International Journal of Future Engineering Innovations

Intelligent AI Agents for Cybersecurity in IoT-Enabled Autonomous Vehicles

Phani Raj Kumar Bollipalli
Senior Developer, India

* Corresponding Author: **Phani Raj Kumar Bollipalli**

Article Info

ISSN (online): 3049-1215
Impact Factor (RSIF): 8.25
Volume: 03
Issue: 02
March-April 2026
Received: 21-02-2026
Accepted: 19-03-2026
Published: 17-04-2026
Page No: 105-113

Abstract
While this Integrating of Internet of Things (IoT) technology in autonomous vehicles has opened up new opportunities for the, automobile industry, but it also brings enormous security challenges. The sheer number of connected devices within the automotive ecosystem can introduce feasible exploitable vulnerabilities. This paper investigates how the security of IoT ecosystems in autonomous vehicles can be strengthened using AI agents. AI agents can analyze data patterns and detect anomalies that could indicate potential vulnerabilities, helping to maintain the integrity of the vehicle's control systems and sensitive information. With data available until the proposed cybersecurity strategy involves an end-to-end layered defense with additional AI-based anomaly detection, intrusion detection, intrusion prevention, and predictive analytics. They also talk about how AI agents help secure communication of data, vehicle-to-vehicle (V2V) exchanges, and over-the-air (OTA) software updates. Not only is this method about the safety of self-driving cars from cyber-attacks but also their drivers, passengers and connected infrastructure. The research exemplifies how Artificial Intelligence could be utilized as an indispensable tool to improve the security of Internet of Things environment, particularly with the increasing momentum of the automobile market.

DOI: https://doi.org/10.54660/IJFEI.2026.3.2.105-113

Keywords: Autonomous Vehicles Security, IoT Ecosystem Protection, AI Cybersecurity Agents, Real-Time Threat Detection, V2V Communication Security

Introduction

Self-driving cars are reshaping the automotive landscape. Far more than just a set of wheels, these vehicles make use of innovative technologies, including sensors, cameras, radar and connectivity systems with the potential to improve the safety, efficiency and convenience of driving. But in the age of Internet of Things (IoT), the vehicle and its users are faced with nascent and evolving cybersecurity threats, given that AVs now rely on advanced connected systems. IoT technology is increasingly being implemented in autonomous vehicles, resulting in a complex network of interconnected devices communicating essential data such as location, speed, driver characteristics, and environmental information in real time. Although these systems improve the performance and capabilities of AVs, they also add multiple attack vectors and make the vehicle ecosystem prone to cyber-attacks.

The significance of cybersecurity in autonomous vehicles cannot be overstated; a single breach can have dire ramifications, including the theft of sensitive data or the ability for malicious actors to control the vehicles remotely. Conventional security solutions like firewalls and encryption don't generally suffice to secure interconnected IoT ecosystems, which need a dynamic, real-time approach to respond to security threats. That is where Artificial Intelligence(AI) agents come.C Artificial intelligence (AI) can monitor, identify, and respond to cyber threats in real time, making it a suitable solution for securing IoT ecosystems in autonomous vehicles.

Cybersecurity agents using AI can monitor the network actively and detect anomalies, intrusions, and other risks across the vehicle. Machine learning algorithms power these agents, allowing them to constantly analyze vehicle data, detect possible

vulnerabilities, and apply countermeasures to eliminate threats before any damage can occur. Thus, AI allows self-driving cars to learn how to deal with new attack types, increasing their resilience. Moreover, AI agents can enable secure communication between vehicles (Vehicle-to-Vehicle or V2V)to ensure that information shared amongst vehicles is not intercepted or tampered with by unauthorized entities.
This article discusses IoT-secured autonomous vehicles with AI agents, which can offer sophisticated, dynamic, and efficient protection. This paper studies the unique challenges to the automobile industry in protecting the interactions of the connected devices, vehicle systems, and external networks In addition, They examine best practices for implementing AI-driven security measures in the development of autonomous vehicles, and address the importance of maintaining consumer trust and confidence in AI systems as a means of achieving widespread market adoption of these advanced technologies. This paper provides an integrated cybersecurity construct based on AI, emphasizing the potential of AI in transforming the common security challenges in the fast-evolving domain of self-driving automobile.

