Adaptive Security Architecture for Intelligent Vehicles Using Hybrid IDS-IRS Integration

Srinivasarao Thumati, Desidi Narsimha Reddy, M Venkateswara Rao, Tirumalasetti Lakshmi Narayana, Venkateswari ketineni, Vadali Pitchi Raju

Abstract—**Strong cybersecurity protocols must be put in place to protect against possible cyber breaches, especially with the proliferation of autonomous vehicles. The purpose of this research is to determine whether it is possible to develop an intelligent vehicle-specific autonomous intrusion response system (IRS). In order to determine the best course of action in the event of an intrusion, the IRS's suggested system can do so in real time and in a dynamic manner. Some of the important contributions include a comprehensive review of different response methods, a framework for evaluating costs and impacts dynamically, and the use of selection algorithms such as Simple Additive Weighting (SAW), Linear Programming (LP), game theory, and AI-driven applications. Extensive testing has proven that the system works well in terms of reaction speed, resource usage, and overall effectiveness. This demonstrates how the technology may greatly improve car safety. The results of this study lay the groundwork for the IRS to build better and more adaptable frameworks in the future.**

Index Terms—**Autonomous vehicles, Intrusion response system, Cybersecurity, Intelligent vehicles, Linear Programming, Game theory, AI-based mechanisms**

I. Introduction

THE Intelligent vehicles, made possible by lightning-fast technological development, enhance safety, efficiency, and the user experience with the integration of sophisticated software, sensors, and communication systems. These vehicles represent the mobility of the future; they often have autonomous driving capabilities, advanced driver assistance systems (ADAS), and seamless communication. Nonetheless, the growing intricacy and interconnectivity of intelligent vehicles render them vulnerable to various cybersecurity threats, positioning them as prime targets for malicious attacks [1]. Cyber intrusions in intelligent vehicles can lead to severe outcomes, including unauthorized access to vehicle systems and the total takeover of vehicle functions. Such intrusions pose a significant risk to passenger safety, can disrupt traffic flow, and may be leveraged for unlawful activities. The critical nature of these threats demands the creation of strong security measures capable of detecting, assessing, and responding to intrusions in real-time [2]. Conventional security measures, including firewalls and intrusion detection systems (IDS), have become inadequate in the realm of intelligent vehicles, given their dynamic and real-time operational contexts. An autonomous intrusion response system (IRS) is essential, capable of not only detecting intrusions but also autonomously determining and implementing suitable responses to lessen the effects of these threats. An effective IRS for intelligent vehicles should evaluate the nature and severity of the intrusion, taking into account the potential impact on vehicle safety and performance, and choose the most appropriate response strategy from various options [3]. Many individuals are increasingly recognizing the potential security vulnerabilities associated with smart vehicles. Consequently, vehicles need to possess the ability to respond swiftly to cyber threats. To achieve that capability, it is essential to address three fundamental questions. Refer to Figure 1 for Q1: In this scenario, what are the possible courses of action? Question 2: What criteria should be applied when evaluating these responses Question 3: In what ways can the assessment of these responses inform the selection of one or more during runtime? This article aims to explore and categorize potential responses to these issues by analyzing the impacts of various cyber-attacks. The investigation further encompasses a cost-benefit evaluation of assaults and responses, alongside a dynamic risk assessment, utilizing data including attack specifics and vehicle status. This evaluation facilitates the selection of appropriate responses. The study also examines various methods of response selection, highlighting the most effective ones for automobile systems [4]. This study investigates the design and implementation of an IRS specifically tailored for intelligent vehicles. The IRS operates on a framework of dynamic cost and impact evaluation, enabling it to evaluate the outcomes of different response strategies in real-time. The system utilizes a range of algorithms to ensure, such as Simple Additive Weighting (SAW), Linear Programming (LP), and AI-based mechanisms [5].

Manuscript received April 16, 2025; revised July 30, 2025.

Srinivasarao Thumati is an Assistant Professor in the Department of Electrical and Electronics Engineering, Prasad V Potluri Siddhartha Institute of Technology, Vijayawada, Andhra Pradesh, India (e-mail: srinuthumati@gmail.com).

Desidi Narsimha Reddy is a Data Consultant of Soniks Consulting LLC, USA (e-mail: dn.narsimha@gmail.com).

M Venkateswara Rao is a Professor and HOD in the Department of Computer Science and Engineering, Vignana Bharathi Institute of Technology, Ghatkesar, Hyderabad, Telangana, India (e-mail: venkat2m2@gmail.com).

Tirumalasetti Lakshmi Narayana is an Assistant Professor in the Department of Electrical and Electronics Engineering, Aditya University, Surampalem, Andhra Pradesh, India (e-mail: tlaxman17@gmail.com).

Venkateswari ketineni is an Assistant Professor in the Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Guntur, Andhra Pradesh, India (e-mail: venkateswariketineni@gmail.com).

Vadali Pitchi Raju is a Professor of Department of Mechanical Engineering, Indur Institute of Engineering & Technology, Siddipet, Telangana, India (e-mail: vpraju2000@gmail.com).

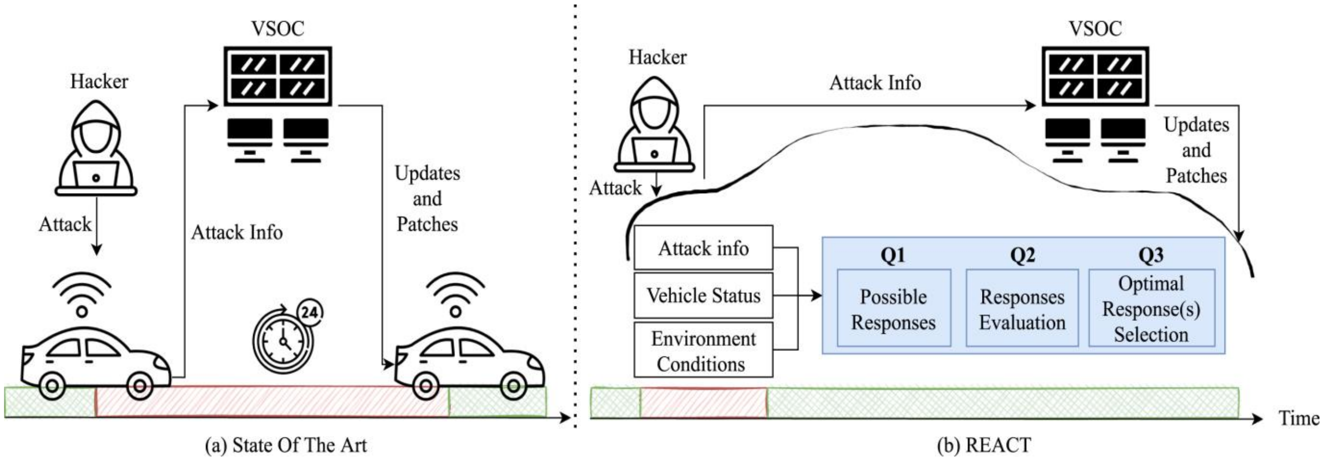

Fig. 1. Existing system delays patching via VSOC.

