Journal of Theoretical and Applied Information Technology
31st August 2025. Vol.103. No.16

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

# AI-POWERED INTRUSION RESPONSE FOR INTELLIGENT VEHICULAR ECOSYSTEMS

**L. K. SURESH KUMAR[1], RAVI UYYALA[2], JAIDEEP GERA[3], A L SREENIVASULU[4], P. SASIREKHA[5], KUNCHANAPALLI RAMA KRISHNA[6]**

[1]Department of Computer Science & Engineering, University College of Engineering, Osmania University Hyderabad, Telangana, India
[2]Department of Computer Science and Engineering, Chaitanya Bharathi Institute of Technology, Gandipet, Hyderabad, Telangana, India
[3]Department of Computer Science and Business Systems, RVR & JC College of Engineering, Guntur, Andhra Pradesh, India
[4]Department of Computer Science and Engineering, Vignana Bharathi Institute of Technology, Ghatkesar, Medchal, Hyderabad, Telangana
[5]Department of Electrical and Electronics Engineering, M. Kumarasamy College of Engineering, Karur, Tamilnadu, India
[6]Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur, Andhra Pradesh, India
E-mail: suresh.l@uceou.edu, uyyala.ravi@gmail.com, gera.jaideep@gmail.com, akula.srinivasulu@vbithyd.ac.in, sasirekhap.eee@mkce.ac.in, tenalirama@kluniversity.in

**ABSTRACT**

Implementing strict cybersecurity measures to protect against cyber-attacks is absolutely necessary, given the increasing number of intelligent vehicles on the road. This study aims to learn more about the potential for creating an intelligent vehicle-specific autonomous intrusion response system (IRS). The proposed IRS system can instantly assess the consequences of intrusions and ascertain the best methods of response depending on the situation. Among the most significant contributions are a thorough analysis of different response techniques, a system for evaluating costs and impacts dynamically, and the application of various selection algorithms including Simple Additive Weighting (SAW), Linear Programming (LP), game theory, and AI-based procedures. Research has shown that the system works well in terms of response quality, efficiency of time, and consumption of resources. This proves that the technology has the ability to greatly enhance car safety. The findings of this study lay the groundwork for future framework improvements and adaptations by the Internal Revenue Service.

**Keywords:** *Intrusion response system, Cybersecurity, Intelligent vehicles, Linear Programming, Game theory, AI-based mechanisms*

## 1. INTRODUCTION

The emergence of intelligent vehicles can be attributed to the exponential rise of technology. To enhance the user experience, safety, and efficiency, these cars employ intricate software, sensors, and communication systems. Transportation cars of the future typically have cutting-edge technology including autonomous driving capabilities, advanced driver assistance systems (ADAS), and seamless communication. Notwithstanding this, AI cars are prime targets for malevolent attacks due to their expanding complexity and interconnection, which leaves them open to a broad range of cybersecurity vulnerabilities [1]. Unauthorized access to car systems or complete control of vehicle functions are two examples of the catastrophic consequences that might result from cyber invasions in intelligent vehicles. These consequences can show up in many forms. Passenger safety, road jams, and criminal targeting are all possibilities that might result from such incursions. The seriousness of these attacks makes the need for real-time detection, evaluation, and reaction to intrusions all the more pressing [2]. Due to the ever-changing and real-time nature of intelligent automobiles' operational environment, standard security solutions such as firewalls and intrusion detection systems (IDS) are insufficient.

