# Enhancing Intrusion Detection in Autonomous Vehicles Using Ontology-Driven Mitigation

Manale Boughanja * , Zineb Bakraouy , Tomader MAZRI , Ahmed SRHIR

Posted Date: 30 September 2025

doi: 10.20944/preprints202509.2492.v1

Keywords: Security, Ontology; Intrusion detection system; autonomous vehicle; threat; mitigation; semantic knowledge

 doi:10.20944/preprints202509.2492.v1



*Article*

# Enhancing Intrusion Detection in Autonomous Vehicles Using Ontology-Driven Mitigation

**Manale Boughanja [1], Zineb Bakraouy [1], Tomader Mazri [2] and Ahmed Srhir [2]**

[1] Mohammed First University, ENSAO, SmartICT Lab, Oujda, Morocco
[2] Department of Electrical Engineering, Networks and Telecommunication Systems, National School of Applied Sciences, Ibn Tofail University, Kenitra, Maroc
* Correspondence: m.boughanja@ump.ac.ma

**Abstract**

With the increasing complexity of autonomous vehicle (AV) networks, ensuring enhanced cybersecurity has become a critical challenge. Traditional security techniques often struggle to adapt dynamically to evolving threats. This study proposes a novel domain ontology to assess its coherence and effectiveness in structuring knowledge about AV security threats, intrusion characteristics, and corresponding mitigation techniques. Developed using Protégé 4.3 and the Web Ontology Language (OWL), the ontology formalizes cybersecurity concepts without directly integrating with an Intrusion Detection System (IDS). By providing a semantic representation of attacks and countermeasures, the ontology enhances threat classification and supports automated decision-making in security frameworks. Experimental evaluation demonstrated its effectiveness in improving knowledge organization and reducing inconsistencies in security threat analysis. Future work will focus on integrating the ontology with real-time security monitoring and IDS frameworks to enhance adaptive intrusion response strategies.

**Keywords:** security; ontology; intrusion detection system; autonomous vehicle; threat mitigation; semantic knowledge

## 1. Introduction

Vehicular Ad Hoc Networks (VANETs) are a specialized subset of mobile ad hoc networks (MANETs) that enable vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communications. With the increasing integration of internet connectivity in modern vehicles, security concerns have become more prominent. Vehicles now synchronize with mobile devices, provide real-time navigation and weather updates, and exchange safety-critical information. However, this digital transformation also exposes vehicles to cyber threats, where attackers can exploit vulnerabilities to hijack control systems, compromise passenger safety, or disrupt road networks. Numerous studies have been conducted in the field of intrusion detection to improve the accuracy and reduce the false positives. The authors of [1] propose a comprehensive taxonomy that classifies IDSs into four main categories (fingerprinting, parameter monitoring, informational level, and machine learning), while [2] introduces VoltageIDS, a method specifically targeting bus and masquerade attacks. Another approach presented in [3] is based on parameter monitoring, but shows its limitations when faced with periodic packets. The authors in [4] apply information theory by analyzing time intervals to detect anomalies, and [5] leverage deep learning on GPS sensors to enhance the security of collected data. Despite their advances, traditional intrusion detection systems (IDS) remain limited: they rely on static rules or machine learning models, but lack a semantic understanding of the threat landscape. Thus, while they can detect an attack in progress, they struggle to guide the choice of an appropriate response effectively. The integration of an ontological approach makes it possible to overcome these

 doi:10.20944/preprints202509.2492.v1



limitations by structuring and enriching intrusion data. Thanks to the interrelationships expressed in the ontology, it becomes possible to automatically reason about the nature of attacks and associate each intrusion with the most relevant mitigation strategy, thereby strengthening the security of autonomous systems. This paper proposes a domain ontology for analyzing and enhancing attack mitigation strategies in AV security. Our goal is to develop a structured semantic representation that enables automated reasoning about intrusion types and countermeasures. By leveraging ontology-based knowledge representation, we aim to:

- Enhance the interpretability of detected intrusions by formalizing relationships between threats and mitigation strategies.
- Improve decision-making in IDS by providing a knowledge-driven framework to recommend suitable countermeasures.
- Facilitate seamless integration of security policies within AV systems, ensuring adaptive protection mechanisms.

This paper follows this structure: Section 2 reviews related work on ontologies in the context of autonomous vehicle (AV) security. Section 3 focuses on the classification of intrusions in AVs and the challenges specific to these systems. Section 4 outlines the security requirements for intrusion detection in AVs. Section 5 presents our proposed ontology-based methodology for mitigating cyber threats targeting AVs. Section 6 discusses the results and implications of our approach. Finally, the Conclusion and Perspectives section summarizes our findings and proposes future research directions for improving AV security.

## 2. Related Work

In the context of the Semantic Web, ontology refers to a structured set of concepts within a specific domain of expertise [6]. There are typically two global units in the ontology. The first aspect pertains to terminology, which defines the characteristics of the components constituting the ontology domain. This is analogous to defining a class in object-oriented programming, where we specify the nature of the objects we will manipulate later. The second part of the ontology concerns the relationships between multiple instances of the classes described in the terminology. Within ontology, concepts define one another, enabling reasoning and knowledge manipulation [7]. In the past few years, there has been some intrusion detection-based ontology. The author in [8] proposed an intrusion detection based on an ontology for security that provides a set of primitives for the design units of the security domain to enable both formal system specifications and inter-SafeBot communication. In [9], a security solution for web services is proposed to maintain the integrity and authentication of all services. The solution was deployed in DAML-S and used agents. The solution is based on a reasoning engine that determines whether agents and web services have similar security features or not by using a semantic matchmaker. Another ontology was provided by [10] for wired network security attacks. This ontology concentrates on both threats and vulnerability profiles. In [11], they propose an ontology modeling approach to assist vehicle drivers with safety alert messages in time-critical situations based on the Intelligent Driver Assistance System (I-DAS). It focuses on generating alert messages based on contextual parameters such as driving situations, etc. The proposed I-DAS collects information from the driver, vehicle, and external environmental sensors and transmits it to the system. The entries are captured and merged according to the context. The acquired input data is assimilated based on its respective contexts and sent to Context-Aware Reasoning. Their ontology is based on I-DAS where the authors explain the representation of a variety of control systems that serve as a common basis for domain understanding, decision-making, and information sharing. The authors in [12] explain the operation of moving from a fully manual to an automated vehicle; this ontology is based on five layers. Each layer represents a functionality taken into account and the level of control of a car. The second ontology is for situation awareness, which explains the different points that should be included in the ontology, such as Quality of Service (QoS) and specific vehicle characteristics, such as speed and location. In [13], an ontology-based architecture