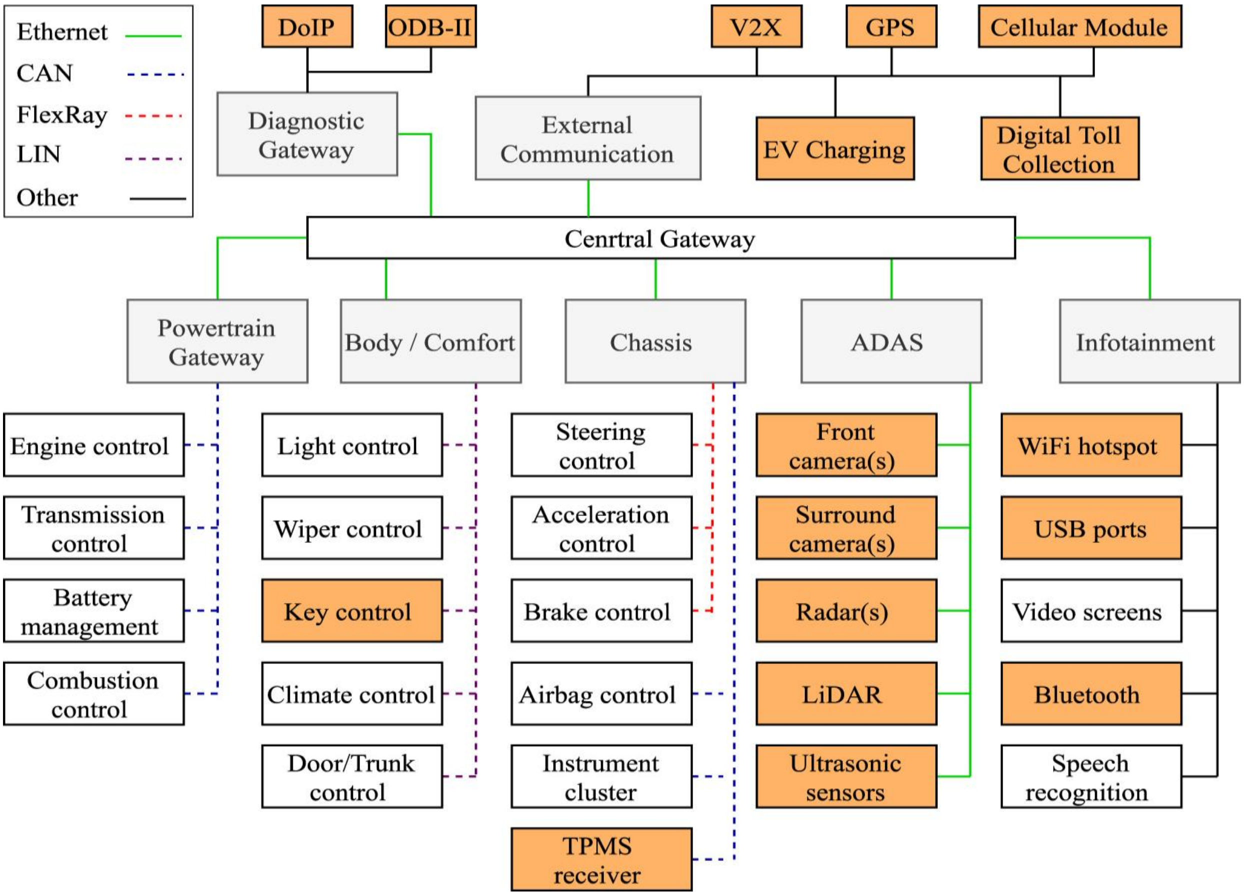

Fig. 2. Reference vehicle design with potential assault surfaces.

The selection of these algorithms is based on their capacity to address the distinct challenges presented by the automotive environment, including limitations in resources, the necessity for real-time decision-making, and the demand for exceptional reliability. This study aims to enhance the security and resilience of intelligent vehicle systems by establishing a solid framework for autonomous intrusion response. This paper seeks to tackle the distinct challenges presented by the automotive environment, with the goal of advancing the development of next-generation vehicle security systems that can effectively protect the intricate, interconnected systems that characterize contemporary transportation [6].

To understand the incorporation of IRS into contemporary vehicles and the possible responses they provide, it is essential to first examine their system architecture. Figure 2 presents a typical, practical, and thorough reference architecture frequently found in modern vehicles. A contemporary automobile consists of intricately linked subsystems. The figure demonstrates that modern vehicles are equipped with a multitude of embedded devices, known as ECUs, which are strategically placed throughout the vehicle and interact with each other via different network types, such as CAN, Flexray, and Ethernet. ECUs are classified into different domains or zones based on their functionalities, including infotainment, Advanced Driver Assistance Systems (ADAS), and powertrains. Alongside ECUs, modern vehicles feature a variety of sensors (including cameras and LiDAR), advanced communication technologies for external connectivity, and diagnostic ports (such as OBD-II). These elements collectively establish a significant attack surface for a range of potential threats and attacks.

II. Effective Approaches for Addressing scenarios

In the realm of intelligent vehicles, addressing a cyber-intrusion requires a prompt and efficient response, given that the implications frequently pertain to passenger safety, the integrity of vehicle systems, and the protection of sensitive data. An autonomous intrusion response system (IRS) must be equipped with a variety of response strategies that can be dynamically selected according to the nature and severity of the intrusion, the operational state of the vehicle, and the potential impact on its functionality. When developing response strategies, the initial factor to consider is the timing of the response [7]. Immediate responses are initiated promptly upon detection of an intrusion, with the objective of neutralizing the threat before it can inflict substantial harm. Instances encompass the prevention of harmful data packets, the segregation of affected systems, or the activation of a secure mode in essential vehicle components. These responses are generally utilized in scenarios where the intrusion presents an urgent risk to safety or the operation of the vehicle. Delayed responses entail observing the intrusion over a period before determining the most suitable course of action. This methodology proves beneficial in scenarios where the intrusion does not pose an immediate danger or when additional data is required to comprehend the complete extent of the threat. Delayed responses could entail the collection of further forensic data, notifying the driver or a remote security team, or getting the vehicle ready for a more thorough countermeasure [8]. Response strategies may be classified into two distinct categories: passive and active. Passive responses consist of unobtrusive actions that do not directly disrupt vehicle operations. These may encompass documenting the intrusion for subsequent examination, revising security protocols, or modifying the vehicle's threat detection settings [9]. Passive responses are generally employed when the intrusion is considered low-risk or when an active response might lead to unnecessary disruption. Active responses, on the other hand, entail direct intervention in the vehicle's systems to mitigate the intrusion. This may entail disabling specific vehicle functions, redirecting data streams, or implementing intricate countermeasures such as system reboots or software rollbacks. Proactive measures are essential when the intrusion presents a considerable risk to the vehicle's safety or operational integrity [10]. Proactive strategies encompass anticipatory measures implemented to avert intrusions from happening initially or to mitigate their effects should they arise. These strategies encompass consistent security updates, ongoing surveillance of system vulnerabilities, and the application of adaptive security mechanisms that progress in reaction to new threats. Proactive responses are crucial for sustaining a strong security posture in intelligent vehicles, as they diminish the chances of successful intrusions [11].