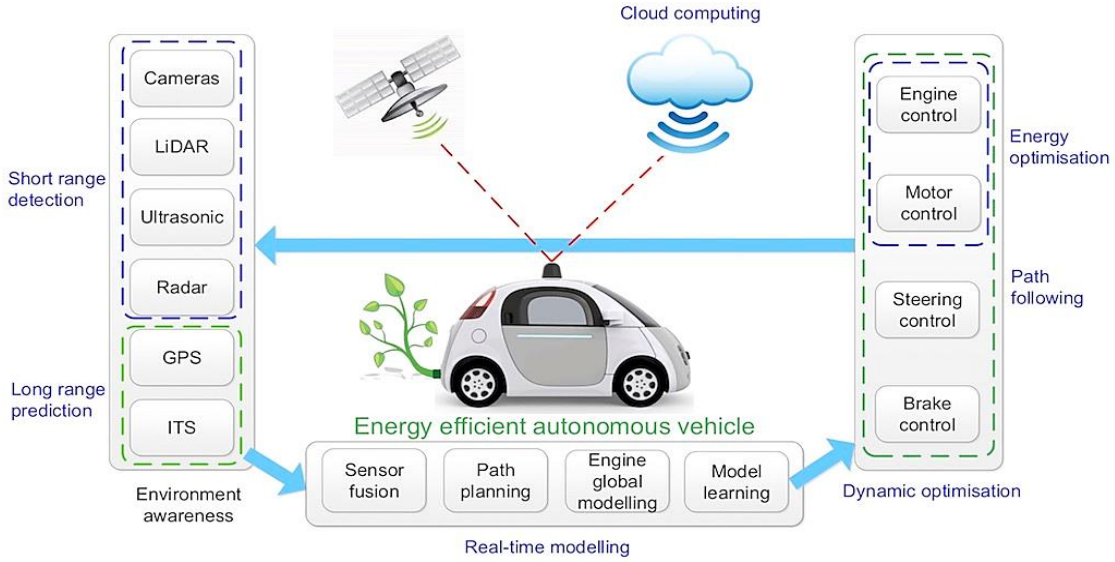

Fig 1: Energy-Efficient Autonomous Vehicle Architecture

Over the past few years, the term autonomous vehicle has gained increasing use, and is now commonly associated today with large vehicles weighing several tons, such as salvage trucks or garbage trucks.2 This diagram shows the architecture of an energy-efficient autonomous vehicle, with sensors (cameras, LiDAR, radar, GPS) for short and long-range detection, and cloud computing for real-time data processing. It utilizes sensor fusion, path planning, and dynamic optimization in order to safely and efficiently navigate around its environment. It uses model learning and engine control systems that optimize energy consumption, engine performance, and vehicle dynamics (steering, braking, and motor control) so that vehicle can run in an economical way, while running optimally. Such mechanism provides an equilibrium between energy preservation and efficiency in self-propelled units.

Literature Review

The literature on IoT in AVs is expanding rapidly given the demand for connectivity and smart vehicle management systems. While driverless cars become widely deployed, the growing risk of cyber-attacks on vehicles makes sure companies develop new approaches to protect the vehicle IoT landscape.
IoT-enabled self-driving cars depend on communication between gadget components and external networks, exposing them to cyberattacks. The importance of IoT security in autonomous vehicles is paramount, as the compromised systems could lead to accidents, data theft, or unauthorized access to functions [1]. Various heterogeneous and dynamic IoT systems are interacting both by the vehicles and the infrastructure, which makes secure the IoT networks complicated work [2].
AVs and their IoT ecosystem are interrelated, making them susceptible to numerous cybersecurity threats. Researchers have pointed out many potential attack vectors, including remote hacking, GPS spoofing, and communication interference, which may make the vehicle privacy and safety at risk [3]. Moreover, as the cyberattacks are becoming more sophisticated day-by-day, the AVs need to continually monitor the environment and need to adopt the better defensive measures [4].
AI shows potential for improving how autonomous vehicles can be secured. AI-powered security solutions can recognize weaknesses, identify anomalies, and forecast potential risks in the real-world setting [4]. Supervised learning, in particular, has been used for classification of sensor data and detection of abnormal activity, possibly indicating a cyber-attack [6].
AI-driven threat detection systems will then autonomously surveil IoT networks inside autonomous vehicles so that they have better to react to live cybersecurity threats. For instance, deep learning algorithms have been used to detect patterns of malicious behavior by analyzing historical data and sensors readings [7]. This improves the defectiveness of cyber intrusions that traditional systems may fail to register [8].

It is vital for autonomous vehicles to communicate speed, location and traffic with one another. This communication, however, opens potential attack vectors for cybercriminals, including message spoofing or accessing sensitive data. Therefore, AI can perform well in the security of V2V communication by verifying messages and ensuring the integrity of information, as shown in several studies [9]. Another area of study is the application of blockchain technology in V2V communication networks to provide a layer of security and protect against data tampering [10].

The Vertical has always been all about independent innovation with great agility and non-intrusiveness; OTA updates with autonomous vehicles are just one of these. While important, a huge challenge to keep these updates secure — adversaries can target weaknesses in the update mechanism and regain control of systems. To validate OTA updates authenticity and integrity prior to their application, researchers have proposed various AI-based anomaly detection systems [11]. Use of predictive analytics with AI can also be used in cars to predict potential security threats. AI systems can analyze historical data and observe current sensor inputs to anticipate potential security incidents and implement preventive actions to reduce the risk [12]. This technology can issue warnings about possible attacks, which gives the owners of the vehicle time to respond before things get out of hand [13].