 doi:10.20944/preprints202509.2492.v1



to enhance the driving environment through a network of traffic sensors is proposed. The ontology is based on four layers. The sensor layer detects different values of measurements, such as traffic flow and weather conditions. The second layer is data, and the related layer presents the emplacement of the data we can say that is concerned with the database and where the data is stored. The third is the ontology layer where a general ontology is described to provide different concepts involved in the road traffic scenario such as; sensors, drivers, and behaviors. The fourth is the agent layer, where the agents perform all tasks to improve the driving process. Another ontology is presented in [14]to drive contextual modeling and reasoning (OCM), consisting of four contextual pieces of information. Physical scenes as well as lane information. Road users represent the vehicle and the road user. The instrumented vehicle and its related properties include lane change and gear change. Finally, the sensors here we talk about the model and the sensor's functionality. The main purpose of this ontology is to provide the relationship between classes and their properties. In the past few years, there has been some intrusion detection-based ontology. The author in [8] proposed an intrusion detection based on an ontology for security that provides a set of primitives for the design units of the security domain to enable both formal system specifications and inter-SafeBot communication. Another ontology was provided by [10] for wired network security attacks. This ontology concentrates on both threats and vulnerability profiles. The authors in [15] explain the operation of moving from a fully manual to an automated vehicle; this ontology is based on five layers. Each layer represents a functionality taken into account and the level of control of a car. The second ontology is for situation awareness, which explains the different points that should be included in the ontology, such as Quality of Service (QoS) and specific vehicle characteristics, such as speed and location. In [13], an ontology-based architecture to enhance the driving environment through a network of traffic sensors is proposed. The ontology is based on four layers. The sensor layer detects different values of measurements, such as traffic flow and weather conditions. The second layer is data, and the related layer presents the emplacement of the data we can say that is concerned with the database and where the data is stored. The third is the ontology layer where a general ontology is described to provide different concepts involved in the road traffic scenario, such as sensors, drivers, and behaviors. The fourth is the agent layer, where the agents perform all tasks to improve the driving process. Another ontology is presented in [14] to drive contextual modeling and reasoning (OCM), consisting of four contextual pieces of information. Physical scenes as well as lane information. Road users represent the vehicle and the road user. The instrumented vehicle and its related properties include lane change and gear change. Finally, the sensors here we talk about the model and the sensor's functionality. The main purpose of this ontology is to provide the relationship between classes and their properties. The authors in [16]present a taxonomy of processes and semantics to represent and model space and time evolution in a GIS (Geographic Information System). Their approach is based on an event-based description of the spatial process. Sets of procedures define events. They have shown how semantic formalization allows a complete decomposition and representation of complex spatiotemporal models. In [17], they propose a system that profits from traffic management in emergencies and allows for making immediate decisions. The system reacts immediately, considers the neighboring vehicles, and collaborates with them to reach a consensus in real time. They provide in [18] an ontology-based approach to provide data access and query abilities to streaming data sources by providing the user with the possibility to express their needs at a conceptual level. In [19], the authors designed a mapping language called SASML (Sensors Annotation and Semantic Mapping Language) that provides a schema for annotating sensors and sources. In [20], they proposed an ontological approach to handle the problem of data integration while preserving their original significance and representation. They also examine the idea of ontology to benefit from data integration across a service- oriented architecture for applications in transportation systems. In [21], and [22], they propose an Ontological Anomaly Detection Approach (OADA) to identify anomalies in network traffic, specifically targeting network scans, DNS tunnel attacks, and telemetry data irregularities. The author in [23], proposes a Cyber threat intelligence to enhance and model an enhanced cyber- security solution. The author proposes an ontology-based

 doi:10.20944/preprints202509.2492.v1



approach to ensure semantic data interoperability between the heterogeneous components of an IDS. This contribution focuses on modeling and structuring anomaly-related information used in the incident detection process, as well as describing the system's components, their observations, measurements, and communication features [24]. The author introduces the KG-ID methodology, which utilizes a knowledge graph to analyze CAN frames and signal features for detecting various types of attacks [25]. The authors aim to identify key forensic challenges in autonomous vehicles (AVs), they introduce high-level ontological digital forensic investigation framework components, which serve as a starting point for developing a comprehensive framework [26].

## 3. Intrusion in Autonomous Vehicle: Classification and Challenges

Ensuring robust intrusion detection and mitigation in autonomous vehicles (AVs) requires a comprehensive analysis of security threats and their impact on AV operations [27]. These intrusions stem from vulnerabilities across multiple layers, including software, hardware, and communication networks, each presenting unique risks. A precise understanding of the origin of these threats is essential, as it dictates their classification and directly informs the most effective mitigation strategies. By leveraging advanced detection techniques and adaptive defense mechanisms, AVs can proactively address security breaches, enhancing resilience against evolving cyber threats and ensuring safer autonomous mobility.

### *3.1. Classification of Attack*

Autonomous vehicles face a wide range of threats that can jeopardize their safety, reliability, and overall functionality [28]. Our research has classified these attacks into two broad categories: interface-based attacks, which exploit the vehicle's communication channels, and methodology-based attacks, which aim to manipulate its behavior. In the following subsections, we will detail these two types of attacks and their implications.

#### 3.1.1. Interface Based Attack

Surface-based attacks leverage the various layers of the autonomous vehicle, each layer being vulnerable to specific attacks. These attacks can be divided into several sub-categories:

- **Attacks on the perception layer (sensor level):** Sensors have a crucial role to play in detecting the vehicle's environment. GPS spoofing, for example, involves the injection of falsified GPS signals, which mislead the navigation system and direct the vehicle to incorrect destinations. LiDAR and camera spoofing involves manipulating the data collected by these sensors to create false objects or conceal real obstacles, thereby disrupting the vehicle's decision-making process [29]. Finally, adversarial attacks on AI modify the input data used by artificial intelligence models, which can mislead the vehicle and lead to incorrect driving decisions [30].
- **Attacks on the communication layer**: AVs constantly interact with other vehicles (V2V) and external infrastructures (V2I). Man-in-the-Middle (MitM) attacks intercept these communications, enabling attackers to modify or falsify them. On the other hand, Denial of Service (DoS/DDoS) attacks aim to saturate communication networks, disrupting essential services such as navigation, communication with other vehicles or security alerts [31]. On the other hand, false message injection is another potentially devastating attack, where falsified messages are sent into V2V or V2I channels, distorting coordination and decision-making between vehicles and the infrastructure.
- **Attacks on the decision-making layer**: AVs depend on artificial intelligence systems to make decisions in real-time. Data poisoning involves injecting malicious data into learning models, distorting vehicle behavior, and increasing the risk of erroneous decisions [32]. In addition, manipulation of reinforcement learning involves altering the rewards given to the AI system to influence its learning process, which disrupts the vehicle's decisions and may lead it to adopt unsafe behavior.

 doi:10.20944/preprints202509.2492.v1



- **Attacks on the control layer**: These attacks aim to directly modify the vehicle's actions. Braking override prevents the vehicle from stopping, even in situations where stopping is necessary to avoid an accident [33]. Acceleration manipulation forces the vehicle to accelerate unexpectedly, compromising the safety of passengers and other road users.