An autonomous intrusion response system (IRS) is necessary if attacks can be detected and appropriate countermeasures can be determined and executed on its own to mitigate the risks posed by such attacks. A good intelligent vehicle intrusion detection system (IRS) should be able to determine the type and level of intrusion, consider how it might affect the vehicle's performance and safety, and then select the best response method from among several possibilities [3]. The potential security risks linked with smart automobiles are starting to be noticed by more and more people. For this reason, cyber-responsibility is a critical component of a safe vehicle. But you need to answer three important questions before you can have that potential. Review Figure 1 and Question 1: If this were to happen, what would be the best way to handle the situation? What considerations are extremely critical when assessing these replies? Regarding your third question, how can we use the program's current state to choose one or more of these responses. In order to find solutions to the problems that have been brought up, this article will look at the different cyber assaults and classify possible replies based on their effects. The study also includes a dynamic risk assessment that takes into account variables like attack details and vehicle condition, and a cost-benefit analysis of attacks and replies. With the help of this evaluation, you can choose the correct answers. Furthermore, the research finds the most effective methods for response selection when applied to vehicle systems after investigating and analyzing several ways [4]. The goal of this piece is to look at clever car-specific IRS design and implementation possibilities. By utilizing a variety of algorithms, including Simple Additive Weighting (SAW), Linear Programming (LP), game-theoretic techniques, and AI-based procedures, the Internal Revenue Service (IRS) is able to assess the effects of various response techniques in real time, thanks to its foundation in dynamic cost and impact evaluation [5]. These algorithms were chosen for their ability to handle the unique challenges of the automobile setting. Some of these difficulties include having little resources, having to make quick judgments, and needing a high level of reliability. Our goal in conducting this research is to help build smarter, more resilient intelligent vehicle systems by laying the groundwork for autonomous intrusion response. This research aims to pave the path for improved vehicle security systems in the future, ones that can safeguard the complex and interdependent networks that characterize contemporary transportation [6]. To achieve this goal, we will address the unique challenges faced by the automobile industry. Looking at the system architecture of modern cars is the first step in comprehending how IRS is integrated into these vehicles and the possible reactions it offers. Figure 2 shows a general, realistic, and comprehensive reference design. This design is commonly found in contemporary automobiles. Subsystems that are highly integrated make up a modern vehicle. According to the schematic, contemporary vehicles have a plethora of embedded devices, or ECUs. Different forms of networks, like CAN, Flexray, and Ethernet, allow these ECUs, which are dispersed throughout the vehicle, to talk to each other. Various domains or zones are used to categorize electronic control units (ECUs) according to the functions they carry out. Powertrains, infotainment, and advanced driving assistance systems (ADAS) are all part of these spheres and areas. In addition to ECUs, today's vehicles come with a plethora of sensors, including as cameras and LiDAR, as well as diagnostic ports, such as OBD-II, and sophisticated communication technologies for connecting to the outside world. When put together, these elements form a sizable attack surface that many other types of threats and attacks can take advantage of.

## 2. EFFECTIVE APPROACHES FOR ADDRESSING SCENARIOS

The security of sensitive data, the integrity of the vehicle systems, and the safety of passengers are often at stake in the context of intelligent vehicles, making a rapid and effective response to a cyber-intrusion absolutely necessary. Accordingly, an autonomous intrusion response system (IRS) needs a variety of reaction tactics that can be chosen dynamically according to the type and degree of the incursion, the vehicle's operational status, and the possible effect on its functionality. The timing of the response should be the primary concern when establishing response tactics [7]. Quick actions are taken upon detection of an incursion in order to eliminate the danger before it can do substantial harm. Isolating infected systems, blocking harmful data packets, and forcing essential car parts into a safe mode are all examples. In cases where the incursion presents an urgent danger to safety or the operation of the vehicle, several responses are usually used. The opposite is true with delayed responses, which entail keeping an eye on the intrusion for a while before determining what to do.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

When additional information is required to comprehend the entire extent of the threat or when the intrusion is not immediately detrimental, this method is helpful. As a result of delays in responding, it may be necessary to collect more forensic evidence, notify the driver or a remote security team, or get the car ready for a more extensive countermeasure [8]. Another way to classify response tactics is as active or passive. The term "passive response" refers to a set of behaviors that are not disruptive to the vehicle's normal functioning. Some of these measures may involve recording the intrusion for review at a later time, revising security protocols, or modifying the parameters used to detect threats in the vehicle [9]. When the level of risk is modest or if an aggressive response would create needless disruption, passive responses are usually employed. In contrast, active reactions entail addressing the incursion by directly interacting with the vehicle's systems. To accomplish this, it may be necessary to disable specific car features, redirect data flows, or implement more involved countermeasures such as system reboots or software rollbacks. When the invasion seriously compromises the vehicle's security or operation, active measures must be taken [10]. Taking measures ahead of time to forestall or lessen the severity of intrusions is what we mean when we talk about proactive methods. Among these methods are the following: applying adaptive security mechanisms that change in reaction to new threats; regularly updating security software; and continuously monitoring system vulnerabilities. In order to keep intelligent vehicles, secure, proactive measures are necessary to lessen the chances of successful incursions [11].

