the deep neural networks. Projection attacks, another physical method, involve projecting adversarial patterns onto the road surface or objects using a projector, effectively modifying the visual input perceived by the camera [33]. Blinding attacks, using high-intensity lasers or LEDs directed at the camera lens, represent a simple yet effective denial-of-service (DoS) vector, temporarily incapacitating visual perception [34]. While less sophisticated than adversarial manipulation, successful blinding necessitates the system's reliance on other sensor modalities or entering a safe state. Spoofing visual cues might involve placing deceptive objects in the environment or manipulating digital video streams if an attacker gains access to the camera feed before processing.

LiDAR systems are vulnerable to spoofing and jamming. LiDAR spoofing involves injecting carefully timed and angled laser pulses that mimic reflections from phantom objects at specific distances and locations, creating ghost obstacles or vehicles in the resulting point cloud data [35]. By controlling the timing and intensity of emitted pulses, an attacker can generate false positive detections, potentially causing the AV to brake unnecessarily or attempt evasive maneuvers that lead to accidents. Conversely, jamming attacks aim to overwhelm the LiDAR sensor with high-intensity laser signals, effectively blinding it within certain angles or ranges, similar to camera blinding but targeting the LiDAR's operational frequency [36]. The impact is a loss of depth information, hindering the creation of an accurate 3D environment map.

Radar systems can also be targeted with spoofing and jamming attacks. Radar spoofing involves transmitting false radar signals designed to mimic legitimate reflections, creating phantom targets that appear on the radar's display [37]. Sophisticated spoofing might even attempt to hide legitimate objects by generating signals that interfere destructively. Jamming involves broadcasting noise or interference at the radar's operating frequencies to saturate the receiver, rendering

it unable to detect real targets [38]. Radar's reliance on Doppler shift for velocity measurement offers some resilience but is not immune to advanced spoofing techniques mimicking realistic target movement.

GPS/GNSS systems, crucial for vehicle localization and timing, are notoriously susceptible to spoofing and jamming attacks [39]. GPS jamming involves transmitting radio noise on GNSS frequencies, effectively drowning out the weak satellite signals and causing a denial-of-service for positioning. GPS spoofing is more insidious; it involves broadcasting counterfeit GPS-like signals that appear legitimate to the vehicle's receiver but transmit false position and time information. A synchronized spoofer can gradually shift the perceived location without triggering immediate anomaly detection based on sudden jumps [40]. Successful GPS spoofing can mislead the AV about its current location, causing navigation errors, inaccurate map matching, and potentially dangerous deviations from its planned path. The reliance on precise timing signals also makes the system vulnerable to timing spoofing, affecting functions that depend on accurate time synchronization, such as V2X communication or sensor data fusion timestamping. Attacks can also target Sensor Fusion systems directly [41]. Instead of attacking individual sensors, an attacker might aim to feed conflicting or subtly manipulated data from multiple sensors into the fusion algorithm, exploiting potential weaknesses in how the system weighs, correlates, or validates disparate inputs. For instance, a sophisticated attack might combine minor spoofing on GPS with a subtle adversarial patch on a visual target, creating a scenario where the fusion algorithm produces a dangerously incorrect world model that is difficult to detect by simply checking individual sensor outputs [42].

3.2 Attacks on Vehicle-to-Everything (V2X) Communication

V2X communication is designed to augment the AV's situational awareness by enabling direct exchange of information with other vehicles (V2V), infrastructure (V2I), pedestrians (V2P), and the network (V2N). While intended to enhance safety and efficiency, the wireless nature of V2X protocols (like DSRC and CV2X) exposes them to significant cyber threats [27]. The security of V2X communications relies heavily on Public Key Infrastructure (PKI) and security credentials, managed by systems like the Security Credential Management System (SCMS) in DSRC or equivalent components in C-V2X, to authenticate messages and ensure their integrity [43]. However, implementation vulnerabilities or attacks bypassing cryptographic protections remain a concern.

A primary V2X attack vector is Message Injection/Spoofing. An attacker can craft and broadcast malicious V2X messages impersonating legitimate sources (vehicles, infrastructure units) [44]. Examples include injecting false Basic Safety Messages (BSMs) reporting non-existent vehicles or obstacles, fabricating Cooperative Awareness Messages (CAMs) with incorrect location or speed data, or sending deceptive Decentralized Environmental Notification Messages (DENMs) about phantom hazards [45]. Successfully injected messages can trick an AV's planning system into taking unnecessary evasive actions (leading to collisions with real objects) or ignoring real threats.

Message Modification involves intercepting legitimate V2X messages and altering their content before retransmitting them. While cryptographic signatures (like ECDSA used in IEEE 1609.2) are designed to prevent this by ensuring message integrity, vulnerabilities in key management, protocol implementations, or side-channel attacks on the cryptographic modules could potentially enable modification. Message Replay attacks involve capturing valid V2X messages and retransmitting them later. Although message timestamps and sequence numbers are intended to mitigate replay, an attacker might replay messages from a different context or with slightly manipulated timing information to confuse the receiving vehicle [46]. For instance, replaying an emergency brake warning from a recent event when no immediate threat exists could still disrupt traffic flow or trigger dangerous reactions.

Jamming attacks on V2X communication simply involve flooding the designated V2X radio channels with noise, preventing legitimate messages from being received. This constitutes a denial-of-service attack that degrades the AV's awareness and disables V2X-dependent safety applications [47].

Sybil Attacks involve an attacker creating numerous fake identities (pseudonyms or temporary certificates) to flood the V2X network with messages, potentially overwhelming the system or creating a false impression of traffic density or event severity [48]. This could be used to trigger coordinated false alerts or disrupt distributed applications like platooning.

Man-in-the-Middle (MitM) Attacks on V2X communication are more complex but potentially devastating, allowing an attacker to intercept, read, modify, and relay messages between legitimate parties. While V2X security standards aim to prevent this through authentication and integrity checks, successful key compromise or exploitation of implementation flaws could make MitM possible, enabling sophisticated manipulation of the information exchanged between vehicles and

infrastructure [49]. The impact of these attacks is direct: degrading situational awareness, causing incorrect decisions, and potentially leading to unsafe maneuvers or loss of collaborative functionality like platooning or cooperative merging.

3.3 Attacks on Machine Learning Models

Machine learning, intense learning, forms the backbone of many AV functionalities, from object recognition and behavior prediction to decision-making. The susceptibility of ML models to adversarial manipulation constitutes a significant security concern [50, 51]. Beyond the perception attacks mentioned earlier, ML models throughout the AV stack are potential targets.

Adversarial Machine Learning (AML) techniques broadly fall into several categories. Evasion attacks (also known as inference-time attacks) aim to cause a deployed model to make incorrect predictions by carefully crafting malicious inputs [52]. In the context of AVs, this is vividly demonstrated by adversarial patches on physical objects or subtle digital perturbations applied to sensor data streams before they reach the ML model [34]. Such attacks can cause the perception system to miss pedestrians, misread signs, or incorrectly classify other vehicles. AML can also target ML models used in prediction (e.g., predicting pedestrian trajectories) or planning (e.g., predicting other drivers' intentions), leading to incorrect behavioral anticipation and potentially dangerous maneuvers.

Poisoning attacks (or training-time attacks) involve injecting malicious data into the training dataset used to build or fine-tune the ML model [53]. Suppose an attacker can influence the data collected for training or gain access to the training pipeline. In that case, they can strategically insert poisoned examples that force the model to learn specific malicious behaviors or create backdoors that trigger misbehavior only when presented with specific, rare inputs [54]. For example, poisoning data might cause the vehicle to ignore stop signs under specific, unusual lighting conditions or react aggressively to certain vehicles.