3.1.2. Methodology-Based Attack

Methodology-based threats refer to the specific techniques used by attackers to penetrate autonomous vehicle systems. These types of threats fall into three broad categories:

- **Cyber-attacks**: refer to attempts to intrude into a vehicle's electronic systems, usually carried out remotely by malicious attackers [34]. One of the most common forms is the exploitation of vulnerabilities in vehicle systems via wireless connections. Using these exploits, attackers can take control of vital vehicle systems, as has been observed in vehicle hacking incidents, particularly those involving Tesla cars. Another form of cyber attack involves malware and ransomware, which are used to infect vehicle systems. This can either disable the vehicle or compromise sensitive data, forcing the attacker to demand a ransom to unlock access or prevent the disclosure of private information [35]. In addition, attacks using backdoors or logic bombs can be introduced during vehicle software updates. Backdoors enable attackers to gain remote access to the vehicle's systems, while logic bombs can be activated at a specific time to disrupt its operation.
- **Physical attacks** are a direct impact on the vehicle's hardware components, particularly sensors and communication systems. For example, the manipulation of sensors can include actions such as covering, blocking or degrading them, preventing the vehicle from correctly perceiving its environment [36]. This can lead to errors of judgment or failures in autonomous driving systems, compromising vehicle safety.
- **Social engineering attacks**: also called insider threats, exploit the manipulation of individuals or loopholes in the supply chain to compromise a vehicle's systems. Phishing techniques and fraudulent software updates are commonly used to trick users or employees into installing malware on vehicle systems [37]. These attacks are often disguised as legitimate software updates but contain malicious elements that enable the attacker to take control of the system.

The figure 1, summarizes our classification:

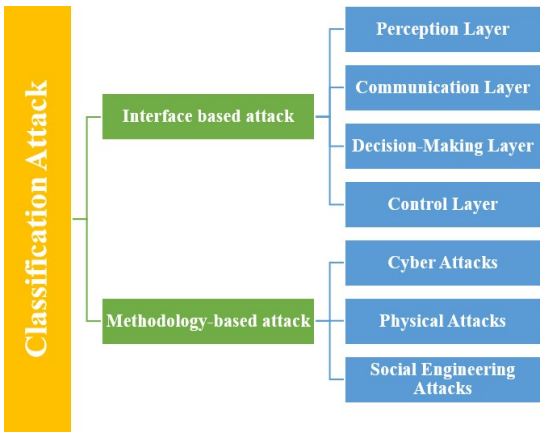


**Figure 1.** Classification Attack in AV.

*3.2. Challenges Related to the Safety of Autonomous Vehicles*

While the classification of attacks provides an understanding of the different threats faced by autonomous vehicles, it is equally important to analyze the challenges associated with guaranteeing their security. These challenges stem from vulnerabilities in the software, hardware, and

 doi:10.20944/preprints202509.2492.v1



communication layers, as well as external factors such as malicious actors and policy violations. The following section explores these challenges in detail.

3.2.1. Intrusions Due to System Vulnerabilities

Autonomous vehicles rely on an extensive set of sensors and computing units to process environmental data [38]. These components introduce vulnerabilities from multiple sources:

- Software-based vulnerabilities: Unpatched software, unsecured third-party applications, and malicious firmware updates can allow attackers to exploit the system.
- Communication vulnerabilities: AVs communicate via Vehicle-to-Everything (V2X) protocols, which are susceptible to eavesdropping, spoofing, and man-in-the-middle attacks.
- Hardware-based vulnerabilities: Malfunctioning electronic control units (ECUs), sensor failures, or unauthorized physical access can introduce security risks.

3.2.2. Intrusions Due to External Actors

AVs interact with both their environment and human operators [39]. Intrusions may arise from:

- Environmental factors: Sensor manipulation (e.g., LiDAR jamming), GPS spoofing, and adversarial road signs can mislead AV decision-making.
- Malicious drivers: Attackers inside nearby vehicles may inject false information into AV networks to mislead detection systems.

Several techniques have been implemented to detect the misbehavior of the vehicle during the interaction with its environment. In [40], proposed a solution to detect the misbehavior of the vehicle and correct it with the necessary mechanism. Another solution is to define the normal behavior [41]; this technique is based on the reputation of the other nodes and permits the system to define a regular behavior in the vehicle itself. A misbehavior detection scheme was proposed in [42] to avoid false messages depending on the vehicle's behavior; this method provides the system with a robust authentication mechanism to exclude any malevolent

3.2.3. Intrusions Due to Security Policy Violations

From a security perspective, intrusions often violate one or more CIA (Confidentiality, Integrity, and Availability) properties [43]:

- Confidentiality attacks: Data breaches exposing AV sensor or user data.
- Integrity attacks: Tampering with AV decision-making by injecting false control commands.
- Availability attacks: Denial-of-Service (DoS) or jamming attacks that disrupt communication.

The figure, present the challenges faced the autonomous vehicle:


**Figure 2.** Challenges related to the safety of autonomous vehicles.

 doi:10.20944/preprints202509.2492.v1



## 4. Security Requirements for Intrusion Detection in Autonomous Vehicle

To mitigate the impact of cyber attacks on autonomous vehicles (AVs), stringent security measures must be implemented at all levels of the AV architecture. These measures guarantee the integrity, confidentiality, and availability of critical vehicle functions, while reducing the risk of intrusion [43]. Below are the essential security requirements for effective detection and mitigation of intrusions into AVs.

### *4.1. Authentication & Access Control*

Authentication and access control mechanisms are essential to prevent unauthorized access to vehicle systems [43]. These measures ensure that only legitimate users and devices can interact with vehicle components.

- Multi-factor authentication (MFA): enhances security by requiring multiple authentication factors (e.g. passwords, biometrics, and security tokens) to access vehicle systems.
- Role-based access control (RBAC): implementation of strict authorization policies based on user roles (e.g. driver, manufacturer, service technician) to limit system access and minimize security risks.

### *4.2. Secure Communication*

Maintaining the confidentiality and integrity of data exchanged between autonomous vehicles and external entities (V2X) is essential to prevent unauthorized interception and manipulation [43].

- End-to-end encryption (E2EE): Use secure cryptographic protocols (e.g. TLS/SSL) to encrypt V2X communications, preventing eavesdropping and data tampering.
- Intrusion Prevention Systems (IPS): Deploy network security solutions to detect and block malicious traffic in real-time, mitigating the risk of network-based attacks such as Man-in-the-Middle (MitM) and Denial-of-Service (DoS).
- Blockchain for V2X security: Leveraging decentralized authentication to verify the legitimacy of messages exchanged between vehicles, infrastructure, and cloud services, reducing the risk of injecting false messages.

### *4.3. AI-Based Intrusion Detection Systems (IDS)*

Artificial intelligence (AI) plays a significant part in detecting and mitigating cyber threats in autonomous vehicles by analyzing patterns and identifying anomalies in vehicle behavior and network traffic [44].