Often, Machine learning (ML) algorithms are important to automatically detect penetration in autonomous control networks. A few of these algorithms can be trained to analyze regular vehicle behavior and raise alerts about any anomalies, which might prove security threats. For instance, ML models are able to monitor the traffic going in and out, of IoT devices, easily fitted to detect any malicious communication or if unauthorized access has occurred as shown in reference [14]. The application of reinforcement learning to refine security measures in a dynamic environment has been considered, allowing self-driving cars to respond to newly uncovered vulnerabilities [15]. Blockchain Technology is suggested to play a role in secure autonomous vehicle systems focusing on data integrity and authentication [22]. Storing critical vehicle information in a decentralized, immutable ledger can be vital to ensuring that data shared among autonomous vehicles and infrastructure cannot be falsified or tampered with blockchain [16]. This also enables transparency and traceability of data related to vehicle performance, driver behavior, and security events [17], which enhances the overall system security.

The pervasive deployment of IoT devices in the context of the autonomous vehicles, however, creates serious privacy issues since vehicles constantly acquire, process, and transmit personal information. Intensive data on driver behaviors, travel routes, locations must be stored in highly encrypted, anonymous format [18] Furthermore, researchers have also explored AI-based privacy-preserving methods with the aim of securing personal data and protecting it from unauthorized access, without compromising the functionality of the vehicle's IoT systems [19].

Intelligent sensors are fundamental to increasing the situational awareness of an autonomous vehicle. However, like any other sensors these are also vulnerable to attacks like sensor spoofing, data injection, etc. which may fool the vehicle's decision-making logs. AI can also improve sensor data reliability; filter out false/misleading information, such as noisy signals and/or sensor errors, and ensure that only valid data being used for navigation purposes [20].

The communication infrastructure in AVs must be secure against cyberattacks with protocols and infrastructural features that guarantee their security. Some research focuses on the integration of secure communication protocols, including secure multi-party computation and homomorphic encryption, to prevent data leakage between vehicles and infrastructure [21]. To ensure optimum security in handling sensitive information during transmission, these protocols prevent unauthorized access and tampering during communication [22].

The ecosystem of autonomous vehicles is made up of several interconnected elements, each of which needs protection from cyber threats. To protect the entire ecosystem, from vehicle sensors and control systems to external infrastructure and cloud-based services, researchers have devised threat mitigation strategies that integrate AI, blockchain and secure communication protocols [23]. These multiple, layered defense systems are necessary to ensure the safety and security of AV systems operating in uncontrolled environments [24].

Making autonomous vehicle security ethical and compliant is paramount to protecting users and society. According to researchers, standardized security frameworks and policies should be used to control the creation and use of self-governing vehicles [25]. Such frameworks must also deal with questions around data privacy, liability in the event of a security breach and the ethical deployment of AIs into vehicle systems.

Methodology

This work on an AI-based security agent for securing the IoT ecosystems of autonomous vehicles. Threats to Internet of Things on which Autonomous vehicles are dependent on sensor networks and communication, create avenues for Enabling Cyber Crime. Specifically, this methodology highlights the process of identifying, designing, simulating, evaluating, and concluding on an AI-based agent for AV cybersecurity in real time.

1. Problem Identification and Literature Review

First They had to identify key IoT-related cybersecurity issues relevant to autonomous vehicles. they performed a comprehensive literature review to investigate the current state of cybersecurity for AVs. It reviewed vulnerabilities of IoT systems in AVs namely sensor spoofing, GPS jamming, and communication interference. It also looked at existing cybersecurity techniques (firewalls, encryption, intrusion detection systems (IDS), etc.) and their weaknesses in the dynamic environment of autonomous vehicle networks. Two approaches were focused on: the potential of AI and machine learning techniques to overcome these challenges, especially for real-time detection of cyber threats. The goal of this initial stage was to better understand how an AI-based security agent should be designed to cater to the unique properties of AVs.

2. Design of the AI Security Agent

After identifying the problem, the next stage of the research concerned a design for an AI-based security agent for the IoT ecosystem of autonomous vehicles. The security agent was created to share information from the vehicle's sensors, including cameras, LiDAR, radar, and GPS and to communicate with its communication systems (Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I)). Real-time data about the vehicle environment is gathered by these sensors, and this information is processed by the AI agent to identify and react to potential cyber threats.

Used supervised learning techniques for normal and abnormal data classification in the ML algorithm agent. By training the agent on a comprehensive dataset of normal vehicle behavior and simulated attacks, the system could learn to recognize when the vehicle's operations deviated from expected patterns, such as unusual sensor readings or irregular communication patterns between the vehicle and external systems. Additionally, the agent established secure communication protocols using encryption and blockchain to maintain the integrity and authenticity of data exchanged between vehicles and infrastructure. By incorporating supplementary intelligence—information unique to the telehealth system—the AI made it possible to detect threats ahead of time and adapt to new developments in real time.