Reactive strategies are implemented following the detection of an intrusion, concentrating on alleviating its impacts and reinstating standard vehicle operations. Reactive responses generally demand more resources, as they involve real-time decision-making and prompt actions to mitigate threats. An effective IRS must integrate both proactive and reactive strategies to provide thorough protection against various cyber threats. Another important aspect to consider is the extent of the response. System-level responses encompass actions that influence the whole vehicle, including initiating a global reset, activating a safe mode, or disabling communication interfaces [12]. Such responses are generally designated for critical intrusions that jeopardize the vehicle's overall safety or integrity. Responses at the component level specifically address systems or components that have experienced compromise. For instance, an IRS could identify a faulty sensor, sever communication with a compromised external device, or deactivate a particular software module. Responses at the component level offer greater precision and can effectively uphold the overall functionality of the vehicle while tackling the specific intrusion. Although the objective of an IRS in intelligent vehicles is to function independently, there are situations where human involvement may be required. Automated responses are carried out without any human intervention, depending solely on the IRS's algorithms to evaluate the circumstances and determine the most appropriate course of action. These responses are essential in situations that demand swift decision-making, particularly when the vehicle is in motion and immediate threats need to be addressed. Human-in-the-loop responses entail notifying a human operator—like the vehicle's driver or a remote security team—who can subsequently make decisions or override the automated system. This method proves beneficial in intricate or unclear scenarios where human discernment is essential to reconcile security requirements with operational factors [13]. The IRS ought to be structured to work harmoniously with human operators, equipping them with the essential information needed for informed decision-making. Ultimately, the IRS faces the decision of choosing between customized and standard responses. Responses are tailored to fit the specific nature of the intrusion and the operational context of the vehicle. For example, if an intrusion aims at a vehicle's navigation system, the response team might concentrate on isolating and securing that system while ensuring that other functions remain unaffected. Customized responses tend to yield better results, though they necessitate more intricate decision-making processes [14]. In contrast, generic responses are established actions that can be utilized across a broad spectrum of intrusions. These could encompass fundamental actions such as initiating a safe mode or severing connections with external networks. Although they may lack the precision of customized replies, generic responses are easier to implement and can serve as a swift and dependable method for mitigating threats. The effectiveness of an IRS in intelligent vehicles hinges on its capacity to choose the most suitable response strategy for a specific situation. By integrating a variety of response strategies—spanning immediate and proactive measures to delayed and reactive actions—the

IRS can establish a strong defense against cyber intrusions, safeguarding the safety and integrity of intelligent vehicles in a progressively connected world [15].

III. Evaluation of Costs and Impacts That Are Dynamic

In the realm of intelligent vehicles, a robust intrusion response system (IRS) needs to dynamically assess the costs and impacts linked to intrusions and their respective responses. This assessment is essential for guiding decisions that harmonize security needs with the operational demands of the vehicle. By analyzing the different elements that affect the cost and consequences of both intrusions and responses, the IRS can enhance its strategies to reduce potential harm while maintaining vehicle performance. Intrusions in intelligent vehicles can differ significantly in their characteristics, intensity, and possible outcomes [16]. To effectively evaluate the consequences of an intrusion, the IRS needs to take into account various factors:

The intensity of an intrusion plays a crucial role in assessing its possible effects on the vehicle. Severe intrusions that affect essential systems, including braking, steering, or communication networks, present urgent risks to passenger safety and the overall integrity of the vehicle. Conversely, low-severity intrusions, like minor data breaches or efforts to access non-critical systems, might not have an immediate impact but still deserve scrutiny. The particular systems that are the focus of an intrusion significantly affect its overall consequences. For instance, a breach impacting the vehicle's autonomous driving system could lead to severe repercussions, whereas a breach aimed at the infotainment system may cause inconvenience without posing any immediate threat. The IRS should prioritize responses according to the importance of the impacted systems [17].

Certain intrusions possess the capability to spread throughout the vehicle's network, impacting various systems or extending to other connected vehicles or infrastructure. The IRS needs to assess the probability of such propagation and implement measures to mitigate the intrusion before it leads to extensive harm. The duration required to identify an intrusion is a significant consideration. Timely identification facilitates more efficient interventions, possibly averting the escalation of the intrusion. Nevertheless, late identification can elevate the intricacy and expense of the necessary response, as the breach may have already inflicted considerable harm or jeopardized several systems. The context surrounding an intrusion can greatly affect its consequences. For example, an intrusion identified when the vehicle is stationary may be considered less critical than one identified while the vehicle is in motion. In a similar vein, intrusions that take place in high-risk settings, like crowded urban locales or adverse weather conditions, may necessitate more immediate and comprehensive responses [18]. Upon detecting an intrusion, it is essential for the IRS to assess the potential costs and impacts associated with the various response strategies available. This assessment guarantees that the chosen response effectively addresses the threat while also reducing any adverse effects on the vehicle and its passengers. The duration needed to execute a response is a vital consideration, especially in situations where the vehicle is in transit. Quick reactions are crucial for addressing severe threats, yet they can entail compromises regarding precision or resource usage [19]. The IRS is tasked with finding a balance between the urgency of action and the possible effects on vehicle operations. Various responses might necessitate distinct degrees of computational, memory, or energy resources. In environments with limited resources, like those encountered in intelligent vehicles, it is crucial for the IRS to guarantee that the chosen response does not significantly drain these resources, as this could affect the vehicle's overall performance.

Certain responses might require adjustments to vehicle operations, which could involve disabling specific functions or activating a safe mode. The IRS needs to assess the possible disruptions resulting from these responses, taking into account elements like passenger safety, vehicle performance, and the capacity to maintain driving capabilities. Certain responses may have enduring consequences for the vehicle’s systems, including software rollbacks, system resets, or hardware isolation. Although these measures might be essential for countering the intrusion, they can also lead to vulnerabilities, diminish system performance, or necessitate further maintenance. The IRS needs to carefully consider these long-term costs in relation to the immediate benefits of the response. In certain instances, the reaction to an intrusion might be shaped by legal and regulatory obligations [20]. For example, some jurisdictions may require particular actions in the case of a cybersecurity breach, including reporting the incident to authorities or informing those affected. The IRS is required to ensure that its responses adhere to these stipulations while effectively tackling the pressing threat at hand. The ongoing assessment of expenses and effects is an essential element of a successful IRS for smart vehicles. By meticulously evaluating both intrusion-related and response-related factors, the IRS can arrive at well-informed decisions that safeguard the vehicle’s systems, guarantee passenger safety, and uphold operational integrity. This strategy enables the IRS to respond to the changing threat environment, ensuring a versatile and robust defense against cyber intrusions.

IV. Optimal Selection Algorithms

Choosing the most effective response strategy is essential for an autonomous intrusion response system (IRS) in intelligent vehicles. The process of making a decision entails assessing various factors associated with the intrusion and the possible responses, followed by selecting the strategy that provides the optimal balance between addressing the threat and preserving vehicle functionality. A variety of algorithms can be utilized to reach this objective, each possessing distinct advantages and drawbacks. To enhance the selection process, the IRS can utilize a range of algorithms, each specifically designed to tackle distinct elements of the decision-making process [21].