- Anomaly-based detection: using machine learning algorithms to monitor deviations from normal operations in network communications, sensor inputs, and system behaviors, thus identifying potential attacks in real-time [45].
- Adversarial ML defense techniques: implementing robust AI models that resist adversarial attacks by improving training methods, using adversarial learning, and integrating model-checking techniques to improve resilience [46].

### *4.4. Secure Software & Hardware*

Ensuring the security of software and hardware components is key to safeguarding autonomous vehicles against cyber threats and unauthorized modifications [47].

- Secure booting and code signing: implementation of cryptographic validation mechanisms to ensure that only trusted and verified software is executed on vehicle components, preventing unauthorized firmware updates or malware injections.

 doi:10.20944/preprints202509.2492.v1



- Hardware Security Modules (HSM): use of dedicated security chips to securely store and manage cryptographic keys, preventing unauthorized access to encryption keys and protecting sensitive vehicle data.

*4.5. Resilience & Recovery Mechanisms*

Autonomous vehicles, even with enhanced safety measures, need to be equipped with safety mechanisms to respond effectively to cyber incidents and ensure continued safe operation [48].

- Safety mechanisms: design autonomous systems to enter a safe operating mode if a cyber attack is detected, enabling the vehicle to stop or continue operating with minimal risk to passengers and the environment.
- Redundant systems: integrate backup sensors, isolated control units, and redundant communication networks to maintain essential functionality in the event of system failure or security breaches.

The table 1, summarizes the security requirements for intrusion detection in Autonomous vehicles:

**Table 1.** Security requirements for intrusion detection in Autonomous vehicle.

| Security Technique | Security Measure | Security Requirement | | |
|---|---|---|---|---|
| | | Confidentiality | Integrity | Availability |
| Authentication & Access Control | Multi-factor authentication (MFA) | * | * | * |
| | Multi-factor authentication (MFA) | * | * | * |
| Secure Communication | End-to-end encryption (E2EE) | * | * | |
| | Intrusion Prevention Systems (IPS) | | * | * |
| | Blockchain for V2X security | * | * | |
| AI-Based Intrusion Detection Systems (IDS) | Anomaly-based detection | * | * | |
| | Adversarial ML defense techniques | | * | * |
| Secure Software & Hardware | Secure booting and code signing | * | * | |
| | Hardware Security Modules (HSM) | * | * | |
| Resilience & Recovery Mechanisms | Safety mechanisms | | * | * |
| | Redundant systems | | | * |

## 5. Methodology and Proposed Ontology

*5.1. Procedures for Ontology Creation*

Intrusion detection in autonomous vehicles is becoming a crucial foundation for protecting against threats. Existing authentication and access control mechanisms are insufficient to counter these sophisticated attacks. However, one of the biggest challenges in implementing a credential-based security system is accurately identifying intrusions and determining the appropriate response

 doi:10.20944/preprints202509.2492.v1



to mitigate threats. A promising approach is leveraging a semantic asset such as an ontology, which structures knowledge to enhance intrusion detection and response.

The ontology consists of four main stages:

- **Planning** involves defining the problem and outlining the tasks needed to address it. This includes detecting security threats in autonomous vehicles, identifying mitigation techniques, assessing their impact, and structuring these tasks by categorizing relevant elements (e.g., vehicle communication, attack types, and mitigation strategies). Additionally, this step defines actors and their attributes, mapping their interactions within the system.
- **Control** ensures the ontology's execution is accurate, error-free, and effectively resolves the identified security issues.
- **Quality Assurance** follows, focusing on testing the ontology and validating the interactions between different entities to confirm its reliability.
- **Exploitation** is the final stage, where the ontology is deployed in real-world scenarios after extensive testing. Figure 3, illustrates this ontology-based process:

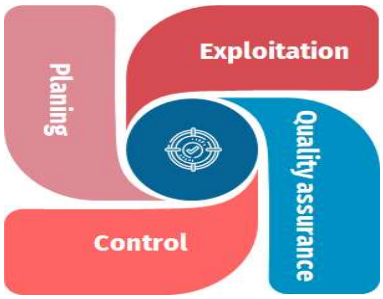


**Figure 3.** Ontology Process.

*5.2. Proposed Ontology*

Our contribution is to construct an ontology for the security domain. We have based ourselves on the METHONTOLOGY methodology [49], which is the basic support for the conceptualization of the ontology to be created through a set of intermediate semi-formal representations. The logic of descriptions is the formalism adapted for expressing the semi- formal ontology OWL. The ontology definition language is chosen to codify the ontology using OWL Protected ontology editor. Finally, the Pallet inference system is used to test the consistency of the ontology throughout the development process. Our contribution, essentially, is an ontology to secure the autonomous vehicle to mitigate the detected security problems. Throughout its movement, the autonomous vehicle needs to interact with its environment. The environment is potentially heterogeneous and unpredictable and can influence the process of its movement. Therefore, the autonomous vehicle must be sensitive to its safety context to reason about it and verify if the requirements and capabilities acquired for its execution are satisfied. We used a development process for our ontology construction, starting from raw knowledge and arriving at a functional application ontology represented by the OWL language. The main steps of this process are inspired by the methodology of ontology construction " METHONTOLOGY " [26]. The application of each step of this process is based on the exploitation of the HEMMAM work [50]. This process is composed of five steps, as presented in the figure below:

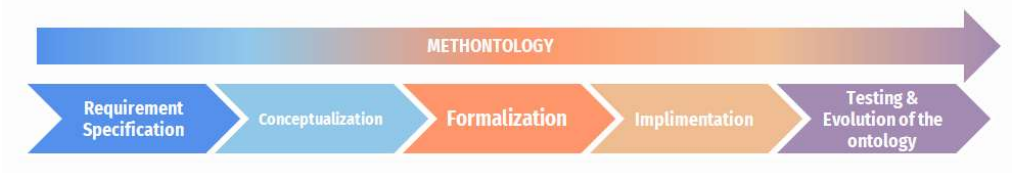


**Figure 4.**

 doi:10.20944/preprints202509.2492.v1



We will detail each of these steps in the following subsection.

*5.3. Ontology-Based to Secure Autonomous Vehicles*

After introducing the process used to build our ontology, we will construct the ontology related to autonomous vehicle security. We will follow the steps of the ontology construction process outlined in the previous section.

5.3.1. Specification

Ontology development begins with the specification phase, which establishes a requirements specification document. In this document, we will derive the ontology of the construct through the following five aspects:

- ***The knowledge domain:*** the ontology we have just constructed is part of the autonomous vehicle security domain. It can draw its concepts from the domain of computer security.
- ***The objective*****:** the main objective of incorporating ontologies in an autonomous vehicle is to conceal the heterogeneity concerning the security to guarantee better interoperability of the security policies to decrease the severity of the risk using the knowledge domain of the ontology.
- ***Users*****:** This aspect provides the set of users to exploit the ontology. In our case, the ontology users are the autonomous vehicles that need to exploit the ontologies to maintain the required goal.
- ***Information sources***: the information sources on which we based ourselves to arrive at the construction of the application ontology are technical documents of autonomous vehicle security.
- ***The scope of the ontology***: This aspect consists in determining a priori the list of terms of the ontology (the most important ones); among these terms, we can mention: Vehicle, Countermeasure, Threat, etc.