Model Inversion attacks attempt to infer sensitive information about the training data from the deployed model's outputs [55]. While less directly threatening to immediate safety, a successful inversion attack could lead to privacy breaches if the training data included personally identifiable information or details about specific locations.

Model Extraction attacks aim to steal the intellectual property embodied in a trained model, including its architecture and parameters, by querying it and observing its outputs [56]. An extracted model could then be used to train more effective adversarial attacks against the deployed system or be replicated for commercial purposes.

The impact of successful AML attacks on AVs is profound, directly undermining the system's ability to understand its environment, predict events, and make safe decisions. The opaque nature of deep learning models (the "black box" problem) makes it challenging to understand why a model makes a particular decision, complicating the detection and diagnosis of adversarial manipulations [47].

3.4 Attacks on In-Vehicle Networks and Internal Systems

Compromising the internal vehicle network or ECUs grants attackers control over critical vehicle functions, potentially leading to loss of control or direct manipulation of safety systems, as shown in Fig. 4, while Table I summarizes the different attack vectors discussed in the literature.

4. Autonomous Vehicle Attacks

The CAN bus remains a primary target due to its inherent lack of security features. Messages on the CAN bus are broadcast to all connected ECUs, and there is no mechanism for source authentication or encryption. Any device connected to the bus can inject messages, modify the bus state, or eavesdrop on traffic [58]. The simplified arbitration process based on message ID means that a lower ID message has higher priority; an attacker can exploit this by injecting high-priority messages to suppress legitimate, safety-critical ones (e.g., brake commands) or inject malicious high-priority commands (e.g., sudden acceleration, avoid breaking).

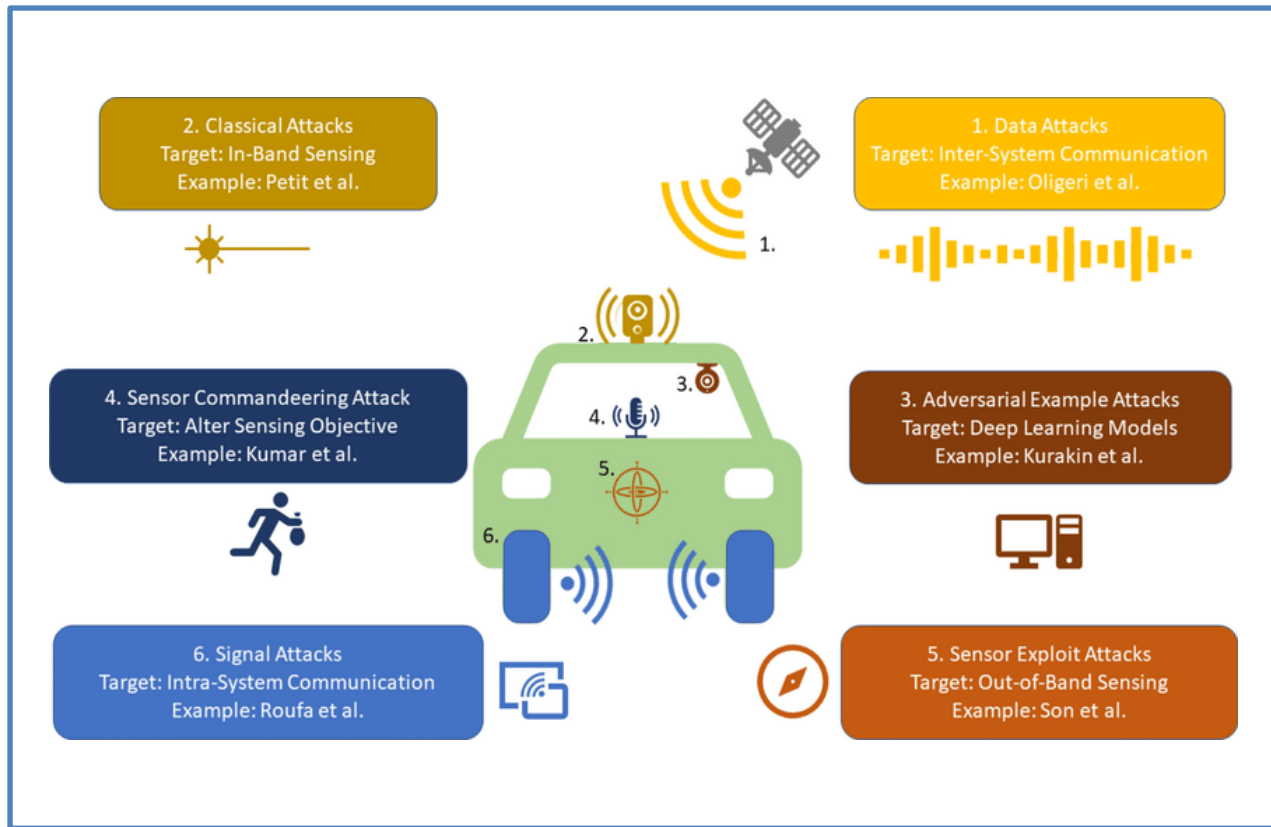


Figure 4. Attack vehicle Autonomous cited from [57].

Table 1. Summary of Attack Vectors and their Attack Type

Attack Vector	Attack Type	Reference
Camera-Based Perception	Adversarial ML attacks on visual scenes	[31]
	Physical AML via adversarial stickers/patches on stop signs	[32]
	Projection attacks using adversarial patterns	[33]
	Blinding attacks with high-intensity lasers/LEDs	[34]
LiDAR Systems	Spoofing with phantom objects	[35]
	Jamming with high-intensity laser signals	[36]
Radar Systems	Spoofing with false radar signals	[37]
	Jamming by broadcasting noise/interference	[38]
GPS/GNSS Systems	Jamming by transmitting radio noise	[39]
	Spoofing with counterfeit GPS-like signals	[40]
Sensor Fusion Systems	Feeding conflicting/manipulated data into fusion algorithms	[41, 42]
V2X Communication	Message Injection/Spoofing (e.g., false BSMs, CAMs, DENMs)	[44, 45]
	Message Modification via intercepted and altered messages	[43]
	Message Replay attacks with captured and retransmitted messages	[46]
	Sybil Attacks creating numerous fake identities	[48]
	Message Replay attacks with captured and retransmitted messages	[46]
	Sybil Attacks creating numerous fake identities	[48]
Machine Learning Models	Evasion attacks causing incorrect predictions	[52]
	Poisoning attacks injecting malicious data into training datasets	[53, 54]
	Model Inversion attacks inferring sensitive training data	[55]
	Model Extraction attacks stealing model architecture and parameters	[56]

CAN bus attacks include [58]:

- **Message Injection:** Broadcasting forged messages to control specific vehicle functions (e.g., spoofing speed sensor data to affect cruise control, injecting fake steering commands).
- **Denial-of-Service (DoS):** Flooding the bus with messages to consume bandwidth and prevent legitimate ECUs from communicating, potentially freezing the vehicle's state or triggering limp-home modes.
- **Message Modification/Suppression:** While harder remotely, physical access or ECU compromise allows modifying or suppressing legitimate messages by exploiting the bus's collision resolution mechanism, when available.

Reverse engineering the CAN bus protocol to understand message IDs and data formats for specific vehicle models is a prerequisite for crafting targeted attacks [59].