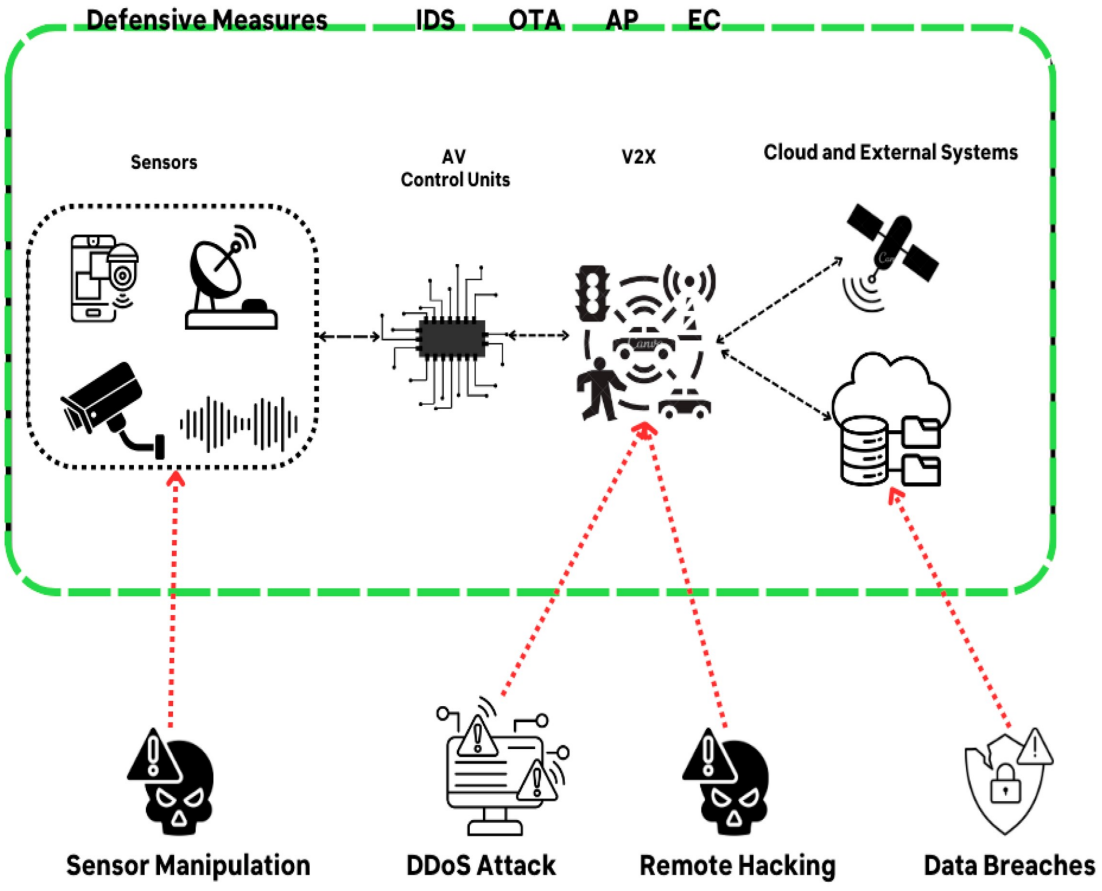


*Figure 1: Cybersecurity threats within the autonomous vehicle ecosystem*

Journal of Theoretical and Applied Information Technology
31st August 2025. Vol.103. No.16