A. *Simple Additive Weighting (SAW)*

Simple Additive Weighting (SAW) is a multi-criterion decision-making (MCDM) method that is both intuitive and effective for selecting optimal responses in an IRS. SAW works by assigning weights to different criteria, which could include factors like response time, resource consumption, disruption level, and intrusion severity. Each potential response is then scored based on these criteria, with the final decision being the response that achieves the highest weighted sum [22].

B. *Linear Programming (LP)*

Linear Programming (LP) is a mathematical optimization technique that is particularly useful when the decision-making process involves constraints. In the context of an IRS, LP can be used to find the optimal response strategy that minimizes or maximizes a particular objective function, such as minimizing response time or maximizing system security, while adhering to constraints like limited resources or safety requirements [23].

C. *Game-Theoretic Algorithm*

Game-theoretic algorithms are based on the principles of game theory, which studies the strategic interactions between decision-makers. In the context of an IRS, these algorithms can model the interaction between the vehicle (as the defender) and potential attackers. By anticipating the possible moves of the attacker, the IRS can choose a response strategy that minimizes the potential damage while maximizing the vehicle's security posture [24].

D. *AI-Based Mechanisms*

AI-based mechanisms** involve the use of machine learning (ML) and artificial intelligence (AI) to dynamically select optimal response strategies. These mechanisms can learn from historical data and adapt to new threats in real-time. Techniques such as reinforcement learning, neural networks, and decision trees can be used to continuously improve the IRS's decision-making capabilities [25].

E. *Adoption of SAW and LP*

The autonomous intrusion response system (IRS) in intelligent vehicles can benefit greatly from a hybrid method that combines Simple Additive Weighting (SAW) and Linear Programming (LP). The initial decision-making is facilitated by the simplicity and flexibility of SAW, while the response plan is refined and finalized by the optimization power of LP.

The integration of SAW and LP can be achieved through a two-step process:

In the first step, the IRS uses the SAW method to quickly evaluate and score potential response strategies based on predefined criteria such as response time, disruption level, and resource consumption. This step allows the IRS to narrow down the list of possible responses to those that are most promising given the current intrusion scenario. Once a subset of high-scoring responses has been identified, the IRS applies Linear Programming to optimize the final selection. The LP model can be designed to minimize an objective function, such as the overall cost or time required for the response, while considering the constraints of the vehicle's operational environment (e.g., available computational resources, safety requirements). This step ensures that the selected response is not only effective but also optimal in terms of resource usage and impact on vehicle operations. By adopting a hybrid approach that combines SAW and LP, an autonomous IRS can achieve a balance between rapid decision-making and optimized response selection. This method enhances the overall resilience of intelligent vehicles against cyber intrusions, ensuring that they remain safe, functional, and secure in a dynamic and potentially hostile environment.

V. Proposed Automotive Intrusion Response Systems

An effective Intrusion Response System (IRS) for intelligent vehicles must be carefully designed to handle the unique challenges posed by the automotive environment. This section outlines the proposed architecture and deployment strategy for such a system, focusing on the critical components and how they work together to ensure vehicle security. The deployment of an IRS within an intelligent vehicle requires a well-coordinated integration with the vehicle's existing systems. The IRS should be distributed across various subsystems to provide comprehensive coverage and timely responses to intrusions [26]. Key vehicle components like the powertrain, infotainment system, communication networks, and autonomous driving modules should have sensors and reaction mechanisms to create a distributed IRS. That way, the IRS can keep an eye out for dangers no matter where they come from and react to them instantly. The IRS should take advantage of edge computing capabilities since intrusion detection and response are latency-sensitive. Reduce dependence on slow or unreliable external networks and maximize response times with IRS data processing and decision-making inside the vehicle [27].

For the purpose of exchanging information amongst its many components, the Internal Revenue Service is required to utilize encrypted communication methods. This involves the use of secure protocols and the encryption of data while it is in transit in order to prevent the data from being intercepted or altered by malicious actors. When it comes to preserving the system's overall security, it is essential to make certain that the integrity and confidentiality of communications are protected. There should be processes in place at the IRS that allow for regular updates and adjustments. In order for the system to be able to update its detection and response algorithms without requiring a significant amount of downtime, it must be able to be updated when new threats surface. The deployment of new threat signatures, response methods, and software fixes can all be accomplished through the use of over-the-air (OTA) updates. The Internal Revenue Service (IRS) is made up of a number of essential components that collaborate with one another to identify intrusions, assess replies, and put into action the most effective strategy. The incursion Detection Module (IDM) is accountable for continuously monitoring the systems of the vehicle for indications of an incursion. The identification of potential dangers is accomplished by the utilization of a combination of signature-based detection, anomaly detection, and behavioral analysis. The Intrusion Detection System (IDM) is designed to function with low latency, which guarantees that its detection of intrusions occurs as rapidly as possible. Once an intrusion has been discovered, it is the responsibility of the DE, which is the main component of the IRS, to choose the proper response approach [28]. It makes use of the algorithms that have been presented, such as SAW and LP, in order to evaluate alternative reactions taken into consideration the severity of the intrusion, the resources that are available, and the operational context of the vehicle at the moment.

VI. Results and Discussions

A thorough evaluation of the planned IRS's efficacy is necessary to guarantee it satisfies the performance and security standards of intelligent cars. Details about the evaluation's execution, testbed configuration, use cases, and outcomes are detailed in this section. Python was the language of choice for developing the planned IRS. To build Linear Programming and its basicx technique, we utilized the widely-used PuLP library and the GNU Linear Programming Kit as solvers. The improved SAW method remains unaffected by this decision since it employs only standard Python mathematical operators. The IRS evaluation testbed employs an embedded system configuration to faithfully replicate the automotive infrastructure. Our solution's precision was ensured by utilizing a Raspberry Pi 4 Model B Rev 1.2, specifically selected for its 1.5 GHz ARM-based quad-core CPU. These are quite comparable in power to the high-performance CPUs commonly used in cars. There are two major aspects of the proposed IRS that will be reviewed here. Before comparing it to modified SAW, LP with maximum benefit, and LP with least cost, we will examine its performance in optimal response selection. We will also look at how each algorithm uses memory and how long it takes to obtain optimal responses.