Automotive Ethernet and free Wi-Fi, increasingly used for high-bandwidth communications (e.g., camera data, infotainment, and diagnostics) and as a backbone network, introduces IP-based vulnerabilities familiar from traditional IT networks. This includes potential for IP spoofing, port scanning, denial-of-service floods, and exploits targeting network services or connected devices [60]. Segmentation and firewalling are crucial, but must be carefully implemented to avoid introducing safety risks or hindering necessary communication.

ECU Attacks can be achieved through various mechanisms [61]:

- **Firmware Hacking:** Identifying vulnerabilities in ECU firmware allows attackers to compromise or replace it with malicious code, gaining persistent control over the hardware and the functions it manages.
- **Unauthorized Access:** Exploits can target software vulnerabilities in external interfaces like the OBD-II port, USB ports, Wi-Fi/Bluetooth modules, or cellular connectivity. Vulnerable infotainment systems or telematics units, being more connected to the outside world, often serve as entry points to pivot deeper into the vehicle network.
- **Side-Channel Attacks:** Analyzing physical properties like power consumption, electromagnetic emissions, or timing of operations can reveal cryptographic keys or sensitive data processed by an ECU.

A successful ECU compromise can allow an attacker to bypass security measures, control safety-critical functions (steering, braking, engine management), extract sensitive data, or install persistent backdoors.

4.1 Data Privacy Threats

Autonomous vehicles are prodigious data collectors, continuously gathering vast amounts of information about their environment, occupants, and operation. This data, while essential for autonomous function and potential service improvements, simultaneously presents significant privacy risks if not handled securely and responsibly. The data lifecycle—spanning collection, storage, processing, transmission, and sharing—introduces multiple vulnerability points [62]. Location data is inherently sensitive, detailing routes traveled, destinations, and frequency of visits to specific locations (e.g., home, work, medical facilities, and even a variety of private life environments). Tracking this data, potentially aggregated over time, allows for profiling individuals' activities, habits, and lifestyles. Sophisticated analysis could infer sensitive information about health conditions (e.g., malicious access to wearable devices recording a vast array of biological functions), social connections, affiliations, and intimate social relationships.

Driving behavior data, including speed, acceleration, braking patterns, and maneuvering style, can reveal personality traits, stress levels, or even potential medical conditions affecting driving ability. This data is valuable for insurance companies and mobility service providers, but poses privacy risks if shared without explicit consent or adequate anonymization. Sensor data can capture personally identifiable information (PII) from the environment. Camera data might record faces of pedestrians, license plates of other vehicles, or details visible through windows. LiDAR point clouds could, in some cases, reveal identifiable shapes. Combining this external data with internal vehicle information exacerbates the privacy risk. In-vehicle infotainment (IVI) systems and connected mobile devices synchronized with the vehicle can expose contacts, call logs, message histories, and contacts, streaming service usage, and browsing history. The compromise of the IVI system serves as a direct pipeline to this sensitive personal information. Cloud storage and processing of AV data, often used for data analytics, model training, and remote diagnostics, presents traditional cloud security and privacy concerns. Data breaches, insecure APIs, or inadequate access controls in cloud infrastructure managing AV data repositories could expose sensitive personal and vehicle information [63].

The risks are amplified by the potential for data brokerage and sharing with numerous third parties—manufacturers, service providers, employers, insurance companies, infrastructure operators, and even governments. Without strong privacy-preserving mechanisms and clear policies, this data could be used for targeted advertising, discriminatory practices, or

surveillance. Regulatory frameworks like GDPR in Europe and CCPA in California impose stringent requirements on data handling and necessitate explicit user consent, but technical solutions are required to ensure compliance and robust protection against breaches [64, 65]. Ethical considerations surrounding pervasive data collection and the potential for surveillance capabilities inherent in AV technology also warrant serious attention [66].

5. Defense Mechanisms and Mitigation Strategies

Countering the diverse threat landscape necessitates a multi-layered, defense-in-depth approach, integrating security considerations at every stage of the autonomous vehicle's design, development, and operation. Mitigation strategies range from bolstering the security of individual components to implementing system-wide architectural safeguards and privacy-preserving techniques.

5.1 Secure Sensor Data Processing and Fusion

Defending against sensor attacks involves validating incoming data, detecting anomalies, and building resilience into perception algorithms. Anomaly Detection techniques applied to sensor data streams can identify patterns deviating from expected behavior, potentially flagging spoofed or jammed inputs. Statistical methods monitor data distributions, while machine learning-based approaches learn normal sensor characteristics to spot outliers [67]. Data Validation and Redundancy exploit the availability of multiple sensors. By cross-checking data from heterogeneous sensors (e.g., comparing LiDAR distance measurements with camera-based object size and radar velocity), the system can identify inconsistencies indicative of a sensor compromise [68]. Physical redundancy (multiple sensors of the same type) and analytical redundancy (using models of vehicle dynamics or environmental physics to predict expected sensor readings) provide further validation capabilities [69]. Making ML Models Robust to adversarial examples is an active research area. Adversarial training involves augmenting the training data with adversarial examples to make the model more resilient [70]. Defensive distillation trains a second model on the softened outputs of a first model, reducing the gradients and making the model harder to attack [71]. Input sanitization techniques attempt to detect or filter out adversarial perturbations in the input data before it reaches the ML model. Runtime monitoring observes the internal states or outputs of the ML model during inference to detect suspicious behavior that might indicate an adversarial input, even if the final output is superficially plausible [72]. However, achieving robust ML in complex, high-dimensional spaces remains a significant challenge. Using certified robustness techniques aims to provide mathematical guarantees about a model's resistance to bounded adversarial perturbations [73].

5.2 Secure Vehicle-to-Everything (V2X) Communication

Securing V2X communication primarily relies on robust cryptographic mechanisms and trusted management systems. The Security Credential Management System (SCMS) provides a PKI framework for managing certificates used to authenticate V2X messages [43]. Vehicles and infrastructure units receive short-lived, privacy-preserving pseudonymous certificates that change frequently, preventing long-term tracking while enabling message authentication and integrity checks. Digital signatures (e.g., using ECDSA as specified in IEEE 1609.2) are appended to V2X messages, allowing receiving entities to verify the sender's identity and ensure the message has not been tampered with in transit [28].

Implementing Intrusion Detection Systems (IDS) specific to V2X traffic can help identify malicious activity [43]. Anomaly-based V2X IDS can detect unusual patterns in message frequency, origin distribution (Sybil attacks), or content inconsistency (spoofed data contradicting other sources). Reputation systems where vehicles share information about potentially malicious senders can also contribute to filtering out untrustworthy messages [74].

Defending against GPS spoofing in the context of V2X often involves integrating GPS data with other localization sources. Secure Positioning techniques utilize sensor fusion combining GNSS readings with IMU data, wheel odometry, LiDAR/camera-based SLAM (Simultaneous Localization and Mapping), and potentially V2X messages from trusted sources to maintain an accurate and robust position estimate that is less susceptible to manipulation of a single source [75]. Anomaly detection on GNSS signals themselves (e.g., checking signal strength, consistency across satellites) also plays a role.

5.3 Robust Machine Learning for AVs

Beyond perception robustness, securing ML models involves protecting the data they are trained on and ensuring their integrity and predictable behavior. Secure Training Data Management practices are essential to prevent poisoning attacks.

This includes rigorous data validation, provenance tracking, and potentially distributed or privacy-preserving training methods [76].

Techniques to enhance Adversarial Robustness (discussed in sensor security) apply broadly to any ML component in the AV. This includes training defenses, but also exploring different model architectures (e.g., using ensembles or alternative activation functions) that might exhibit greater inherent robustness. Runtime Monitoring of ML models during operation is crucial, employing techniques that go beyond simple output validation to check for internal consistency, unexpected activation patterns, or divergence from trusted models.