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

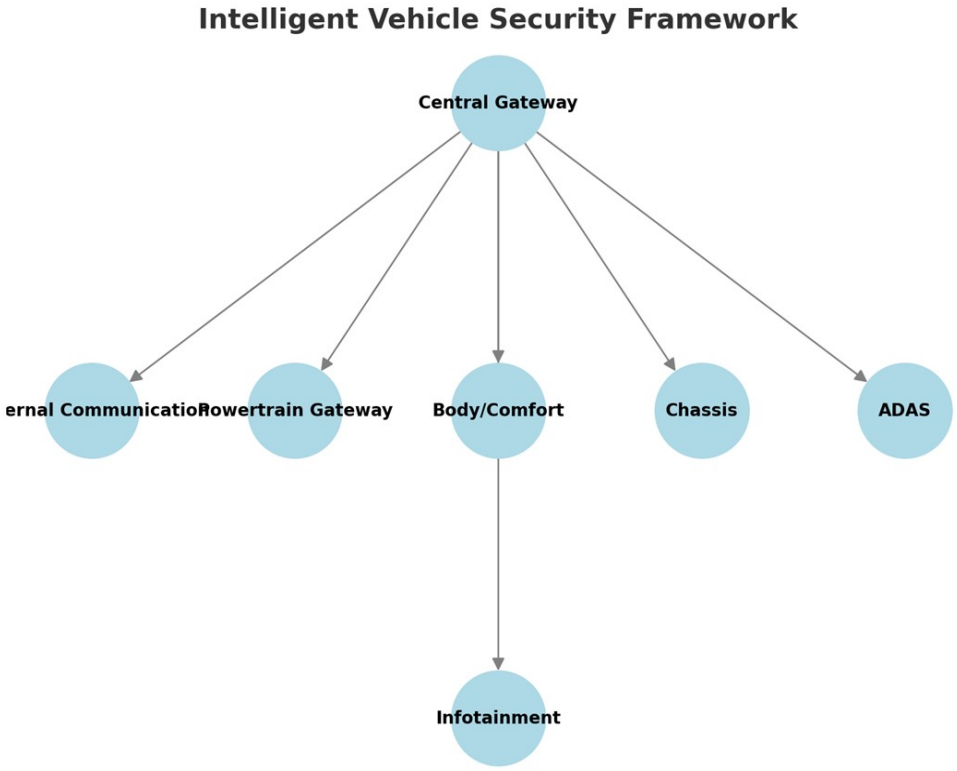


*Figure 2: Reference vehicle design with potential assault surfaces.*

Following the detection of an intrusion, reactive methods are implemented with the goal of minimizing its impact and returning the vehicle to its usual operating state. Because they call for swift action to eliminate dangers, reactive responses usually use more resources than proactive ones. Protecting against all possible cyber-attacks requires an IRS that strikes a good balance between preventative and reactive measures. The breadth of the response is another important factor to think about. Activating a global reset, going into safe mode, or turning off communication interfaces are all examples of system-level responses that impact the entire vehicle [12]. Only very serious incursions that endanger the vehicle's general safety or integrity would normally trigger these reactions. Conversely, responses at the component level zero in on particular compromised systems or components. An IRS could stop a particular software module, cut off contact with a compromised external device, or isolate a broken sensor. More accurate component-level reactions can keep the car running smoothly even as they fix the particular intrusion. While fully autonomous operation is the ideal for intelligent vehicle IRSs, there are several situations that may necessitate human intervention. The IRS's algorithms evaluate each case and determine the optimal course of action; no human intervention is required to carry out automated answers. When the car is in motion and you need to neutralize urgent dangers, for example, these reactions are crucial since you need to make a decision quickly. With a human-in-the-loop response, a person other than the automated system can be notified and take action, such the driver or a remote security team. When weighing security requirements against operational factors becomes a matter of human judgment in complicated or unclear circumstances, this method can be helpful [13]. The IRS should be built such that it can work in tandem with human operators, giving them all the data they need to make smart choices. Lastly, the Internal Revenue Service needs to choose between personalized and generic answers. The operational context of the vehicle and the type of incursion determine the tailored response. To illustrate the point, the IRS may isolate and secure the navigation system of a car in the event of an infiltration, while ensuring that no other functions are compromised. In most cases, tailored replies work better, although they do necessitate more intricate decision-making procedures [14]. In comparison, generic replies are a set of pre-defined steps that can be used for

various types of intrusions. Commonplace measures like entering a safe mode or cutting off access to outside networks could fall into this category. While customized replies offer the highest level of precision, generic responses are easier to develop and can effectively neutralize threats quickly and reliably. An IRS's usefulness in autonomous cars is conditional on its capacity to choose the best course of action in every particular circumstance. Incorporating a varied set of reaction techniques allows the IRS to effectively defend intelligent cars in an increasingly connected environment from cyber-attacks. These strategies can range from rapid and preemptive steps to delayed and reactive responses [15].