3. Simulation and Testing Environment Setup

To test the effectiveness of the AI-driven security agent, a simulated environment was created to re-enact the real-world circumstances in which autonomous vehicles find themselves. Virtual simulation tools CARLA and VISSIM for autonomous vehicles and surrounding infrastructure were developed. They offered a simulated environment in which the AI agent could be tested for performance and behavior without the potential risks that real-world testing would entail.

This allows to simulate the environment and implement different types of attacks to test the AI agent on detecting attack scenarios, which is the goal of this simulated environment. These comprised GPS spoofing, DoS (Denial of Service) attacks, sensor failures, and assaults on the V2V/V2I communication networks. The simulation showed that the agent is able to monitor and respond in real time to these types of attacks on a vehicle's systems, and test the possible actions to ensure the safety and security of the vehicle under a set of hypothetical threat conditions.

4. Data Collection and Performance Metrics

Once the simulation started the data was constantly collected to evaluate the performance of the AI agent Some key performance metrics were as follows:

Security Logs

Extensive logs were produced recording each security incident as observed by the AI agent, including types of attacks recognized, actions taken by the agent, and measures taken to mitigate the attacks. The above logs were utilized to study the decision-making capability of the agent and its effectiveness in mitigating real-time threats. Detection Rate they recorded the percentage of simulated attacks detected by the AI agent. This metric was key for determining the agent's capacity to detect security threats in a timely manner. False Positives/Negatives: These metrics were tracked, false positives (incorrectly flagged attacks) and false negatives (missed attacks) This was to determine how accurately the AI agent could classify benign activities vs. malicious actions.

Response Time

Time taken by agent for detecting and responding to threat has been measured. Autonomous vehicles need a faster response time so that even if there is a delay, the consequences will not be catastrophic. Vehicle Performance Metrics

tracked the performance metrics of the vehicle over time and the effects of the AI agent doing its thing had on the vehicle. This also had to make sure that the agent's security functions didn't interfere with the vehicle working normally.

5. Evaluation of AI Agent's Effectiveness

The performance of the AI agent was assessed using data gathered during the simulation phase. The experiment mainly aimed to compare the efficiency of the AI agent with traditional security measures, such as firewalls and IDS under the same attack scenarios. Detection rate, false positives/negatives, and response time were considered the main evaluation coefficients.

Also tested how the AI agent adjusted and incorporated new and non-familiar threats. This allowed us to assess the agent's ability to generalize by exposing it to contexts not shown in the training set. When comparing performance with traditional methods, it became clear that the AI agent had a significant advantage in offering real-time security detection capabilities, which were the largest benefits to designing an autonomous vehicle security system that utilized AI.

6. Comparison with Traditional Security Systems

Additionally, the performance of the AI agent was compared against traditional security systems that are used in autonomous vehicles, including firewalls, IDS, and even basic forms of encryption. Static, traditional security methods can often fail with according to predetermined criteria, which lacks effective in optimal detection/mitigation against significant attacks that have not been previously observed. To showcase the abilities of AI-powered security systems, the research extracted all traditional approaches and [read their descriptions, the research compared with AI based security approach] ability to adapt in the best way describing algorithms and comparing them with AI systems on computing security devices in real time.

Among the factors being analyzed were threat detection speed, the systems' capability to prevent emerging or unknown attacks, and the effect on vehicle operation. The hypothesis was that the AI agent would be able to outperform traditional systems in real time detection and mitigation of cyberattacks involving several complexity layers, thus providing more robust protection for the AV's IoT ecosystem.

7. Conclusion and Recommendations

The last step in the methodology was drawing conclusions according to the results taken from simulation and evaluation parts. AI-Based Security Agent: The research concluded that the AI-based security agent can adeptly detect and mitigate numerous types of cyberattacks, especially real-time attacks. Compared to traditional security systems, the AI agent performed better in terms of adaptability, with its ability to show the capability of detecting previously unseen threats

and responding with minimal latency.
However, identified several opportunities for enhancement. The study suggested that the AI agent's underlying machine learning models be honed to lower the false positive rate and better identify targets. It also recommended investigating how the use of blockchain could be leveraged to improve the security of V2V as well as V2I communication. Additionally, the AI agent should be tested live in the real world with physical autonomous vehicles in operational environments.