Explainable AI (XAI) research, while primarily aimed at improving transparency and trust in AI decisions, can indirectly aid security by providing insights into why a model made a particular decision, potentially highlighting instances where it relied on suspicious or unusual features that might indicate adversarial manipulation or data poisoning [77]. If an AV needs to brake suddenly due to an object detection, an XAI component could explain which visual features triggered the detection, allowing for post-incident analysis or even real-time validation.

5.4 In-Vehicle Network Security

Protecting the internal vehicle network, particularly the vulnerable CAN bus, is paramount. Intrusion Detection Systems (IDS) are widely researched for automotive networks [78]. CAN IDS can be deployed within individual ECUs, at gateways connecting different network segments, or on a central security module. Approaches include:

- Signature-based IDS: Detecting known malicious message patterns or sequences.
- Anomaly-based IDS: Learning normal traffic patterns (timing, frequency, message content) and flagging deviations. Machine learning techniques are frequently employed here [79].
- Specification-based IDS: Defining rules based on the expected behavior and message flow of specific ECUs and flagging any violation [80]. This requires precise knowledge of the network's intended operation.

Challenges for CAN IDS include the high data rate, real-time requirements (detection must be fast enough to prevent harm), and the difficulty of deploying and updating detection logic across numerous resource-constrained ECUs.

Network Segmentation divides the vehicle network into isolated zones (e.g., safety-critical, infotainment, powertrain) connected via secure gateways. Firewalls or security policies enforced by gateways restrict communication between zones, limiting the lateral movement of an attacker who has compromised one segment [81] (e.g., preventing a compromised infotainment system from sending commands to the braking system).

Implementing Cryptography on CAN is challenging due to its bandwidth limitations and real-time constraints. However, research explores adding lightweight message authentication codes (MACs) or even partial encryption to critical messages [82]. Concepts like "CAN Bus Guardians" are proposed, which are hardware components positioned on the bus to enforce security policies and filter unauthorized messages [24]. Secure Boot mechanisms ensure that only trusted, cryptographically signed software and firmware are loaded and executed when the vehicle starts [83]. Secure Firmware Over-the-Air (FOTA) Updates are essential for patching vulnerabilities and deploying new features, but the update process itself must be secured against tampering or malicious injection [84]. This involves encrypted and authenticated update packages and secure update delivery channels. Access Control Mechanisms within ECUs and at the network level restrict which entities can send or receive specific messages or access certain functions based on predefined policies and identities.

5.5 Hardware-Based Security Modules (HSMs)

Anchoring security in hardware provides a critical root of trust. Hardware Security Modules (HSMs) or Secure Elements are dedicated, tamper-resistant microcontrollers designed to perform cryptographic operations securely and store sensitive keys [85]. They can manage certificates, perform digital signing and verification, and execute cryptographic algorithms in isolation from the main processor, protecting keys from software attacks.

Trusted Platform Modules (TPMs), standardized hardware components, provide secure storage for cryptographic keys and can measure and attest to the integrity of the system's software stack from boot-up onwards [86]. By verifying the boot process and software components, a TPM helps ensure that the system is running in a known, trusted state before critical functions are enabled. These hardware roots of trust are fundamental building blocks for implementing secure boot, managing cryptographic identities, and enabling secure communication channels within and outside the vehicle.

5.6 Privacy-Preserving Architectures and Techniques

Protecting the vast amounts of data collected by AVs requires specific architectural considerations and privacy-enhancing technologies. Data Minimization is a foundational principle, advocating for collecting only the data strictly necessary for a specific function and deleting it when no longer required [87].

Differential Privacy provides a mathematical guarantee that the inclusion or exclusion of any single individual's data does not significantly affect the outcome of a query or analysis, thus protecting individual privacy while allowing aggregation [88]. Noise is intentionally added to the data or query results, calibrated to the sensitivity of the information. Applying differential privacy to AV data can allow manufacturers or researchers to analyze driving patterns or train models without compromising the privacy of individual drivers [89].

Homomorphic Encryption allows computation to be performed directly on encrypted data without decrypting it [90]. While computationally intensive, advancements are making it more feasible for specific applications, enabling processing of sensitive AV data (e.g., biometric data) in untrusted environments like the cloud while maintaining confidentiality [91]. Secure Multi-Party Computation (SMPC) enables multiple parties to jointly compute a function on their respective inputs without revealing the inputs to each other [92]. This could potentially be used for collaborative data analysis or training ML models among different entities (e.g., multiple vehicle manufacturers) without sharing raw data.

Local Differential Privacy (LDP) applies perturbations to data *before* it leaves the vehicle, offering stronger privacy guarantees as sensitive data is not shared even with the data collector [93]. This could be applicable for collecting statistics about vehicle usage or sensor performance. Implementing transparent Privacy Policies and robust User Consent Management mechanisms is crucial, giving occupants control over how their data is collected, used, and shared [94]. Technical solutions must underpin these policies to enforce user preferences.

5.7 Overall System Security Engineering

Ensuring comprehensive security requires integrating it into the entire vehicle development lifecycle, not treating it as an afterthought. Threat Modeling and Risk Assessment should be conducted early and iteratively, identifying potential vulnerabilities and attack paths for different system components and scenarios [95]. This informs design decisions to mitigate risks proactively.

Employing Secure Coding Practices and conducting rigorous Security Testing (including penetration testing, fuzzing, and vulnerability scanning) are fundamental for identifying and remediating software flaws [58, 96]. Formal verification techniques can provide mathematical proof of correctness for critical security properties of isolated components or protocols [97].

Establishing a Secure Development Lifecycle (SDL) for all software and hardware components ensures security requirements are defined, implemented, and verified at each phase. Given the complex supply chains in automotive manufacturing, ensuring Supply Chain Security is also vital; components and software sourced from third parties must meet stringent security standards and be free of known vulnerabilities or backdoors [98]. Table II summarizes and compares the literature according to their defense mechanisms.

Defense Area	Techniques	Strengths	Limitations
Sensor Data Processing and Fusion	Sensor Data Processing and Fusion	Sensor Data Processing and Fusion	Sensor Data Processing and Fusion
Machine Learning Robustness	Adversarial Training [70]; Defensive Distillation	Enhances model resilience; Provides formal guarantees	Potential trade-off with model accuracy; Computational overhead
V2X Communication Security	Security Credential Management System (SCMS) [43]; Digital Signatures [28]; Intrusion Detection Systems (IDS) [74]; Secure Positioning [75]	Ensures message authenticity; Detects malicious activities	Certificate management complexity; Vulnerable to advanced spoofing attacks
In-Vehicle Network Security	Intrusion Detection Systems (IDS) [78];	Protects internal communications;	Limited by CAN bus constraints;

	Network Segmentation [81]; Cryptographic Measures [82]; Secure Boot and Firmware Updates [83, 84]	Prevents unauthorized access	Implementation complexity
Hardware-Based Security Modules	Hardware Security Modules (HSMs) [85]; Trusted Platform Modules (TPMs) [86]	Provides root of trust; Secure key storage	Additional hardware costs; Integration challenges
Privacy-Preserving Techniques	Data Minimization [87]; Differential Privacy [88, 89]; Homomorphic Encryption [90, 91]; Secure Multi-Party Computation (SMPC) [92]; Local Differential Privacy (LDP) [93]	Enhances user privacy; Enables secure data analysis	Computationally intensive; Potential impact on data utility
System Security Engineering	Threat Modeling and Risk Assessment [95]; Secure Coding Practices [58]; Security Testing [96]; Formal Verification [97]; Supply Chain Security [98]	Proactive vulnerability mitigation; Ensures software integrity	Requires continuous updates; Coordination across supply chain

6. Key Challenges and Open Issues

Despite significant research and development efforts, several critical challenges persist in achieving truly secure and privacy-preserving autonomous vehicles, requiring sustained focus from researchers and industry practitioners.