We summarize this phase in an RDF document presented in the figure below:

```
<!-- Classes -->
<owl: Class RDF: about="ex: Threat"/>
<owl: Class RDF: about="ex: Vulnerability"/>
<owl: Class RDF: about="ex: AttackMethod"/>
<owl: Class RDF: about="ex: Intrusion"/>
<owl: Class RDF: about="ex: VehicularIDS"/>
<owl: Class RDF: about="ex: DefenseMechanism"/>
<!-- Object Properties -->
<owl: ObjectProperty rdf: about="ex:exploits">
   <rdfs: domain RDF: resource="ex: Threat"/>
   <rdfs: range rdf:resource="ex:Vulnerability"/>
</owl:ObjectProperty>
```

**Figure 5.** An RDF document specifying the ontology.

5.3.2. Conceptualization

Once most knowledge has been acquired, it must be arranged and structured according to intermediate semi-formal descriptions that are easy to understand and independent of any implementation language [51]. We construct the concept classification hierarchy and illustrate the organization of ontology concepts in a hierarchical order that expresses subclass relationships. A universal concept, "Thing," which generalizes all root concepts of various concept hierarchies, is employed to establish a single global hierarchy.

To develop our concept taxonomy, METHONTOLOGY proposes the use of four relations:

- A concept $C_1$ is a subclass of concept $C_2$ if and only if every instance of $C_1$ is also an instance of $C_2$. For example, a Vehicle is a subclass of the class Entity.

 doi:10.20944/preprints202509.2492.v1



- A Disjoint Decomposition of concept C is a set of subclasses of C that do not cover C entirely and do not share any common instances. For example, the concepts Low, Moderate, and Critical form a Disjoint Decomposition of the concept of Security Level.
- An Exhaustive Decomposition of concept C is a set of subclasses of C that together cover C completely and may share common instances.
- A Partition of concept C is a set of subclasses of C that together cover C entirely and have no overlapping instances. For instance, the concepts Proactive, Detective, and Corrective form a Partition of concept types.

We will present the classification and the corresponding binary diagram based on these defined relations. The figure below illustrates the binary relationship diagram.

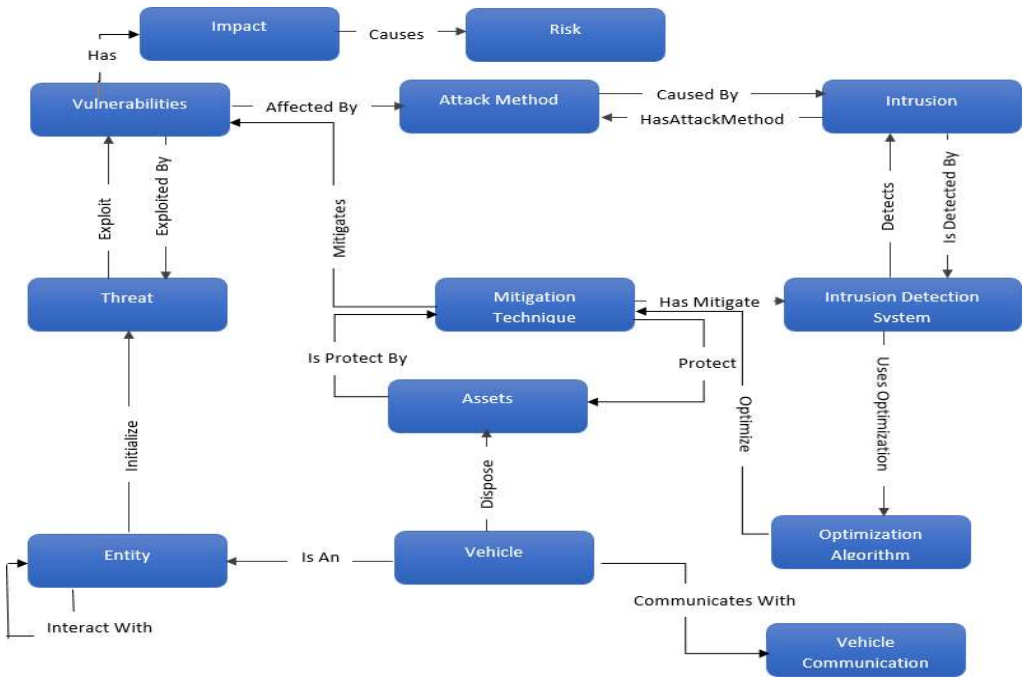


**Figure 6.** Binary relationship diagram.

5.3.3. Formalization

In this step, we will use description logic to formalize the conceptual model obtained in the previous conceptualization phase. The formalization process consists of two main steps: TBox and ABox construction.

- TBox defines the concepts and roles of an ontology using descriptive logic constructs. Whereas an ABox describes individuals, a TBox formalizes the conceptual structure of the domain by establishing general relationships between concepts. For example, the statement *"A vehicle has at least one asset"* can be expressed in description logic as:

$$\textit{Vehicle} \equiv \exists \textit{disposes}.\ \textit{Assets}$$

This axiom means that any individual classified as a Vehicle must have at least one asset type. Such terminological axioms enrich the semantics of a detection system and provide a basis for automated reasoning. In addition, we construct the TBox by specifying the subsumption relationships that exist between different concepts and roles. For example, to indicate that the *Owner* class subsumes the *Driver* class, we write:

$$\textit{Driver} \sqsubseteq \textit{Owner}$$

 doi:10.20944/preprints202509.2492.v1



The ABox (Assertional Box) contains assertions about individuals in a domain, i.e., concrete facts. It complements the TBox by specifying which instances belong to which concepts and how the instances are related by roles. The ABox describes observable and verifiable data. For example, if the TBox defines the concept Vehicle and the role ownsAsset, the ABox may contain the following assertions:

- Vehicle1 : Vehicle
- Asset1 : Asset
- Vehicle1 ownsAsset Asset1

5.3.4. Implementation and Test

Our choice was to implement our ontology in OWL, representing a coding language. The implementation passes through several steps, from the class creation to the instance definition. We used the Pallet system to test the ontology. We distinguish two types of tests: consistency test and satisfiability test; the first one removes the inconsistency between the concepts and uses the subsumption test incorporated in the Pallet system. On the other hand, the second one allows checking for each concept the existence of the instances; a concept C is satisfiable if and only if there exists at least an interpretation I (instance) for the concept C.

According to the tests we applied to the ontology, no errors occurred

The proposed ontology was tested in Protégé using the Pallet system, as presented in figures 7 and 8 show the consistency and the classification test, and the results were satisfying.