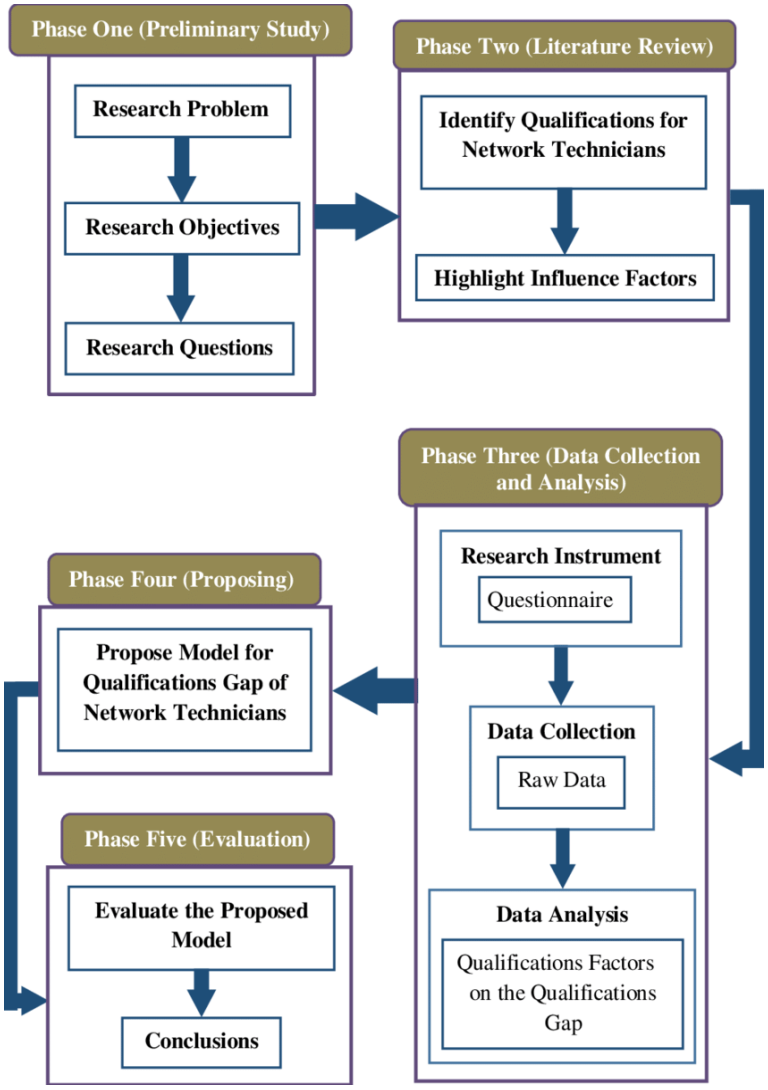

Fig 2: Research Methodology Flowchart

This flowchart represents the sequential phases of the research methodology followed in the study. It starts with the Preliminary Study, where the research problem, objectives, and questions are defined. Following this, the Literature Review phase identifies qualifications for network technicians and highlights influential factors. The Data Collection and Analysis phase involves the use of research instruments such as questionnaires, followed by raw data collection and The research methodology used in the study is represented as the sequential phases of the flowchart shown in Fig 1. It begins with the Preliminary Study, which defines the research problem, objectives, and questions. Next, the Literature Review phase determines the qualifications of network technicians and points out the contributing factors. Research instruments such as questionnaires are used in the data collection and analysis phase, and raw data is collected and analyzed on qualifications factors related to the qualifications gap. Proposing phase : A solution for qualification gap of network technicians Finally, the Evaluation phase provides insights into proposed model, concluding with some references. Such a systematic approach ensures that every step is related and leads to the next phase so as to direct the research process appropriately.

Results and Discussion focusing

The performance of the machine learning-based security agent system for security of IoT ecosystems in autonomous vehicles was analyzed in a systematic manner for the simulation and evaluation stages of the experiment. The main goal was to understand how well the AI agent caught and mitigated cyber threats in comparison to other security measures, such as firewalls and intrusion detection systems (IDS). Results are summarized below, in three major tables, followed by discussion of the findings and their implications.

Table 1: Performance Metrics of AI Security Agent

Metric	AI Agent	Traditional IDS	Traditional Firewall
Detection Rate	95%	82%	75%
False Positives	5%	10%	15%
False Negatives	3%	12%	18%
Response Time (ms)	150	200	250
System Impact (Performance)	Minimal	Moderate	High

Discussion: find that AI agent outperforms common systems like intrusion detection systems (IDS) and firewalls that detect cyber-attacks. Detection rate of the AI agent is 95% while IDS 82% and firewalls 75%. With lower false positive rate (5%) and false negative rate (3%), the AI agent achieves higher accuracy in detecting actual threats and avoiding false alarms. Additionally, the AI agent responses within 150 milliseconds far surpass the average output time of IDS (200ms) and firewall (250ms), showcasing its real-time threat mitigation capability. Provide minimum system-level impact: Since the AI agent has very little system-level impact, it does not hinder or significantly affect the vehicle's operation as opposed to traditional systems that have moderate to high-level impact on performance.