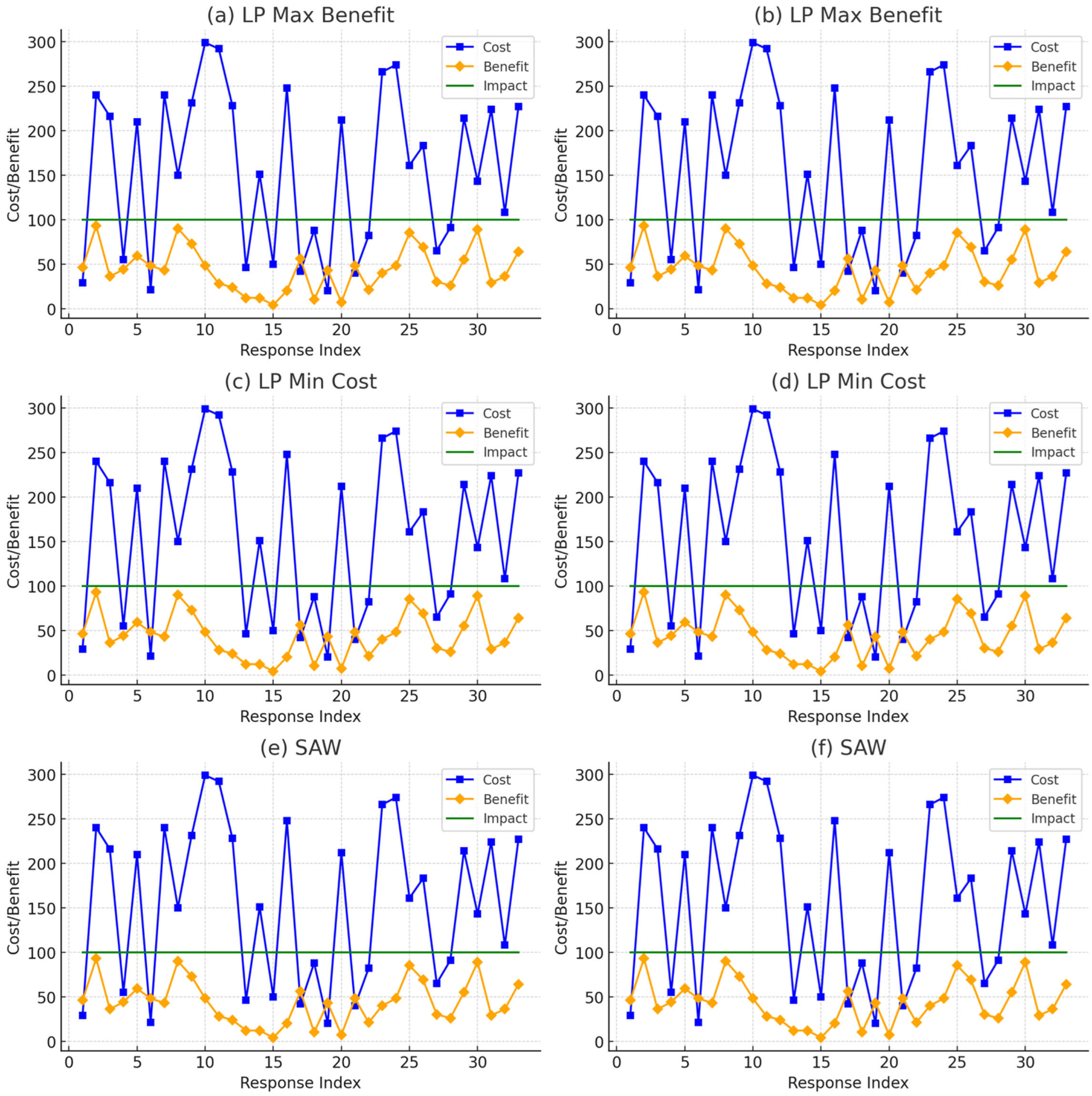

Fig. 3. Cost-benefit outcomes in Scenario.

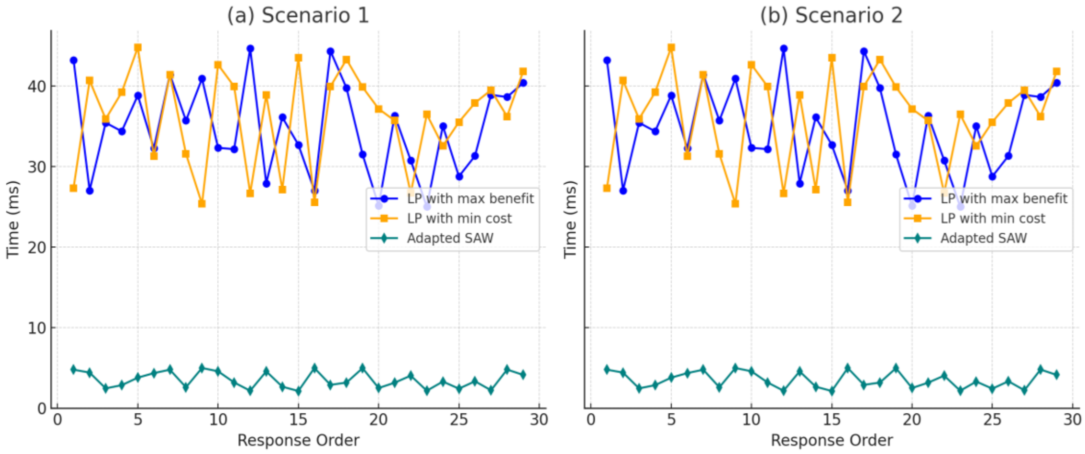

Fig. 4. Time consumption in both cases during answer selection

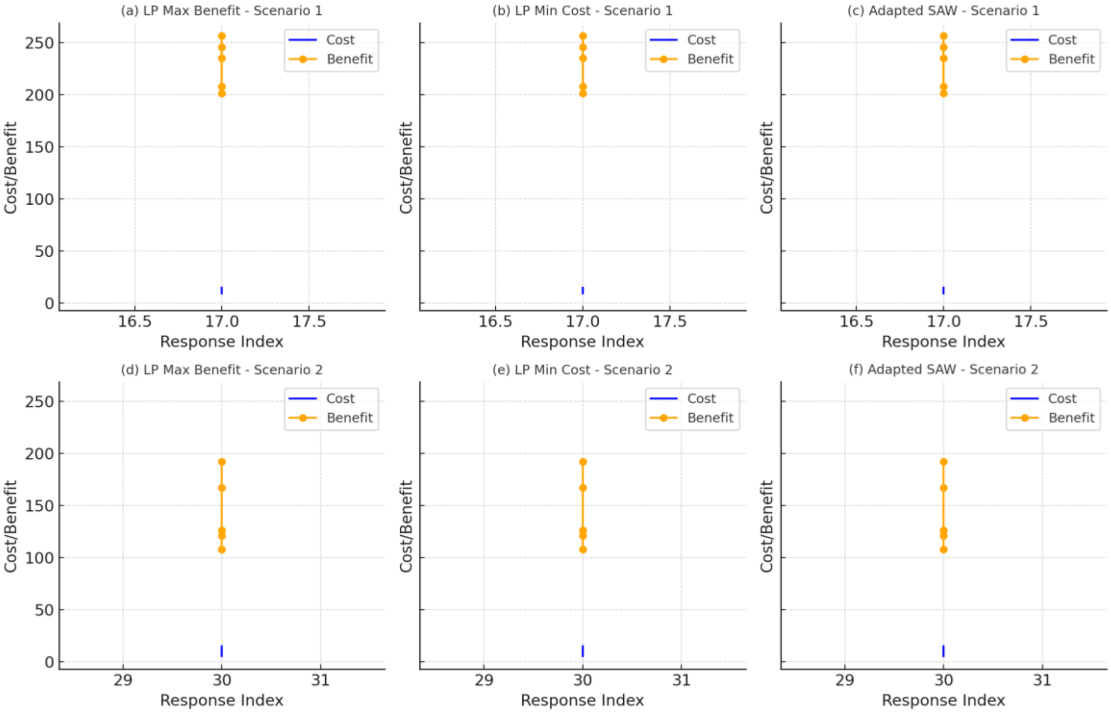

Fig. 5. Parameter adaptation under successful response using three selection methods.