## 3. EVALUATION OF COSTS AND IMPACTS THAT ARE DYNAMIC

The ability to dynamically assess the costs and implications of intrusions and actions is crucial for an effective intrusion response system (IRS) in the context of intelligent cars. In order to make educated decisions that strike a balance between the vehicle's operational needs and the necessity for security, this evaluation is vital. To reduce potential damage while keeping vehicle operation, the IRS must optimize its actions by recognizing the numerous aspects that influence the cost and impact of both intrusions and replies. There is a large range in the type, severity, and possible outcomes of intrusions in intelligent cars [16]. The IRS has to take a lot of things into account in order to determine the true extent of an intrusion's effects:

The possible effect on the vehicle is highly dependent on the intensity of the incursion. Critical systems like braking, steering, or communication networks are particularly vulnerable to high-severity breaches, which can quickly jeopardize passenger safety and the vehicle's integrity. Minor data breaches or efforts to access non-critical systems are examples of low-severity intrusions that still require attention, despite their potential lack of immediate consequence. The extent to which an intrusion affects a system depends on the systems that were specifically targeted. One example is the potential disastrous effects of an intrusion on the vehicle's autonomous driving system, as contrasted with the potential inconvenience and lack of immediate risk that could arise from an incursion on the entertainment system. Based on the severity of the damaged systems, the IRS must prioritize their replies [17].

An intrusion in one part of the vehicle's network could potentially extend to other parts of the network or even other vehicles. Before the intrusion may do extensive damage, the IRS must assess the probability of its propagation and act to contain it. Another important consideration is the amount of time it takes to identify an intrusion. It is possible to respond more effectively and stop the intrusion from getting worse if caught early. The intrusion may have already done substantial damage or affected numerous systems by the time detection is delayed, which can make the necessary response more complex and expensive. The impact of an intrusion can be greatly affected by the context in which it occurs. An intruder found when the car is at a standstill, for example, could not be as serious as one found when it's moving. Similarly, more immediate and strong reactions may be necessary in the event of an intrusion in a high-risk setting, such as a crowded urban area or a region experiencing severe weather [18].

After an infiltration has been found, the IRS needs to weigh the pros and cons of each response strategy. This assessment guarantees that the chosen action eliminates the danger while keeping the car and its passengers safe to the greatest extent possible. In situations where the vehicle is moving, the time needed to execute a response becomes much more important. Mitigating high-severity risks requires rapid reactions, but there may be accuracy or resource consumption trade-offs [19]. The Internal Revenue Service has to weigh the importance of speed against the possible effects on vehicle operations. The amount of time, effort, and power needed to process various responses could vary widely. For intelligent vehicles and other environments with limited resources, the IRS must make sure that the chosen reaction won't drain them too much, otherwise the vehicle won't be able to function properly.

Disabling features or switching to a safe mode are two examples of responses that could require a short or long-term adjustment to the way the vehicle operates. Taking into account aspects including passenger safety, vehicle performance, and the capacity to continue driving, the IRS must assess the possible interruption that these responses may produce. Software rollbacks, system resets, and hardware isolation are some of the responses that might affect the vehicle's systems in the long run. These measures may be required to stop the invasion, but they come with the risk of making the system less secure, slower, or more maintenance intensive. The Internal Revenue Service (IRS)

needs to consider both the short-term profits and the costs of this action. Compliance with applicable laws and regulations may play a role in how an organization reacts to an incursion [20]. In the case of a cybersecurity breach, for example, it may be required by law to report the occurrence to the proper authorities or to notify those individuals who have been impacted. The IRS has to handle the immediate threat while also making sure its responses are compliant with these regulations. One essential feature of a good intelligent vehicle IRS is the ability to dynamically assess costs and impacts. The IRS can safeguard the vehicle's systems, guarantee passenger safety, and preserve operational integrity by thoughtfully evaluating intrusion-related and response-related elements. By taking this approach, the IRS can stay ahead of cyber breaches by responding to new threats as they emerge.

## 4. PROPOSED AUTOMOTIVE INTRUSION RESPONSE SYSTEMS (IRS)

The specific threats presented by the automotive setting necessitate meticulous design of an Intrusion Response System (IRS) for smart automobiles. In this part, we will go over the planned design and implementation of such a system, with an emphasis on the main parts and how they interact to keep vehicles safe. It is essential to integrate the IRS with the vehicle's current systems in a coordinated manner before deploying it within an intelligent vehicle. Distributing the IRS among several subsystems allows for more thorough coverage and faster responses to incursions [26]. The IRS is best deployed as a decentralized system, with sensors and reaction mechanisms integrated into autonomous driving modules, communication networks, powertrain, infotainment systems, and communication networks. Because of this, the IRS can keep an eye out for dangers at all times and react to them instantly, no matter where they come from. The IRS should take advantage of edge computing capabilities since intrusion detection and response is 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].