The sheer Complexity and Scale of autonomous systems present a monumental security challenge. Integrating millions of lines of code, numerous interconnected ECUs from multiple vendors, diverse sensor modalities, and complex ML models creates an enormous attack surface with countless potential interaction points and vulnerabilities. Understanding and securing every possible state and interaction within such a system is exceedingly difficult [99]. Meeting Real-Time Constraints simultaneously with robust security is a non-trivial task. Security mechanisms, such as encryption, authentication, or complex anomaly detection, often introduce computational overhead and latency. These must be carefully designed and optimized to avoid interfering with safety-critical operations that demand millisecond-level response times [24]. Balancing security efficacy with performance requirements remains a constant tension. The Heterogeneity and Integration of components from a wide array of suppliers, each with varying security expertise and development processes, introduces integration risks. Ensuring secure interfaces and trusted interactions between components developed by different entities is crucial but challenging to standardize and verify across the entire system lifecycle [100].

The Evolving Threat Landscape means security cannot be a one-time fix. Attackers continuously develop new techniques, exploit previously unknown vulnerabilities (zero-days), and adapt their methods based on deployed defenses. Autonomous vehicles must be designed with mechanisms for continuous monitoring, remote patching (secure FOTA updates), and adaptation to new threats throughout their long operational lifespan. Testing and Validation of security and privacy properties pose significant difficulties. Demonstrating that a complex, learning-enabled cyber-physical system is free from critical vulnerabilities or resilient to unforeseen attacks is exceptionally hard. Exhaustive testing of all possible attack scenarios, especially those involving sophisticated coordination across different system layers or physical environment manipulation (e.g., coordinated sensor spoofing and V2X injection), is practically impossible in simulation or on test tracks

[101]. Developing effective security testing methodologies and benchmarks specific to AVs is an urgent need. Ensuring the security of Over-the-Air (OTA) Updates is critical, but also represents a potential vulnerability. If the update mechanism is compromised, it could be used to install malicious software on the vehicle fleet, effectively acting as a widespread attack vector [102]. The integrity and authenticity of updates, along with the resilience of the update delivery infrastructure, must be rigorously protected.

The Regulatory and Standardization environment for AV security and privacy is still maturing. While some standards exist (e.g., ISO 21434 for automotive cybersecurity engineering, UNECE WP.29 regulations on cybersecurity and software updates), they provide frameworks rather than specific technical solutions and are not yet universally adopted or sufficiently prescriptive for all aspects of AV security [103, 104]. Harmonizing global standards and regulations to provide clear requirements and testing procedures is an ongoing process. Effectively Balancing Safety, Security, and Privacy can be challenging as these goals may sometimes conflict. For example, logging extensive sensor data might enhance safety analysis after an incident but increases privacy risk. Real-time safety decisions might necessitate quickly trusting sensor inputs, even if they could potentially be spoofed, if verification would introduce dangerous latency. Optimal trade-offs must be carefully considered based on rigorous risk assessment. Ultimately, ensuring Public Trust and Acceptance is paramount. A single, highly publicized security incident involving an autonomous vehicle could severely damage public confidence in the technology, hindering its deployment and adoption [105, 106]. Building trustworthy systems is not just a technical challenge but also a social one. Developing robust Incident Response and Forensics capabilities tailored to the complexity and distributed nature of AV systems is also critical. Detecting, containing, analyzing, and learning from security incidents in a timely manner across a fleet of vehicles presents significant technical and logistical hurdles [107].

7. Future Research Directions

Addressing the multifaceted security and privacy challenges facing autonomous vehicles necessitates continued research across various domains. Identifying promising avenues for future work is crucial for building the next generation of resilient and trustworthy AV systems. A fundamental shift towards Proactive Security Design is essential. Rather than treating security as an add-on, it must be integrated using security-by-design and privacy-by-design principles from the initial concept phase through development, testing, and deployment [95, 66]. Future research should focus on developing comprehensive methodologies and tools that enable engineers to systematically incorporate security and privacy requirements into complex cyber-physical system architectures, considering the unique constraints of the automotive environment. Leveraging AI/ML for Security holds significant promise. While ML models are targets of attack, they can also be powerful tools for defense. Future work could explore advanced ML techniques for more sophisticated intrusion detection systems within the vehicle network, across V2X communication channels, and analyzing sensor data for anomalies [79, 67]. Predictive security analysis using AI, anticipating potential attack vectors based on system design and environmental context, represents another compelling direction. Simultaneously, research must continue to focus on securing AI/ML Itself. Developing more inherently robust and interpretable ML models that are less susceptible to adversarial manipulation remains a critical need [73, 77]. Exploring novel architectural designs, training methodologies resilient to poisoning, and effective runtime monitoring and verification techniques for ML models are vital areas for future investigation. The intersection of ML security and formal methods to provide guarantees about AI behavior in safety-critical contexts is also a promising frontier [73].

Developing Cross-Layer Security solutions that consider the interactions and dependencies between different AV system layers is crucial. An attack on one layer (e.g., sensor) might be detected or mitigated by defenses in another (e.g., planning or control). Research is needed on how to design coordinated defenses that share information and respond cohesively to complex, multi-stage attacks [4]. This involves understanding how vulnerabilities propagate across the architecture.

Focusing on Resilience and Fault Tolerance from a security perspective is paramount. Autonomous systems should be designed to operate safely even when components are compromised. Future research could explore architectures and control strategies that allow the vehicle to detect a compromise, isolate the affected component, and degrade gracefully or enter a minimal risk condition rather than failing catastrophically [99]. Applying Formal Verification and Model Checking to critical AV components and security protocols can provide high assurance guarantees. While challenging for complex systems, applying these rigorous mathematical methods to security-sensitive code or protocols (e.g., secure boot, V2X message authentication) can help identify flaws that might be missed by testing [97]. Scaling these techniques to the complexity of AV systems is an open research challenge.

Exploring the potential application of Blockchain and Distributed Ledger Technologies (DLT) for specific AV security challenges is an emerging area. DLT could potentially be used for secure and transparent management of software updates,

identity management for V2X participants, or ensuring the integrity of data shared between parties [108]. However, research must address the significant overhead, latency, and scalability challenges inherent in DLT for real-time automotive applications. Preparing for the threat posed by future Quantum Computing is necessary. Quantum computers could break current public-key cryptography (like RSA and ECC) used in V2X security and secure updates [109]. Research into Post-Quantum Cryptography (PQC) algorithms suitable for the performance and resource constraints of automotive ECUs is vital to future-proof AV security [110]. Considering Human Factors in AV Security is also important. Occupants or nearby pedestrians are part of the AV ecosystem and could potentially be attack vectors (e.g., introducing malicious devices via USB ports) or aids to security (e.g., anomaly reporting via a user interface). Research into secure human-machine interfaces (HMIs), occupant awareness of security status, and secure interaction design is needed [111].