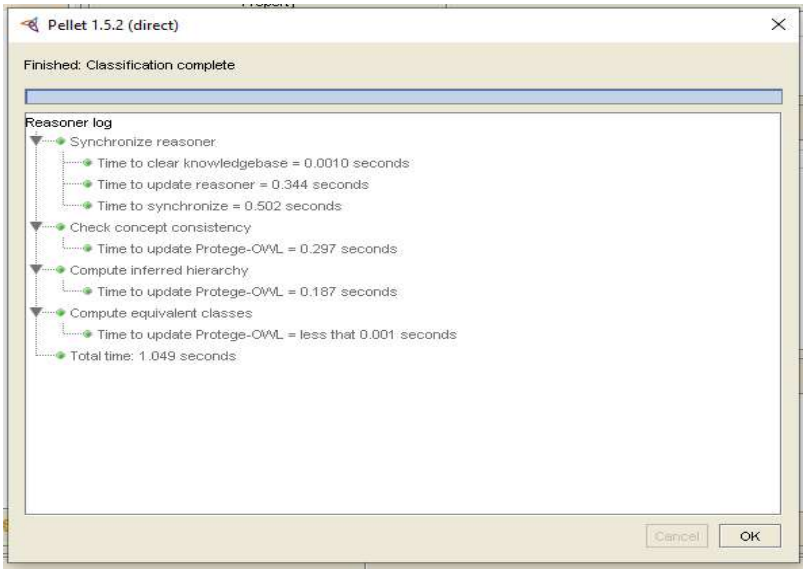


**Figure 7.** Classification test.

 doi:10.20944/preprints202509.2492.v1



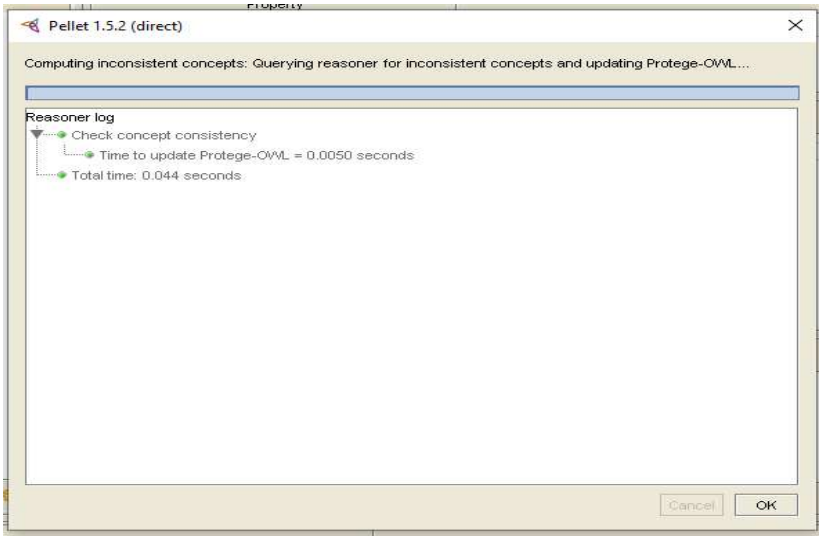


**Figure 8.** Consistency test.

## 6. Discussion

We developed our ontology to structure, and formalize techniques that mitigate cyber-attacks on autonomous vehicles. Drawing on METHONTOLOGY and integrating concepts from computer security, we have developed a model to improve the interoperability of defense mechanisms against identified threats. The approach adopted aims to organize knowledge around available countermeasures and optimize their application according to the attacks detected. Implementation in OWL ensures rigorous structuring that can be exploited by embedded cyber security systems. Our ontology also incorporates a vocabulary related to optimization techniques, allowing for the selection and adjustment of the most appropriate mitigation strategies in real-time, based on the characteristics of newly detected threats.

The validation of our ontology focused on the consistency of the entities and relationships defined, ensuring that cyber security concepts applied to autonomous vehicles are correctly represented. Using the Pallet reasoner enabled us to validate the consistency of our model and confirm that the defined mitigation mechanisms are aligned with the identified threats. The classification of classes was completed in 1.049s, and the consistency check took 0.044s. The results obtained demonstrate that our model respects the principles of classification and concept inheritance, providing a solid foundation for future exploitation. However, several challenges remain. Firstly, the constant evolution of cyber-attacks requires our ontology to be dynamically updated. Although the ontology includes a detailed classification of known attacks, it needs to adapt to emerging threats. The integration of optimization techniques, such as genetic algorithms, could play a key role in enhancing the selection of countermeasures in real-time. These techniques would empower the ontology to adjust defense strategies autonomously according to the nature and impact of attacks. The implementation of simulations in real-life environments is an essential step in evaluating the ontology's effectiveness and refining its optimization models. The next step is to strengthen our ontology with a machine learning (ML) model so that it can acquire new techniques and thus enhance security in line with evolving threats.

## 7. Conclusions and Perspectives

This paper presents a formalized description of various mitigation techniques for autonomous vehicles (AVs) using an ontology-based approach. The ontology addresses intrusion detection by considering vulnerabilities, security measures, and the actors involved, depending on the severity and impact of the system's vulnerabilities. By defining the domain concepts and emphasizing their interrelationships, our ontology lays the groundwork for developing more efficient and reliable

 doi:10.20944/preprints202509.2492.v1



mitigation strategies. Looking forward, the next step is to develop a validation platform aimed at detecting intrusions and selecting appropriate countermeasures based on the semantic understanding of past incidents. This approach will ensure that the selection of mitigation techniques is better aligned with the specific characteristics of the threats, ultimately strengthening the overall security framework of autonomous vehicles. Furthermore, we plan to extend this work to real-time applications and simulations to further refine and optimize the system's response in dynamic, real-world environments.