When the IRS has to share data between itself, it must do it over encrypted methods. To avoid interception or manipulation by malicious actors, this involves encrypting data while it is in transit and utilizing secure protocols. To keep the system secure as a whole, it is essential to guarantee the privacy and authenticity of communications. Regular upgrades and adaptations should be a part of the IRS. The ability to update detection and response algorithms without requiring substantial downtime is crucial for the system to keep up with new threats. The latest threat signatures, response plans, and software fixes can be distributed through over-the-air (OTA) updates. The IRS relies on a number of interdependent parts to identify incursions, assess reactions, and put the best plan into action. The IDM's job is to keep an eye on all of the car's systems for any indication of an attack. To find possible dangers, it employs a mix of signature-based detection, behavioral analysis, and anomaly detection. The IDM is engineered to function with minimal delay, guaranteeing the prompt detection of intrusions. The IRS's central node, the DE, is in charge of deciding how to react in the event of an intrusion [28]. Utilizing algorithms like SAW and LP, it assesses possible reactions according to the level of intrusion, the resources at its disposal, and the vehicle's operational situation at the moment.

## 5. RESULTS AND DISCUSSIONS

To make sure the planned IRS is secure and performs well enough for intelligent vehicles, it needs to be tested thoroughly. The assessment method is detailed in this section, which includes the setup of the testbed, use cases, and the details of the implementation. The suggested IRS was implemented using the Python programming language. The basicx approach for linear programming was implemented using the well-established PuLP library and the GNU Linear Programming Kit as solvers. The improved SAW method remains unaffected by this decision since it employs just standard mathematical operators in Python. The IRS evaluation testbed employs an embedded system configuration to faithfully replicate the automotive infrastructure. Using a Raspberry Pi 4 Model B Rev 1.2, which was selected for its 1.5 GHz ARM-based quad-core processor, ensured the precision of our approach. Their processing power is comparable to that of the high-performance processors commonly found in vehicles. This review will focus on two key aspects of the proposed IRS. First, we'll take a look at how well it does optimal response selection. Then, we'll evaluate three distinct selection algorithms—LP with maximum benefit, LP with minimal cost, and

modified SAW—in terms of memory usage and how long it takes to have ideal responses.