8. Conclusion and Future Work

Autonomous driving technology stands poised to redefine transportation, promising substantial societal benefits. This review has underscored that realizing this transformative potential hinges critically on establishing a robust security and privacy foundation. The exploration of the threat landscape reveals a complex web of vulnerabilities inherent in the intricate interplay of sensor perception, V2X communication, machine learning models, and internal control systems. Attacks ranging from sophisticated adversarial manipulations and deceptive spoofing to fundamental network exploitation and pervasive data breaches pose significant risks to safety, functionality, and user privacy. While existing defense mechanisms—including intrusion detection systems, secure communication protocols, hardware-based security modules, and privacy-preserving techniques—offer crucial layers of protection, their effectiveness is challenged by the inherent complexities and dynamic nature of autonomous systems. The review highlights that no single defense strategy is sufficient; a holistic, multi-layered approach integrating security and privacy considerations throughout the system's lifecycle is imperative. Significant challenges persist, including managing system complexity, balancing security with real-time performance, addressing the heterogeneity of components, adapting to an evolving threat landscape, and establishing comprehensive testing and validation methodologies. Overcoming these hurdles requires sustained research and collaborative efforts across academia, industry, and regulatory bodies. Looking ahead, future research must prioritize proactive security-by-design principles, leverage AI for both defense and understanding adversarial tactics, enhance the robustness of the AI components themselves, and develop cross-layer defenses that account for system-wide interactions. Investigating resilience architectures, applying formal verification methods, exploring nascent technologies like blockchain and post-quantum cryptography, and understanding the human element in AV security are also critical directions. The development of standardized benchmarks and testing procedures will be essential for advancing the state of the art and ensuring compliance. In conclusion, securing autonomous vehicles against cyber and privacy threats is not merely a technical challenge; it is a fundamental prerequisite for earning public trust and enabling the safe and widespread adoption of this revolutionary technology. Continued dedication to rigorous research, collaborative development, and the establishment of effective standards and regulations will pave the way for a secure and trustworthy autonomous future.

Corresponding author

Dr. Qais Al-Na'amneh

q_naamneh@asu.edu.jo

Acknowledgements

Not applicable.

Funding

No funding.

Contributions

G.L; and M.A; Conceptualization, Q.A; and R.H; Investigation, L.D.D Writing (Original Draft), G.L; M.A; Q.A; R.H; and L.D.D Writing (Review and Editing) Supervision, G.L; M.A; Q.A; R.H; and L.D.D Project Administration.

Ethics declarations

This article does not contain any studies with human participants or animals performed by any of the authors.

Consent for publication

Not applicable.

Competing interests

The author declares no competing interests.

References

- [1] David Bissell, Thomas Birtchnell, Anthony Elliot, and Eric L Hsu. Autonomous automobiles: the social impacts of driverless vehicles. *Current Sociology*, 68(1):116–134, 2020.
- [2] Mohammad Aljaidi, Ayoub Alsarhan, Dimah Al-Fraihat, Ahmed Al-Arjan, Bashar Igried, Subhieh M El-Salhi, Muhammad Khalid, and Qais Al-Na’amneh. Cybersecurity threats in the era of ai: Detection of phishing domains through classification rules. In *2023 2nd International Engineering Conference on Electrical, Energy, and Artificial Intelligence (EICEEI)*, pages 1–6. IEEE, 2023.
- [3] Shatha Ali, Mohammad Alshinwan, Osama A Khashan, Mohammad Hijjawi, Arar Altawil, Qais AlNa’amneh, Hazem Abu-Adaiq, Hanan Alhardan, Diaa Salama Abdelminaam, Omar Tarawneh, et al. Intrusion detection for wireless sensor networks using parrot algorithm. In *Machine Intelligence Applications in Cyber-Risk Management*, pages 345–366. IGI Global Scientific Publishing, 2025.
- [4] Qais Al-Na’amneh, Mohammad Aljaidi, Ahmad Nasayreh, Hasan Gharaibeh, Rabia Emhamed Al Mamlook, Ameera S Jaradat, Ayoub Alsarhan, and Ghassan Samara. Enhancing iot device security: Cnn-svm hybrid approach for real-time detection of dos and ddos attacks. *Journal of Intelligent Systems*, 33(1):20230150, 2024.
- [5] Qais Al-Na’amneh, Walid Dhifallah, Rahaf Hazaymih, Laith Alzboon, Ayoub Alsarhan, Mohammed Alshinwan, and Rabia Emhamed Al Mamlook. Analysis for detection and mitigation of version number modification attack in the internet of things. 2025.
- [6] Qais Al-Na’amneh, Walid Dhifallah, Rahaf Hazaymih, Mohammed Amin Almaiah, Asalla Alsheyab, Mohammad Alshinwan, and Braa Qadoumi. Dis flooding attack impact in rpl-based 6lowpan network. In *Machine Intelligence Applications in Cyber-Risk Management*, pages 69–84. IGI Global Scientific Publishing, 2025.
- [7] Qais Al-Na’amneh, Mahmoud Aljawarneh, and Rahaf Hazaymih. A framework for insider threat detection using role-based profile assessment and threshold. In *Utilizing AI in Network and Mobile Security for Threat Detection and Prevention*, pages 97–114. IGI Global Scientific Publishing, 2025.
- [8] Qais Al-Na’amneh, Mahmoud Aljawarneh, Rahaf Hazaymih, and Rabia Emhamed Al Mamlook. Ethical issues in cyber-security for autonomous vehicles (av) and automated driving: A comprehensive review. *Utilizing AI in Network and Mobile Security for Threat Detection and Prevention*, pages 173–196, 2025.
- [9] Amani Abu-Zaid, Mohammad Aljaidi, Qais Al-Na’amneh, Ghassan Samara, Ayoub Alsarhan, and Braa Qadoumi. Advancements and challenges in the internet of drones security issues: A comprehensive review. *Machine Intelligence Applications in Cyber-Risk Management*, pages 1–24, 2025.
- [10] Liyang Li, Guangsheng Wang, Yuan Zhang, Yujiao Cao, Jian Wang, and Zhiwei Luo. Personalized federated learning scheme for autonomous driving based on correlated differential privacy. *Sensors*, 21(1):178, 2021.
- [11] Scott Drew Pendleton, Hans Andersen, Xinxin Du, Xiaotong Shen, Malika Meghjani, You Hong Eng, Daniela Rus, and Marcelo H Ang. Perception, planning, control, and coordination for autonomous vehicles. *Machines*, 5(1):6, 2017.
- [12] Daniel Bastos, Paulo P Monteiro, Arnaldo SR Oliveira, and Miguel V Drummond. An overview of lidar requirements and techniques for autonomous driving. In *2021 Telecoms Conference (ConfTELE)*, pages 1–6. IEEE, 2021.
- [13] Xiaolin Tang, Kai Yang, Hong Wang, Jiahang Wu, Yechen Qin, Wenhao Yu, and Dongpu Cao. Prediction-uncertainty-aware decision-making for autonomous vehicles. *IEEE Transactions on Intelligent Vehicles*, 7(4):849–862, 2022.
- [14] David Arthur, Christopher Becker, Alex Epstein, Bill Uhl, Scott Ranville, A John, et al. Foundations of automotive software. Technical report, United States. Department of Transportation. National Highway Traffic Safety ..., 2022.
- [15] Alessandro De Dominica, Marco De Vincenzi, Roberto Lazzarotti, Fabio Martinelli, and Iaria Matteucci. A systematic review of security issues in automotive ethernet. *ACM Computing Surveys*, 56(6):1–38, 2024.
- [16] ETSI. Intelligent transport systems (its); security; electronic communications highway (ech); security header and certificate formats. Technical report, ETSI, 2021. Available from ETSI, Accessed: April 2025.
- [17] Liyang Chen, Yun Chen, Xiang Li, Hongwei Deng, Yiyang Luo, Jian Zhang, Guang Zeng, Lin Xu, and Tao Luo. A comprehensive review of cybersecurity threats and solutions in autonomous driving systems. *Electronics*, 13(3):588, 2024.
- [18] Amira Guesmi, Muhammad Abdullah Hanif, Bassem Ouni, and Muhammad Shafique. Physical adversarial attacks for camera-based smart systems: Current trends, categorization, applications, research challenges, and future outlook. *IEEE Access*, 11:109617–109668, 2023.
- [19] Amira Guesmi and Muhammad Shafique. Navigating threats: A survey of physical adversarial attacks on lidar perception systems in autonomous vehicles. *arXiv preprint arXiv:2409.20426*, 2024.