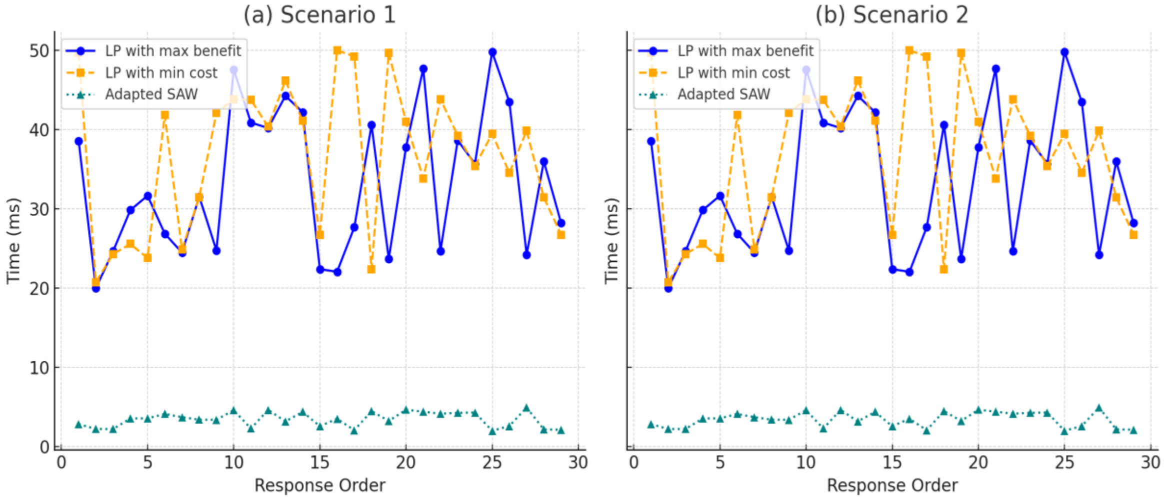

Fig. 6. Parameter adaptation in Scenario using three selection algorithms under consistent response failure.

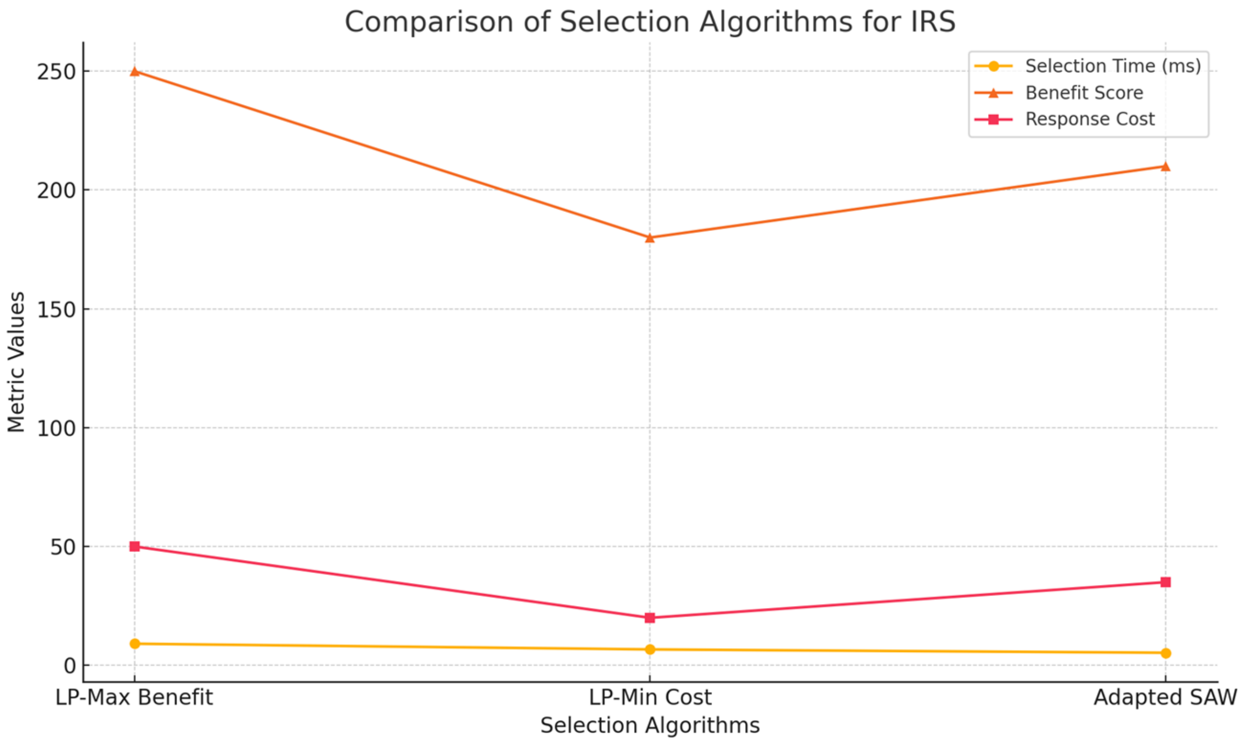

Fig. 7. Comparative performance of IRS selection algorithms based on selection time, benefit score, and response cost

TABLE 1
IMPACT OF THE VELOCITY FOR THE EVALUATED SCENARIOS

	0 km/h	50 km/h	100 km/h
Situation-a	150	160	210
Situation-b	110	120	210

TABLE 2
IMPACT OF VEHICLE VELOCITY ON INTRUSION SEVERITY ACROSS EVALUATED SCENARIOS

Scenario	Velocity	Algorithm	Selected Response	Cost	Benefit	Selection Time (ms)
A	0 km/h	SAW	Response 1	35	210	5.3
A	50 km/h	LP-Min	Response 3	20	180	6.7
B	100 km/h	LP-Max	Response 5	50	250	9.1

TABLE 3
COMPARATIVE ANALYSIS OF SELECTION ALGORITHMS FOR INTRUSION RESPONSE SYSTEM IN INTELLIGENT VEHICLES

Algorithm	Strength	Weakness	Best Use Case
LP-Max Benefit	High effectiveness, optimal security	Higher time and resource cost	Emergency/high-risk scenarios
LP-Min Cost	Resource conservative	Less adaptive, low impact coverage	Embedded low-power systems
Adapted SAW	Fast, balanced, lightweight	May overlook edge-case optimizations	General-purpose scenarios

Here we will provide the outcomes of our IRS testing with two well-known instances. For each of the three selection algorithms—LP with maximum benefit, LP with minimal cost, and the adapted SAW—we will assess the following: response quality, response selection time, memory consumption, and the adaptation of response parameters. The IRS demonstrated a high level of response quality across all use cases. It was able to effectively mitigate threats without causing significant disruption to vehicle operations.