## References


1. W. Wu *et al.*, « A Survey of Intrusion Detection for In-Vehicle Networks », *IEEE Trans. Intell. Transp. Syst.*, vol. 21, nº 3, p. 919-933, mars 2020, doi: 10.1109/TITS.2019.2908074.
2. K. T. Cho et K. G. Shin, « Viden: Attacker identification on in-vehicle networks », in *Proceedings of the ACM Conference on Computer and Communications Security*, 2017, p. 1109-1123. doi: 10.1145/3133956.3134001.
3. A. Taylor, N. Japkowicz, et S. Leblanc, « Frequency-based anomaly detection for the automotive CAN bus », in *2015 World Congress on Industrial Control Systems Security (WCICSS)*, déc. 2015, p. 45-49. doi: 10.1109/WCICSS.2015.7420322.
4. H. M. Song, H. R. Kim, et H. K. Kim, « Intrusion detection system based on the analysis of time intervals of CAN messages for in-vehicle network », *2016 Int. Conf. Inf. Netw. ICOIN*, p. 63-68, janv. 2016, doi: 10.1109/ICOIN.2016.7427089.
5. B. Manale et T. Mazri, « Intrusion detection method for GPS based on deep learning for autonomous vehicle », *Int. J. Electron. Secur. Digit. Forensics*, vol. 14, nº 1, p. 37-52, 2022, doi: 10.1504/IJESDF.2022.120039.
6. J. Bandeira, I. I. Bittencourt, P. Espinheira, et S. Isotani, « FOCA: A Methodology for Ontology Evaluation », 2 septembre 2017, *arXiv*: arXiv:1612.03353. doi: 10.48550/arXiv.1612.03353.
7. F. Neuhaus, « What is an Ontology? », 22 octobre 2018, *arXiv*: arXiv:1810.09171. doi: 10.48550/arXiv.1810.09171.
8. R. Filman et T. Linden, « SafeBots: A paradigm for software security controls », *Proc. New Secur. Paradig. Workshop*, vol. Part F1294, p. 45-51, 1996, doi: 10.1145/304851.304863.
9. G. Denker, L. Kagal, T. Finin, M. Paolucci, et K. Sycara, « Security for DAML Web Services: Annotation and Matchmaking », in *The Semantic Web - ISWC 2003*, D. Fensel, K. Sycara, et J. Mylopoulos, Éd., Berlin, Heidelberg: Springer, 2003, p. 335-350. doi: 10.1007/978-3-540-39718-2_22.
10. A. Simmonds, P. Sandilands, et L. Van Ekert, « An ontology for network security attacks », *Lect. Notes Comput. Sci. Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinforma.*, vol. 3285, p. 317-323, 2004, doi: 10.1007/978-3-540-30176-9_41.
11. S. Kannan, A. Thangavelu, et R. Kalivaradhan, « An Intelligent Driver Assistance System (I-DAS) for Vehicle Safety Modelling using Ontology Approach », *Int. J. UbiComp*, vol. 1, nº 3, p. 15-29, juill. 2010, doi: 10.5121/iju.2010.1302.
12. M. Stocker, M. Rönkkö, et M. Kolehmainen, « Making sense of sensor data using ontology: A discussion for road vehicle classification ».
13. S. Fernandez, R. Hadfi, T. Ito, I. Marsa-Maestre, et J. R. Velasco, « Ontology-Based Architecture for Intelligent Transportation Systems Using a Traffic Sensor Network », *Sensors*, vol. 16, nº 8, p. 1287, août 2016, doi: 10.3390/s16081287.
14. Z. Xiong, V. V. Dixit, et S. Travis Waller, « The development of an ontology for driving context modelling and reasoning », *IEEE Conf. Intell. Transp. Syst. Proc. ITSC*, p. 13-18, 2016, doi: 10.1109/ITSC.2016.7795524.
15. E. Pollard, P. Morignot, et F. Nashashibi, « An ontology-based model to determine the automation level of an automated vehicle for co-driving », in *Proceedings of the 16th International Conference on Information Fusion*, juill. 2013, p. 596-603. Consulté le: 22 mars 2025. [En ligne]. Disponible sur: https://ieeexplore.ieee.org/document/6641334?denied=
16. V. B. Robinson et D. S. Mackay, « Semantic modeling for the integration of geographic information and regional hydroecological simulation management », *Comput. Environ. Urban Syst.*, vol. 19, nº 5-6, p. 321-339, nov. 1995, doi: 10.1016/0198-9715(95)00017-8.

 doi:10.20944/preprints202509.2492.v1




17. « An ontology based approach to traffic management in urban areas | Request PDF ». Consulté le: 22 mars 2025. [En ligne]. Disponible sur: https://www.researchgate.net/publication/280949391_An_ontology_based_approach_to_traffic_management_in_urban_areas
18. J.-P. Calbimonte, « Ontology-based access to sensor data streams », PhD Thesis, Universidad Politécnica de Madrid, 2013. doi: 10.20868/UPM.thesis.15320.
19. X. Zhang, Yu. Zhao, et W. Liu, « A Method for Mapping Sensor Data to SSN Ontology », *Int. J. U- E- Serv. Sci. Technol.*, vol. 8, nº 9, p. 303-316, sept. 2015, doi: 10.14257/ijunesst.2015.8.9.31.
20. A. Seliverstov et R. J. F. Rossetti, « An ontological approach to spatio-temporal information modelling in transportation », *2015 IEEE 1st Int. Smart Cities Conf. ISC2 2015*, 2015, doi: 10.1109/ISC2.2015.7366160.
21. C. Baccigalupo et E. Plaza, « Poolcasting: A Social Web Radio Architecture for Group Customisation », in *Third International Conference on Automated Production of Cross Media Content for Multi-Channel Distribution (AXMEDIS'07)*, nov. 2007, p. 115-122. doi: 10.1109/AXMEDIS.2007.19.
22. B. Alaya, L. Sellami, et P. Lorenz, « An ontological approach to the detection of anomalies in vehicular ad hoc networks », *Ad Hoc Netw.*, vol. 156, p. 103417, avr. 2024, doi: 10.1016/j.adhoc.2024.103417.
23. « A dataset for cyber threat intelligence modeling of connected autonomous vehicles | Scientific Data ». Consulté le: 22 mars 2025. [En ligne]. Disponible sur: https://www.nature.com/articles/s41597-025-04439-5
24. « OAIDS: An Ontology-Based Framework for Building an Intelligent Urban Road Traffic Automatic Incident Detection System | SpringerLink ». Consulté le: 22 mars 2025. [En ligne]. Disponible sur: https://link.springer.com/chapter/10.1007/978-3-030-96311-8_36
25. H. Sun, J. Wang, J. Weng, et W. Tan, « KG-ID: Knowledge Graph-Based Intrusion Detection on In-Vehicle Network », *IEEE Trans. Intell. Transp. Syst.*, p. 1-13, 2025, doi: 10.1109/TITS.2025.3530155.
26. O. Bakare, N. Karie, R. Ryan, et I. Murray, *Towards an Ontological Digital Forensic Investigation Framework for Autonomous Vehicles*. 2024, p. 204. doi: 10.1109/ICAC64487.2024.10851001.
27. E. E. Abdallah, A. Aloqaily, et H. Fayez, « Identifying Intrusion Attempts on Connected and Autonomous Vehicles: A Survey », *Procedia Comput. Sci.*, vol. 220, p. 307-314, janv. 2023, doi: 10.1016/j.procs.2023.03.040.
28. G. Loukas, E. Karapistoli, E. Panaousis, P. Sarigiannidis, A. Bezemskij, et T. Vuong, « A taxonomy and survey of cyber-physical intrusion detection approaches for vehicles », *Ad Hoc Netw.*, vol. 84, p. 124-147, mars 2019, doi: 10.1016/j.adhoc.2018.10.002.
29. X. Hu, T. Liu, T. Shu, et D. Nguyen, « Spoofing Detection for LiDAR in Autonomous Vehicles: A Physical-Layer Approach », *IEEE Internet Things J.*, vol. 11, nº 11, p. 20673-20689, juin 2024, doi: 10.1109/JIOT.2024.3371378.
30. « Cybersecurity of Autonomous Vehicles: A Systematic Literature Review of Adversarial Attacks and Defense Models | IEEE Journals & Magazine | IEEE Xplore ». Consulté le: 22 mars 2025. [En ligne]. Disponible sur: https://ieeexplore.ieee.org/abstract/document/10097455
31. A. Praseed et P. S. Thilagam, « DDoS Attacks at the Application Layer: Challenges and Research Perspectives for Safeguarding Web Applications », *IEEE Commun. Surv. Tutor.*, vol. 21, nº 1, p. 661-685, 2019, doi: 10.1109/COMST.2018.2870658.
32. S. Madhavi, N. C. Santhosh, S. Rajkumar, et R. Praveen, « Pythagorean Fuzzy Sets-based VIKOR and TOPSIS-based multi-criteria decision-making model for mitigating resource deletion attacks in WSNs », *J. Intell. Fuzzy Syst.*, vol. 44, nº 6, p. 9441-9459, janv. 2023, doi: 10.3233/JIFS-224141.
33. M. Hataba, A. Sherif, M. Mahmoud, M. Abdallah, et W. Alasmary, « Security and Privacy Issues in Autonomous Vehicles: A Layer-Based Survey », *IEEE Open J. Commun. Soc.*, vol. 3, p. 811-829, 2022, doi: 10.1109/OJCOMS.2022.3169500.
34. B. G. B. Stottelaar, « Practical cyber-attacks on autonomous vehicles ». Consulté le: 22 mars 2025. [En ligne]. Disponible sur: https://essay.utwente.nl/66766/
35. « Towards a Severity Assessment Method for Potential Cyber Attacks to Connected and Autonomous Vehicles - He - 2020 - Journal of Advanced Transportation - Wiley Online Library ». Consulté le: 22 mars 2025. [En ligne]. Disponible sur: https://onlinelibrary.wiley.com/doi/full/10.1155/2020/6873273