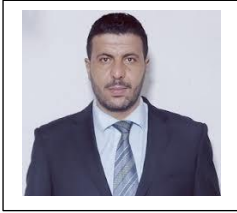
- [20] Muhammad Asif Khan, Hamid Menouar, Mohamed Abdallah, and Adnan Abu-Dayya. Lidar in connected and autonomous vehicles-perception, threat model, and defense. *IEEE Transactions on Intelligent Vehicles*, 2024.
- [21] Wahab Ali Gulzar Khawaja. A survey on radar techniques for detection, tracking, and classification of aerial threats. *Authorea Preprints*, 2023.
- [22] Yu Pan, Didi Xie, Yurui Zhao, Xiang Wang, and Zhitao Huang. Overview of radar jamming waveform design. *Remote Sensing*, 17(7):1218, 2025.
- [23] Sagar Dasgupta, Abdullah Ahmed, Mizanur Rahman, and Thejesh N Bandi. Unveiling the stealthy threat: Analyzing slow drift gps spoofing attacks for autonomous vehicles in urban environments and enabling the resilience. *arXiv preprint arXiv:2401.01394*, 2024.
- [24] Zhen Yang, Jun Ying, Junjie Shen, Yiheng Feng, Qi Alfred Chen, Z Morley Mao, and Henry X Liu. Anomaly detection against gps spoofing attacks on connected and autonomous vehicles using learning from demonstration. *IEEE Transactions on Intelligent Transportation Systems*, 24(9):9462–9475, 2023.
- [25] Yi Zhu, Chenglin Miao, Hongfei Xue, Yunnan Yu, Lu Su, and Chunming Qiao. Malicious attacks against multi-sensor fusion in autonomous driving. In *Proceedings of the 30th Annual International Conference on Mobile Computing and Networking*, pages 436–451, 2024.
- [26] Ziyuan Zhong, Zhisheng Hu, Shengjian Guo, Xinyang Zhang, Zhenyu Zhong, and Baishakhi Ray. Detecting multi-sensor fusion errors in advanced driver-assistance systems. In *proceedings of the 31st ACM SIGSOFT International Symposium on Software Testing and Analysis*, pages 493–505, 2022.
- [27] Alessandro Giaccaglini. *Implementing secured messages for V2X communication*. PhD thesis, Politecnico di Torino, 2024.
- [28] Xiaoya Xu, Yunpeng Wang, and Pengcheng Wang. Comprehensive review on misbehavior detection for vehicular ad hoc networks. *Journal of Advanced Transportation*, 2022(1):4725805, 2022.
- [29] Peng-Yong Kong. A survey of cyberattack countermeasures for unmanned aerial vehicles. *IEEE Access*, 9:148244–148263, 2021.
- [30] Anastasios Giannaros, Aristeidis Karras, Leonidas Theodorakopoulos, Christos Karras, Panagiotis Kranias, Nikolaos Schizas, Gerasimos Kalogeratos, and Dimitrios Tsolis. Autonomous vehicles: Sophisticated attacks, safety issues, challenges, open topics, blockchain, and future directions. *Journal of Cybersecurity and Privacy*, 3(3):493–543, 2023.
- [31] Yunpeng Zhang, Bidit Das, and Fengxiang Qiao. Sybil attack detection and prevention in vanets: A survey. In *Proceedings of the Future Technologies Conference (FTC) 2020, Volume 3*, pages 762–779. Springer, 2021.
- [32] Wonjin Chung, Jungsub Ahn, and Taeho Cho. Mitm attack detection scheme using monitoring information in v2x communication. In *2023 9th International Conference on Computer and Communications (ICCC)*, pages 1257–1261. IEEE, 2023.
- [33] Aseel Alshuaibi, Mohammed Almaayah, and Aitizaz Ali. Machine learning for cybersecurity issues: A systematic review. *Journal of Cyber Security and Risk Auditing*, 2025(1):36–46, 2025.
- [34] Mozghan Pourkeshavarz, Mohammad Sabokrou, and Amir Rasouli. Adversarial backdoor attack by naturalistic data poisoning on trajectory prediction in autonomous driving. In *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition*, pages 14885–14894, 2024.
- [35] Jiacheng Liang, Ren Pang, Changjiang Li, and Ting Wang. Model extraction attacks revisited. In *Proceedings of the 19th ACM Asia Conference on Computer and Communications Security*, pages 1231–1245, 2024.
- [36] Max Panoff, Raj Gautam Dutta, Yaodan Hu, Kaichen Yang, and Yier Jin. On sensor security in the era of iot and cps. *SN Computer Science*, 2(1):51, 2021.
- [37] Christian Szegedy, Wojciech Zaremba, Ilya Sutskever, Joan Bruna, Dumitru Erhan, Ian Goodfellow, and Rob Fergus. Intriguing properties of neural networks. *arXiv preprint arXiv:1312.6199*, 2013.
- [38] Kevin Eykholt, Ivan Evtimov, Earlene Fernandes, Bo Li, Amir Rahmati, Chaowei Xiao, Atul Prakash, Tadayoshi Kohno, and Dawn Song. Robust physical-world attacks on deep learning visual classification. In *Proceedings of the IEEE conference on computer vision and pattern recognition*, pages 1625–1634, 2018.
- [39] Wei Jiang, Tianyuan Zhang, Shuangcheng Liu, Weiye Ji, Zichao Zhang, and Gang Xiao. Exploring the physical-world adversarial robustness of vehicle detection. *Electronics*, 12(18):3921, 2023.
- [40] Erasmo Notaro. *Simulating Malicious Attacks on VANETs for Connected and Autonomous Vehicles*. PhD thesis, Politecnico di Torino, 2023.
- [41] Dudi Biton, Aditi Misra, Efrat Levy, Jaidip Kotak, Ron Bitton, Roei Schuster, Nicolas Papernot, Yuval Elovici, and Ben Nassi. The adversarial implications of variable-time inference. In *Proceedings of the 16th ACM Workshop on Artificial Intelligence and Security*, pages 103–114, 2023.