The use of SAW and LP in the decision-making process ensured that the selected responses were both effective and efficient. Finding out how various optimal selection algorithms rank responses and how useful they are in the grand scheme of things is what the response quality evaluation is all about. That can be accomplished by setting the precondition of every response to "rejected" for every response that is proposed. This will keep the IRS from running out of options when it comes to suggesting answers. Because every action has potential good and bad consequences on the system, we show you the benefit and cost of each option. To maintain consistency in the algorithm evaluation across different measures, default parameters are used for each new test in this evaluation.

The cost and benefit of each proposed response, in the sequence in which the respective algorithms apply them, are shown in Figure 3 for both cases. Figure 3 indicates that for the same scenario, our suggested IRS proposes a different number of responses in a different order depending on the scenario and the selection algorithm used. Some answers were chosen twice, as you can see in the figure. As an example, the option to restart the system that was acting up was chosen twice. Nevertheless, it must be emphasized that the answer was chosen for various systems. To rephrase, the first restart pertains to the camera, whilst the second is associated with the acceleration control. Figure 3 shows that the LP approach that starts at very high benefits is the most beneficial, which is expected. The LP that prioritizes minimizing response costs also begins with a very low cost and saves the selection of more expensive solutions for later stages. It is worth mentioning that the LP that maximizes benefit does not care about cost. Nevertheless, it guarantees that the response cost will never exceed the impact of the breach.

The time required to select an answer by each of the three selection methods is displayed in Figure 4. The figure clearly shows that the LP approaches are slower than the tailored SAW method. Because of the need for iterations and the possibility that its offensive responses will fail to meet necessary preconditions, the optimal LP technique typically takes more time. The fastest, least expensive LP method uses a little less time, but it is less careful when choosing its conservative solutions. Every algorithm works fine on an embedded system with limited resources.

Each scenario was run twice, with five iterations of the outer loop each, to evaluate the effect of parameter changes. We found that the responses were consistently successful in one set of five iterations for each situation, but unsuccessful in the other set. On the premise that the solutions were always effective, Figure 5 displays the pros and cons of the five best answers for each scenario, as assessed by the three selection algorithms. Concurrently, Figure 6 displays the outcomes assuming that the responses were continuously unsuccessful.

Figure 7 illustrates a comparative performance analysis of the three selection algorithms—LP-Max Benefit, LP-Min Cost, and Adapted SAW—used within the proposed Intrusion Response System (IRS). The graph compares three critical metrics: selection time, benefit score, and response cost. The Adapted SAW algorithm demonstrates the lowest selection time (\~5.3 ms), indicating its efficiency for real-time decision-making. LP-Min Cost performs moderately in terms of time (\~6.7 ms) and excels in minimizing resource consumption, recording the lowest response cost (20). In contrast, LP-Max Benefit achieves the highest benefit score (250), showcasing its strength in maximizing intrusion mitigation effectiveness, although it requires the most time (~9.1 ms) and incurs the highest operational cost (50). This figure clearly highlights the trade-offs between speed, efficiency, and effectiveness, supporting context-aware algorithm selection in intelligent vehicular environments.

Since this assessment of dynamic parameter adaptation demonstrates that the optimized SAW methods and LP function effectively with modified parameters, the findings are applicable to both test situations. The LP method with minimal cost optimization, however, is inadequate for dealing with variations in response benefit values brought about by parameter alterations. Consequently, it appears that this technique is less interesting for discovering optimal answers in autonomous IRS. All evaluation indicators showed that the IRS performed well. Intelligent vehicle cybersecurity can be improved with the help of this system because of its responsiveness to various attacks.

Although all algorithms choose the same reaction in all circumstances, regardless of velocity, the incursion impact calculation in Table 1 works as expected. The two situations that were evaluated had significant impact values, which is why this behavior occurred. Where the HEAVENS parameters produce smaller values, like in less violent intrusions or the early stages of a stepping-stone attack, the relative importance of velocity becomes more apparent, leading to different results. Importantly, the suggested IRS design is flexible, allowing users to alter the weights of the HEAVENS parameters as needed. This modification lessens the prominence of fixed HEAVENS parameters, making way for velocity to exert a stronger influence on the selected response.

Table 2 presents the effect of varying vehicle velocities (0 km/h, 50 km/h, and 100 km/h) on the severity of intrusions observed in two distinct scenarios (Situation-a and Situation-b). The results reveal a clear trend: as vehicle velocity increases, the impact values rise accordingly, indicating that intrusions become more severe or consequential at higher speeds. For instance, in Situation-a, the impact increases from 150 at rest to 210 at 100 km/h. A similar pattern is seen in Situation-b, where the impact jumps from 110 at 0 km/h to 210 at 100 km/h. These findings underscore the critical importance of dynamic intrusion response strategies that adapt not only to the nature of the threat but also to the real-time operational state of the vehicle. It also highlights the need for an Intrusion Response System (IRS) that can prioritize and select mitigation actions based on contextual parameters like speed, which significantly influence the overall threat impact.

Table 3 presents a comparative analysis of the three selection algorithms—LP-Max Benefit, LP-Min Cost, and Adapted SAW—used in the proposed Intrusion Response System (IRS) for intelligent vehicles. Each algorithm is evaluated based on its key strengths, limitations, and the most suitable deployment scenarios. The LP-Max Benefit algorithm demonstrates high effectiveness in selecting responses with the maximum possible security benefit, making it ideal for high-risk or emergency scenarios. However, this advantage comes at the cost of increased response time and resource consumption. On the other hand, LP-Min Cost prioritizes minimal resource usage, making it highly efficient in low-power embedded environments, but it lacks flexibility and adaptability in high-impact situations. The Adapted SAW method offers a balanced solution by providing fast response selection with reasonable benefit and cost values, making it well-suited for general-purpose automotive applications. This comparative analysis helps in selecting the appropriate algorithm based on the vehicle's operational context and threat environment.

VII. Conclusion and Outlook

The urgent requirement for strong cyber-security protocols in the automobile sector is met by the suggested Intrusion Response System (IRS) for intelligent vehicles. The IRS offers a versatile and efficient method of reducing cyber risks by integrating sophisticated algorithms with a distributed, edge-based design, such as Simple Additive Weighting (SAW) and Linear Programming (LP). The findings of the evaluation prove that the system can identify intrusions, choose the best response, and keep the vehicle secure and functional. Looking ahead, more research is needed to make the IRS more adaptable to new threats, especially with more autonomous and connected vehicles on the road. Possible directions for future research include creating industry standards for automobile cybersecurity and incorporating more complex AI-based methods. There needs to be more research into the IRS's performance in real-world deployments and its capacity to handle large-scale attacks. An encouraging step toward protecting smart cars from the increasing danger of cyber breaches, the proposed IRS is a major step forward in automotive cybersecurity.