 doi:10.20944/preprints202509.2492.v1




36. « Physical Invariant Based Attack Detection for Autonomous Vehicles: Survey, Vision, and Challenges | IEEE Conference Publication | IEEE Xplore ». Consulté le: 22 mars 2025. [En ligne]. Disponible sur: https://ieeexplore.ieee.org/abstract/document/9499330
37. V. L. L. Thing et J. Wu, « Autonomous Vehicle Security: A Taxonomy of Attacks and Defences », *Proc. - 2016 IEEE Int. Conf. Internet Things IEEE Green Comput. Commun. IEEE Cyber Phys. Soc. Comput. IEEE Smart Data IThings-GreenCom-CPSCom-Smart Data 2016*, p. 164-170, 2017, doi: 10.1109/iThings-GreenCom-CPSCom-SmartData.2016.52.
38. « Intrusion Threats and Security Solutions for Autonomous Vehicle Networks | IEEE Conference Publication | IEEE Xplore ». Consulté le: 22 mars 2025. [En ligne]. Disponible sur: https://ieeexplore.ieee.org/abstract/document/8308273
39. « Potential Cyberattacks on Automated Vehicles | IEEE Journals & Magazine | IEEE Xplore ». Consulté le: 22 mars 2025. [En ligne]. Disponible sur: https://ieeexplore.ieee.org/abstract/document/6899663
40. P. Golle, D. Greene, et J. Staddon, « Detecting and correcting malicious data in VANETs », in *Proceedings of the 1st ACM international workshop on Vehicular ad hoc networks*, in VANET '04. New York, NY, USA: Association for Computing Machinery, oct. 2004, p. 29-37. doi: 10.1145/1023875.1023881.
41. « Vehicle Behavior Analysis to Enhance Security in VANETs | Semantic Scholar ». Consulté le: 22 mars 2025. [En ligne]. Disponible sur: https://www.semanticscholar.org/paper/Vehicle-Behavior-Analysis-to-Enhance-Security-in-Schmidt-Leinm%C3%BCller/470b806a3e385be3980f5f1e545d30af51b1359a
42. M. Ghosh, A. Varghese, A. A. Kherani, et A. Gupta, « Distributed Misbehavior Detection in VANETs », in *2009 IEEE Wireless Communications and Networking Conference*, avr. 2009, p. 1-6. doi: 10.1109/WCNC.2009.4917675.
43. S. Lingras et A. Basu, « The Security of Autonomous Vehicle Software and its National Security Implications », *Eur. J. Appl. Sci. Eng. Technol.*, vol. 3, nº 1, Art. nº 1, févr. 2025, doi: 10.59324/ejaset.2025.3(1).16.
44. « AI-Based Intrusion Detection Systems for In-Vehicle Networks: A Survey | ACM Computing Surveys ». Consulté le: 22 mars 2025. [En ligne]. Disponible sur: https://dl.acm.org/doi/full/10.1145/3570954
45. H. Lundberg, *Increasing the Trustworthiness ofAI-based In-Vehicle IDS usingeXplainable AI*. 2022. Consulté le: 22 mars 2025. [En ligne]. Disponible sur: https://urn.kb.se/resolve?urn=urn:nbn:se:miun:diva-45223
46. P. Sharma, D. Austin, et H. Liu, « Attacks on Machine Learning: Adversarial Examples in Connected and Autonomous Vehicles », in *2019 IEEE International Symposium on Technologies for Homeland Security (HST)*, nov. 2019, p. 1-7. doi: 10.1109/HST47167.2019.9032989.
47. F. Khalid et S. R. Hasan, « Chapter 9 - Hardware security of autonomous vehicles », in *Handbook of Power Electronics in Autonomous and Electric Vehicles*, M. H. Rashid, Éd., Academic Press, 2024, p. 125-138. doi: 10.1016/B978-0-323-99545-0.00012-9.
48. K. Sjoberg, « Resilience and Recovery [Connected and Autonomous Vehicles] », *IEEE Veh. Technol. Mag.*, vol. 16, nº 1, p. 93-96, mars 2021, doi: 10.1109/MVT.2020.3044123.
49. C. Roche, *TOTh 2010, Terminology & Ontology: Theories and applications*, vol. 2010. in TOTh 2010, Terminology & Ontology: Theories and applications, vol. 2010. Annecy, France: Institut Porphyre, Savoir et Connaissance, 2010. Consulté le: 22 mars 2025. [En ligne]. Disponible sur: https://hal.science/hal-01354936
50. K. Vanitha, M. S. Venkatesh, K. R. -, et S. V. Lakshmi, « The Development Process of the Semantic Web and Web Ontology », *Int. J. Adv. Comput. Sci. Appl.*, vol. 2, nº 7, 2011, doi: 10.14569/IJACSA.2011.020718.
51. S. Poyyamozhi, R. Yang, V. Krovi, R. Rai, B. Smith, et D. Kasmier, « Ontology Foundation for the Self-Driving Software Stack », 8 février 2025, *Social Science Research Network, Rochester, NY*: 5129199. doi: 10.2139/ssrn.5129199.