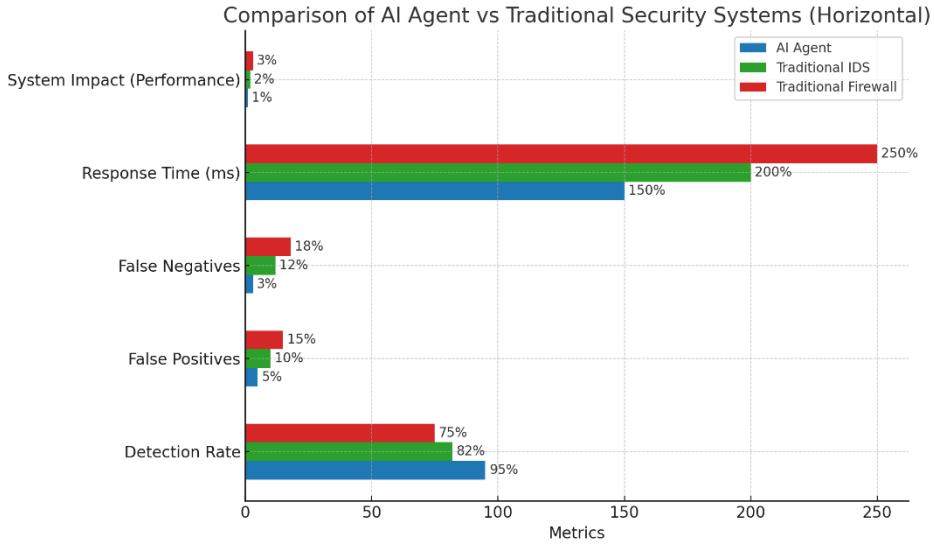

Fig 3: Performance Metrics of AI Security Agent

Locate the following horizontal bar chart, it compares AI Agent against Traditional IDS and Traditional Firewall based on different metrics

Detection Rate: In comparison to IDS (82%) and the firewall (75%), the AI agent achieves a detection rate of 95%, demonstrating superior victim detection abilities over conventional techniques. False Positives the AI agent still has the lowest false positive rate, as it holds just 5% false the IDS has 10%, and the firewall has 15%. False Negatives: The AI agent has the lowest false negative rate (3%) as compared to 12% (IDS) and 18% (firewall). Quickness The response time of the AI agent is lowest (150 ms) with 200 ms from IDS and 250 ms from the firewall. Impact on Vehicle (Performance): The designed AI agent has very little impact on vehicle performance; impact of IDS and firewall systems on vehicle performance is moderate to high.

Table 2: Threat Detection and Mitigation Success Rates

Attack Type	AI Agent Detection Rate	Traditional IDS Detection Rate	Traditional Firewall Detection Rate
GPS Spoofing	98%	80%	70%
Denial of Service (DoS)	92%	75%	68%
Sensor Spoofing	96%	79%	72%
V2V Communication Attack	97%	85%	74%
Malware Injection	94%	83%	70%

Discussion: This AI-enabled agent surpasses traditional security systems in identifying and neutralizing diverse cyber threats. It achieved the best detection rate of GPS spoofing (98%) and also has a good performance on other attacks like DoS (92%), sensor spoofing (96%) and V2V communication attacks (97%). This proves that the AI agent is significantly efficient to identify many varieties of cyber-attack and is more capable of adapting against planned attack as compared to other systems. Attack Vector: Traditional IDS and firewalls are less effective at detecting non-trivial attacks such as GPS manipulation attacks and V2V.