- [42] Xuejun Zhao, Wencan Zhang, Xiaokui Xiao, and Brian Lim. Exploiting explanations for model inversion attacks. In *Proceedings of the IEEE/CVF international conference on computer vision*, pages 682–692, 2021.
- [43] European Parliament. General Data Protection Regulation (GDPR). Retrieved from <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679>, 2016. [Online, last accessed 20-4-2025].
- [44] California Legislative Information. California consumer privacy act (CCPA). 2018. [Online, last accessed 20-4-2025].
- [45] Hafiz Syahmi. Privacy and ethical implications of big data utilization in public transportation surveillance. *International Journal of Advanced Cybersecurity Systems, Technologies, and Applications*, 9(1):1–10, 2025.
- [46] Igal Bilik. Comparative analysis of radar and lidar technologies for automotive applications. *IEEE Intelligent Transportation Systems Magazine*, 15(1):244–269, 2022.
- [47] Rhea Mehta and Kavita Jhahharia. Layered distillation training: A study of adversarial attacks and defenses. In *2024 3rd International Conference for Innovation in Technology (INOCON)*, pages 1–7. IEEE, 2024.
- [48] Ning Wang, Yimin Chen, Yang Xiao, Yang Hu, Wenjing Lou, and Y Thomas Hou. Manda: On adversarial example detection for network intrusion detection system. *IEEE Transactions on Dependable and Secure Computing*, 20(2):1139–1153, 2022.
- [49] Ida Mirzadeh, Mohammad Sayad Haghighi, and Alireza Jolfaei. Filtering malicious messages by trust-aware cognitive routing in vehicular ad hoc networks. *IEEE Transactions on Intelligent Transportation Systems*, 24(1):1134–1143, 2022.
- [50] Debasis Kumar and Naveed Muhammad. A survey on localization for autonomous vehicles. *IEEE Access*, 11:115865–115883, 2023.
- [51] B Sasikala and Shubham Sachan. Decoding decision-making: embracing explainable ai for trust and transparency. *Exploring the frontiers of artificial intelligence and machine learning technologies*, 42, 2024.
- [52] Nordine Quadar, Abdellah Chehri, Benoit Debaque, Imran Ahmed, and Gwangil Jeon. Intrusion detection systems in automotive ethernet networks: challenges, opportunities and future research trends. *IEEE Internet of Things Magazine*, 7(2):62–68, 2024.
- [53] Dingwang Wang and Subramaniam Ganesan. Automotive network security. In *2021 IEEE International Conference on Electro Information Technology (EIT)*, pages 193–196. IEEE, 2021.
- [54] KY Prashanth and UM Rohitha. Cryptographic method for secure object segmentation for autonomous driving perception systems. *SAE International Journal of Connected and Automated Vehicles*, 8(12-08-01-0008), 2025.
- [55] Omid Avatefipour and Haroon Malik. State-of-the-art survey on in-vehicle network communication “can-bus” security and vulnerabilities. *International Journal of Computer Science and Network*, 6(6):1009–1015, 2018.
- [56] Claudius Pott, Philipp Jungklass, David Jacek Csejka, Thomas Eisenbarth, and Marco Siebert. Firmware security module: A framework for trusted computing in automotive multiprocessors. *Journal of Hardware and Systems Security*, 5(2):103–113, 2021.
- [57] Saad El Jaouhari and Eric Bouvet. Secure firmware over-the-air updates for iot: Survey, challenges, and discussions. *Internet of Things*, 18:100508, 2022.
- [58] Cynthia Dwork. Differential privacy. In *International colloquium on automata, languages, and programming*, pages 1–12. Springer, 2006.
- [59] Rahul Bhadani. A survey on differential privacy for spatiotemporal data in transportation research. *arXiv preprint arXiv:2407.15868*, 2024.
- [60] Chuan Zhao, Shengnan Zhao, Minghao Zhao, Zhenxiang Chen, Chong-Zhi Gao, Hongwei Li, and Yu-an Tan. Secure multi-party computation: theory, practice and applications. *Information Sciences*, 476:357–372, 2019.
- [61] Chehara Pathmabandu, John Grundy, Mohan Baruwat Chhetri, and Zubair Baig. Privacy for iot: informed consent management in smart buildings. *Future Generation Computer Systems*, 145:367–383, 2023.
- [62] Badis Hammi, Sherali Zeadally, and Jamel Nebhen. Security threats, countermeasures, and challenges of digital supply chains. *ACM Computing Surveys*, 55(14s):1–40, 2023.
- [63] ISO/SAE. Road vehicles — cybersecurity engineering. International Organization for Standardization, ISO 21434, 2021. Available: <https://www.iso.org/standard/70918.html>.
- [64] UNECE. Regulation on cybersecurity and cybersecurity management system (un regulation no. 155). United Nations Economic Commission for Europe (UNECE), 2021. Available: <https://www.unece.org/trans/main/wp29/wp29regs.html>.
- [65] Jason Carlton. *Data Privacy in Connected Vehicle Infotainment Systems: A Comprehensive Framework for Rental Vehicles*. PhD thesis, University of Michigan-Dearborn, 2024.

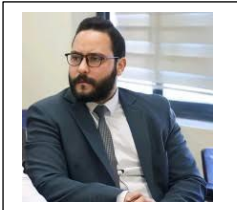
Biographies



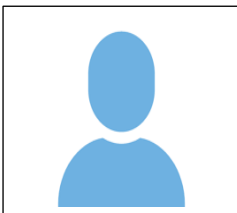
Prof. Giuseppe Lippi was born in Padova (Italy) on October the 4th, 1967. He has taken the degree in Medicine in 1986 and the specialization in Clinical Biochemistry and Laboratory Medicine in 1992. He currently serves as Full Professor of Clinical Biochemistry at the University of Verona (Italy) and director of the clinical chemistry and haematology laboratories of the University Hospital of Verona (Italy). The main areas of research include pre-analytical variability, analytical and clinical validation of biomarkers, metabolism of lipoproteins and relevant assay methods, diagnosis and management of disorders of haemostasis and thrombosis, COVID-19. giuseppe.lippi@univr.it



Dr. Mahmoud Mohammad Aljawarneh. Received the B.S., M.S. and PhD degree in Information Technology from University of Sindh, Jamshoro, Pakistan, in 2011, 2014, and 2019 respectively. From 2012 to 2014 and 2016 to 2018, he was a Research Assistant with the Institute of Information and Communication Technology, University of Sindh, Jamshoro, Pakistan. And From January 2020 to March 2022: he was an Assistant Professor, Computer Science Department, Szabist University, Hyd Campus, Pakistan. And From October 2020 to Current: he is working as an Assistant Professor, Faculty of Information Technology, Applied Sciences Private University, Amman, Jordan. His research interest includes Pervasive Computing, Context-awareness, Internet of Things (IoT), Machine Learning (ML). ma_jawarneh@asu.edu.jo



Dr. Qais Al-Na'amneh received his B.S. in software engineering from Hashemite university, Jordan, in 2015; the M.Sc. (with distinction) in Cyber Security from Hashemite university, Jordan, in 2021; I. Al-Naamneh is currently working as an Instructor with the Cyber Security and Cloud Computing Department, Applied Science Private University, Jordan. Also I have many certificates in Information Technology field like MCSA 2012 (Microsoft Certified Solutions Associate), MS-500 (Microsoft 365 Security Administration Certificate), CCNA (Cisco Certified Network Associate), CSFPC (Cyber Security Foundation Professional Certificate), Yeastar Certified Technician (VoIP phone system), Oracle developer, CEH (Ethical Hacker). q_naamneh@asu.edu.jo



Rahaf Hazaymih received her B.Sc. in Computer Engineering from Jordan University of Science and Technology in 2020. She is currently pursuing a Master's degree in Data Science. Rahaf is working as an AI Engineer, with research interests in Natural Language Processing (NLP), Artificial Intelligence (AI), Machine Learning (ML), Data Science, Cybersecurity, and the Internet of Things (IoT). Rahaf_hazaymih@yahoo.com



Dr. Lachhman Das Dhomeja. Faculty of Engineering and Technology, Sindh University, Jamshoro, Pakistan lachhman@usindh.edu.pk