References

[1] Zhao, J., Zhao, W., Deng, B., Wang, Z., Zhang, F., Zheng, W., Cao, W., Nan, J., Lian, Y., & Burke, A. F. (2024). Autonomous driving system: A comprehensive survey. Expert Systems with Applications, 242, 122836. https://doi.org/10.1016/j.eswa.2023.122836

[2] El-Rewini, Z., Sadatsharan, K., Selvaraj, D. F., Plathottam, S. J., & Ranganathan, P. (2020). Cybersecurity challenges in vehicular communications. Vehicular Communications, 23, 100214. https://doi.org/10.1016/j.vehcom.2019.100214

[3] Khraisat, A., Gondal, I., Vamplew, P., & Kamruzzaman, J. (2019). Survey of intrusion detection systems: Techniques, datasets and challenges. Cybersecurity, 2(1), 1-22. https://doi.org/10.1186/s42400-019-0038-7

[4] Khan, F. I., Amyotte, P. R., & Amin, M. T. (2019). Advanced methods of risk assessment and management: An overview. Methods in Chemical Process Safety, 4, 1-34. https://doi.org/10.1016/bs.mcps.2020.03.002

[5] Kopalle, P. K., Pauwels, K., Akella, L. Y., & Gangwar, M. (2023). Dynamic pricing: Definition, implications for managers, and future research directions. Journal of Retailing, 99(4), 580-593. https://doi.org/10.1016/j.jretai.2023.11.003

[6] samados, A., Aggarwal, N., Cowls, J. et al. The ethics of algorithms: key problems and solutions. AI & Soc 37, 215–230 (2022). https://doi.org/10.1007/s00146-021-01154-8

[7] Kim, K., Kim, J. S., Jeong, S., Park, J., & Kim, H. K. (2021). Cybersecurity for autonomous vehicles: Review of attacks and defense. Computers & Security, 103, 102150. https://doi.org/10.1016/j.cose.2020.102150

[8] Khraisat, A., Gondal, I., Vamplew, P., & Kamruzzaman, J. (2019). Survey of intrusion detection systems: Techniques, datasets and challenges. Cybersecurity, 2(1), 1-22. https://doi.org/10.1186/s42400-019-0038-7

[9] Chunduru, Anilkumar & Robbi, Jyothsna & Sattaru, Vandana & Gothai, E.. (2023). Deep Learning-Based Yoga Posture Specification Using OpenCV and Media Pipe. Applied and Computational Engineering. 8. 80-86. 10.54254/2755-2721/8/20230085.

[10] Qian, Y., Joshi, J., Tipper, D., & Krishnamurthy, P. (2007). Information Assurance. Information Assurance, 1-15. https://doi.org/10.1016/B978-012373566-9.50003-3

[11] Baddu Naik Bhukya, V. Venkataiah, S. Mani.Kuchibhatla, S. Koteswari, R V S Lakshmi Kumari, and Yallapragada Ravi Raju, "Integrating the Internet of Things to Protect Electric Vehicle Control Systems from Cyber Attacks," IAENG International Journal of Applied Mathematics, vol. 54, no. 3, pp433-440, 2024

[12] Shinde, N., & Kulkarni, P. (2020). Cyber incident response and planning: A flexible approach. Computer Fraud & Security, 2021(1), 14-19. https://doi.org/10.1016/S1361-3723(21)00009-9

[13] Zhao, J., Zhao, W., Deng, B., Wang, Z., Zhang, F., Zheng, W., Cao, W., Nan, J., Lian, Y., & Burke, A. F. (2024). Autonomous driving system: A comprehensive survey. Expert Systems with Applications, 242, 122836. https://doi.org/10.1016/j.eswa.2023.122836

[14] Blessing, Elisha. (2023). Exploring innovative approaches and solutions that have been effective in overcoming integration challenges.

[15] Aleedy, Moneerh & Shaiba, Hadil & Bezbradica, Marija. (2019). Generating and Analyzing Chatbot Responses using Natural Language Processing. International Journal of Advanced Computer Science and Applications. 10. 10.14569/IJACSA.2019.0100910.

[16] Micale, D., Matteucci, I., Fenzl, F. et al. A context-aware on-board intrusion detection system for smart vehicles. Int. J. Inf. Secur. 23, 2203–2223 (2024). https://doi.org/10.1007/s10207-024-00821-3

[17] Bhukya, B. N., Rekha, V. S. D., Paruchuri, V. K., Kavuru, A. K., & Sudhakar, K. (2023). Internet of Things for Effort Estimation and Controlling the State of an Electric Vehicle in a Cyber Attack Environment. Journal of Theoretical and Applied Information Technology, 101(10).

[18] Wang, Shaoqiang & Wang, Yizhe & Zheng, Baosen & Cheng, Jiahui & Su, Yu & Dai, Yinfei. (2024). Intrusion Detection System for Vehicular Networks Based on MobileNetV3. IEEE Access. PP. 1-1. 10.1109/ACCESS.2024.3437416.

[19] Inayat, Z., Gani, A., Anuar, N. B., Khan, M. K., & Anwar, S. (2016). Intrusion response systems: Foundations, design, and challenges. Journal of Network and Computer Applications, 62, 53-74. https://doi.org/10.1016/j.jnca.2015.12.006

[20] Adnan Yusuf, S., Khan, A., & Souissi, R. (2023). Vehicle-to-everything (V2X) in the autonomous vehicles domain – A technical review of communication, sensor, and AI technologies for road user safety. Transportation Research Interdisciplinary Perspectives, 23, 100980. https://doi.org/10.1016/j.trip.2023.100980

[21] Ghraizi, D., Talj, R., & Francis, C. (2022). An Overview of Decision-Making in Autonomous Vehicles. IFAC-PapersOnLine, 56(2), 10971-10983. https://doi.org/10.1016/j.ifacol.2023.10.793

[22] Taherdoost, Hamed. (2023). Analysis of Simple Additive Weighting Method (SAW) as a MultiAttribute Decision-Making Technique: A Step-by-Step Guide. Journal of Management Science & Engineering Research. 6. 10.30564/jmser. v6i1.5400.

[23] Kunwar, Rajendra & Sapkota, Hari. (2022). An Introduction to Linear Programming Problems with Some Real-Life Applications. European Journal of Mathematics and Statistics. 3. 21-27. 10.24018/ejmath.2022.3.2.108.

[24] Hanley, John. (2021). GAMES, game theory and artificial intelligence. Journal of Defense Analytics and Logistics. ahead-of-print. 10.1108/JDAL-10-2021-0011.

[25] Sarker, I.H. AI-Based Modeling: Techniques, Applications and Research Issues Towards Automation, Intelligent and Smart Systems. SN COMPUT. SCI. 3, 158 (2022). https://doi.org/10.1007/s42979-022-01043-x

[26] Naik, B., Bhukya, Sarvani, V., Rekha, D., Paruchuri, V.K., Kavuru, A.K., & Sudhakar, K. "Internet of Things for Effort Estimation and Controlling the State of an Electric Vehicle in A Cyber Attack Environment", Journal of Theoretical and Applied Information Technology, 2023, 101(10), pp. 4033–4040.

[27] Abdallaoui, S., Ikaouassen, H., Kribèche, A., Chaibet, A., & Aglzim, H. (2023). Advancing autonomous vehicle control systems: An in-depth overview of decision-making and manoeuvre execution state of the art. The Journal of Engineering, 2023(11), e12333. https://doi.org/10.1049/tje2.12333

[28] Nagarajan, J., Mansourian, P., Shahid, M.A. et al. Machine Learning based intrusion detection systems for connected autonomous vehicles: A survey. Peer-to-Peer Netw. Appl. 16, 2153–2185 (2023). https://doi.org/10.1007/s12083-023-01508-7