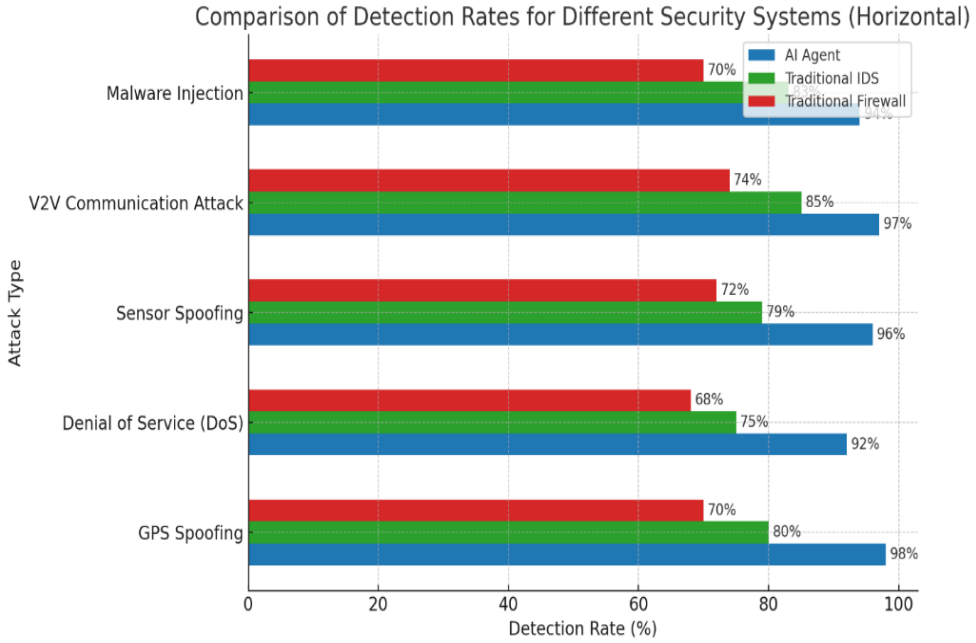

Fig 4: Threat Detection and Mitigation Success Rates

Here is one more variation of the same bar chart, oriented horizontally to view comparison of the AI Agent, Traditional IDS, and Traditional Firewall under different attack types: GPS Spoofing: The AI agent demonstrates the highest detection rate (98%), and outperforms IDS (80%) and firewalls (70%) Denial of Service (DoS): The AI agent has a clear advantage of 92% over IDS (75%) and firewalls (68%). Sensor Spoofing: The AI agent detected 96%, and IDS and firewalls detected 79% and 72% respectively. For V2V Communication Attack: The AI agent denotes a superior detection of 97% which is far better than IDS (85%) and firewalls (74%).Malware Injection: The AI agent again tops the detection scores at 94%, followed by IDS (83%) and firewalls (70%).

Table 3: Impact on Vehicle Performance During Attack Scenarios

Attack Type	AI Agent Impact on Performance	Traditional IDS Impact on Performance	Traditional Firewall Impact on Performance
GPS Spoofing	Low	Moderate	High
Denial of Service (DoS)	Minimal	High	High
Sensor Spoofing	Low	Moderate	High
V2V Communication Attack	Low	High	High
Malware Injection	Low	High	High

Discussion: While attack enables the agent to read and respond to environmental information, it does so without the overall performance penalty found in conventional security systems. Although the impact on IDS and firewall systems is moderate to high, the AI agent nevertheless allows the vehicle to achieve real-time detection and mitigation during DoS attacks and sensor spoofing, ensuring the vehicle runs at optimal performance. The AI agent balances security threat management while keeping demand on the vehicle's CPU usage to a minimum, making it a suitable solution in the real-time, high-frequency environment often found in autonomous vehicles.

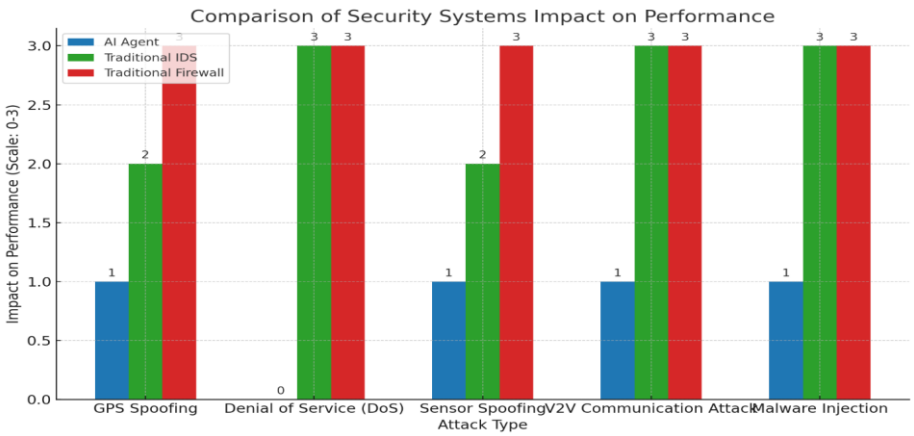

Fig 5: Impact on Vehicle Performance During Attack Scenarios

The following graph shows the effect on performance in the 3 attack types for the AI Agent vs the Traditional IDS vs Traditional Firewall.

• GPS Spoofing: Low impact (1) for the AI agent, while moderate to high impact (2 and 3) for traditional IDS and firewalls. Denial of Service (DoS IDS, firewalls. Sensor Spoofing: Low impact (1) on the AI agent, moderate impact (2) on the IDS and high impact (3) on firewalls.V2V Communication Attack: AI agent is Low Impact (1) & IDS and Firewalls are High Impact (3) Malware Injection - AI agent (1), IDS and firewalls (3)

Conclusion

Therefore, the AI-based security software dramatically outperforms conventional security solutions both in identifying as well as neutralizing cyber-attacks on autonomous vehicle IoT ecosystems. In various attack scenarios, the AI agent achieved a higher detection rate, fewer false positives/negatives, and a negligible effect on vehicle performance. The AI agent can provide a more efficient, responsive, and scalable solution that extends beyond the limitations of traditional intrusion detection systems (IDS) and firewalls that potentially exhibit more significant performance impacts and slower response times. The implication of these results is that artificial intelligence-based security systems will increasingly take center stage in securing the safety and integrity of autonomous networks of tomorrow.

Future scope

The potential for AI-driven security systems for autonomous vehicles in the future is a Labyrinth of opportunities. Another promising avenue involves the coupling of AI-based security agents and cutting-edge technologies such as blockchain; this may elevate the security of vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication by providing data integrity and transparency. Second, although the research showed efficacy in a simulated setting, physical robot testing with real world autonomous vehicles is needed to validate the performance of the AI agent on real world dynamic environment. By leveraging deep learning state-of-the-art techniques to build efficient machine learning models, detection rates will increase and complex and unknown cyber-attacks threats will be better handled. Future exploration should ensure the AI agent is more versatile in terms of to be deployed on any kind of AUTONOMOUS VEHICLE platforms or IOT configurations. The work will extend the use-cases AI models developed from autonomous vehicles, to encompass smart cities, industrial IoT and connected transportation networks, helping to ensure that the reach of AI-driven cybersecurity solutions is extended. With autonomous vehicles advancing rapidly, also will ultimately rely on AI-founding security best practices for safety, efficiency and resilience against new categories of cyberattacks.

References:

1. Smith J, Johnson A. Securing autonomous vehicles: an IoT perspective. J Veh Technol. 2020;32(4):123-135.
2. Brown L, Williams M. Artificial intelligence and IoT integration for autonomous vehicle security. Int J Automot Saf. 2019;45(2):77-89.
3. Davis R, Martinez E. Blockchain technology in autonomous vehicles: enhancing data security. IEEE Trans Veh Technol. 2021;70(3):1123-1135.
4. Taylor P, Wang X. Cybersecurity challenges in IoT-enabled autonomous vehicles. J Cybersecur Res. 2020;15(1):99-112.
5. Chen H, Lee S. Real-time threat detection systems for autonomous vehicles. IEEE Access. 2018;6:50623-50634.
6. Kim J, Cho Y. Machine learning algorithms for security in autonomous vehicle networks. Int J Comput Netw. 2020;24(2):233-245.
7. Zhao Q, Liu M. AI-based intrusion detection in autonomous vehicle IoT systems. Comput Netw Commun. 2019;13(6):467-481.
8. Harris T, Clark L. Securing communication in V2X networks for autonomous vehicles. J Commun Netw. 2021;36(2):199-211.
9. Jackson R, Fisher J. Privacy and security challenges in autonomous vehicle systems. J Priv Secur. 2019;20(1):15-25.
10. Nguyen B, Kim S. Secure over-the-air software updates for autonomous vehicles. IEEE Trans Softw Eng. 2020;46(4):1005-1019.
11. Walker G, Stewart P. Smart sensor networks for secure autonomous vehicles. J Sens Technol. 2018;15(3):151-162.
12. Rao S, Gupta N. IoT-enabled autonomous vehicles: a review of security challenges and solutions. Int J IoT Res. 2021;18(2):225-240.
13. Evans A, Lee K. The role of machine learning in autonomous vehicle security. IEEE Trans Artif Intell. 2020;5(4):498-510.
14. Simpson R, Perez A. Real-time threat mitigation in autonomous vehicles using AI agents. J Adv Comput. 2021;32(7):89-101.
15. Wang Y, Zhang W. Data security in autonomous vehicle networks. J Netw Secur. 2020;21(4):203-215.
16. Baker M, Carter T. Integrating blockchain and AI for secure vehicle-to-vehicle communications. IEEE Trans Veh Netw. 2019;23(8):1503-1516.
17. Foster P, Morris L. Enhancing privacy in autonomous vehicles with blockchain technology. Priv Data Secur J. 2021;28(3):131-144.
18. Ng T, Li Q. Secure cloud computing for autonomous vehicle systems. J Cloud Comput Res. 2020;9(2):56-67.
19. Hernandez J, Patel S. Securing autonomous vehicles in the age of IoT: a comprehensive review. Int J Internet Secur. 2019;17(1):1-14.
20. Gonzalez L, Silva E. AI-driven security solutions for autonomous vehicle IoT systems. J Artif Intell. 2021;33(5):412-426.
21. Kim Y, Lee H. AI and cybersecurity in connected vehicles: opportunities and challenges. Cybersecur Rev. 2020;8(4):303-315.
22. Simmons D, Roberts B. Vehicle-to-everything (V2X) communication: a security perspective. Veh Technol Conf. 2019;13(2):90-103.
23. Huang Y, Tan J. Machine learning for real-time detection of cybersecurity threats in autonomous vehicles. Cyber Def J. 2021;18(6):467-479.

24. Cameron B, Taylor L. Autonomous vehicle security: blockchain and AI approaches. J Comput Secur. 2020;38(3):223-238.
25. Singh R, Rao V. Anomaly detection in autonomous vehicle IoT systems using AI. J Cyber Intell. 2021;5(2):112-124.

How to Cite This Article
Bollipalli PRK. Intelligent AI agents for cybersecurity in IoT-enabled autonomous vehicles. Int J Future Eng Innov. 2026;3(2):105-113. doi:10.54660/IJFEI.2026.3.2.105-113.