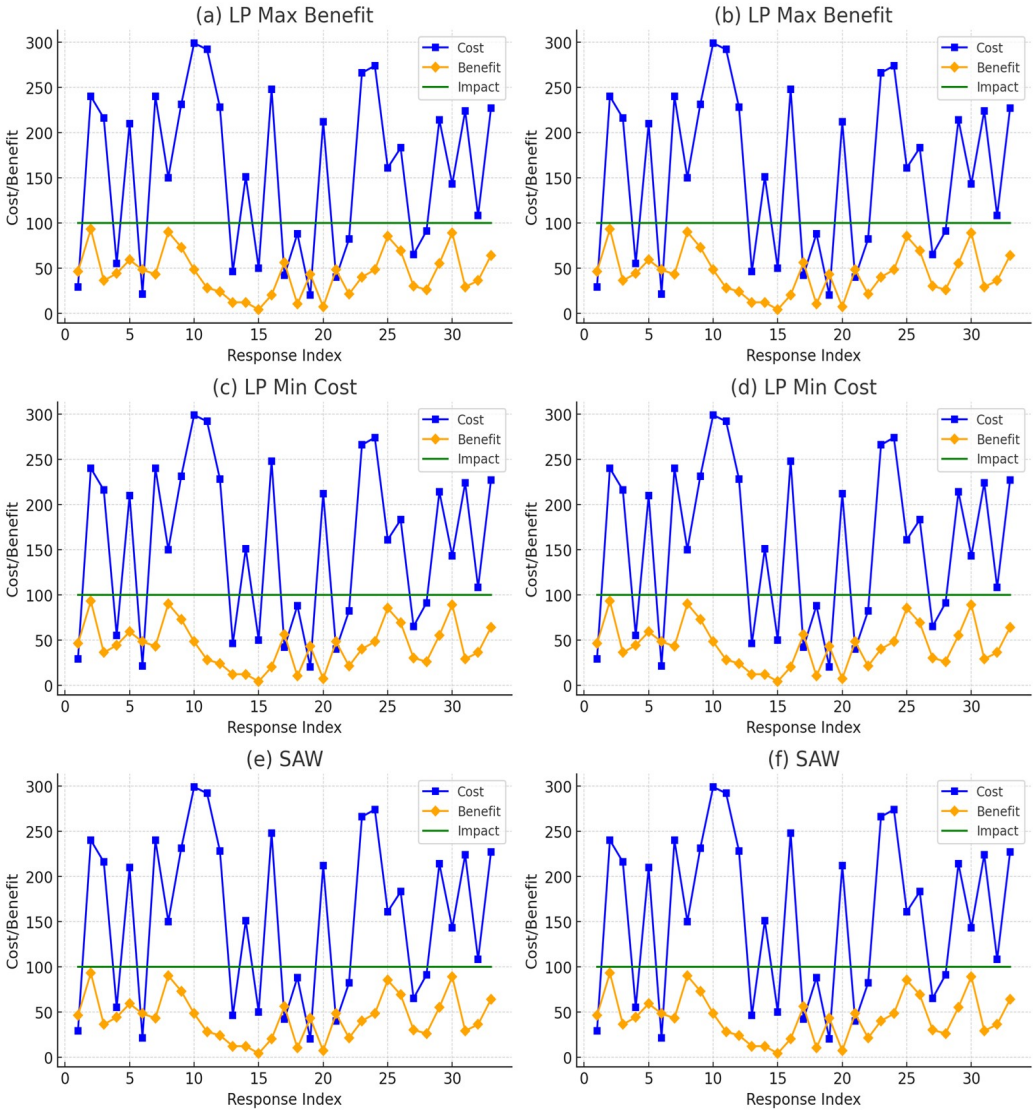


*Figure 3: Cost-benefit analysis of the reaction in Scenario 1 (left) and Scenario 2 (right) utilizing adapted SAW (bottom), LP with minimal cost (middle), and LP with greatest benefit (top).*

Here, using two famous cases, we will provide the results of our IRS testing. We will evaluate the following for each of the three selection algorithms: LP with least cost, the adapted SAW, and LP with maximum benefit: response quality, memory consumption, response selection time, and response parameter modification. Regardless of the use case, the IRS consistently provided high-quality responses. It successfully reduced dangers without substantially impeding vehicle operations. The effectiveness and efficiency of the chosen replies were guaranteed by incorporating SAW and LP into the decision-making process. By evaluating the quality of the responses, we may learn how different optimal selection algorithms rank them and how valuable they are overall. For each suggested response, you can achieve this by making "rejected" the prerequisite of the response. This ensures that the IRS will never run out of potential solutions. Given that any action might have both positive and negative effects on the system, we lay out the pros and drawbacks of each choice for you. Default parameters are utilized for every new test in this evaluation to ensure uniformity across all measurements used to evaluate the algorithm.

Journal of Theoretical and Applied Information Technology
31st August 2025. Vol.103. No.16

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

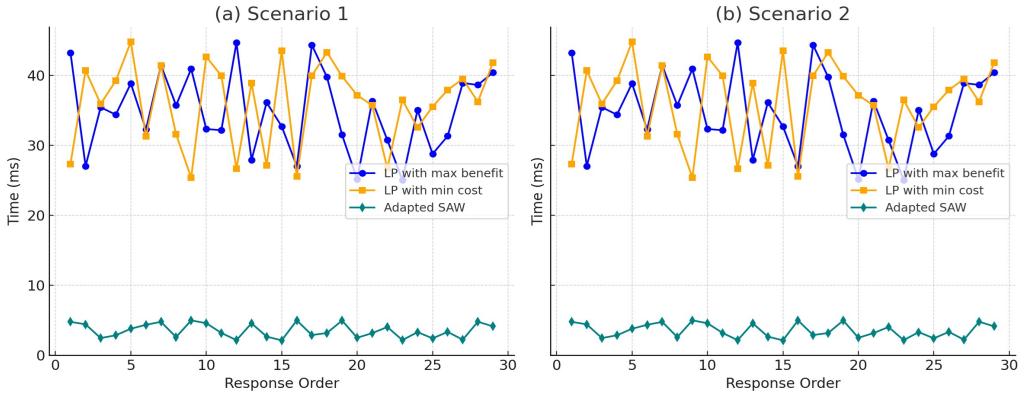


*Figure 4: Time consumption evaluation of the three selection methods for both circumstances during answer selection*

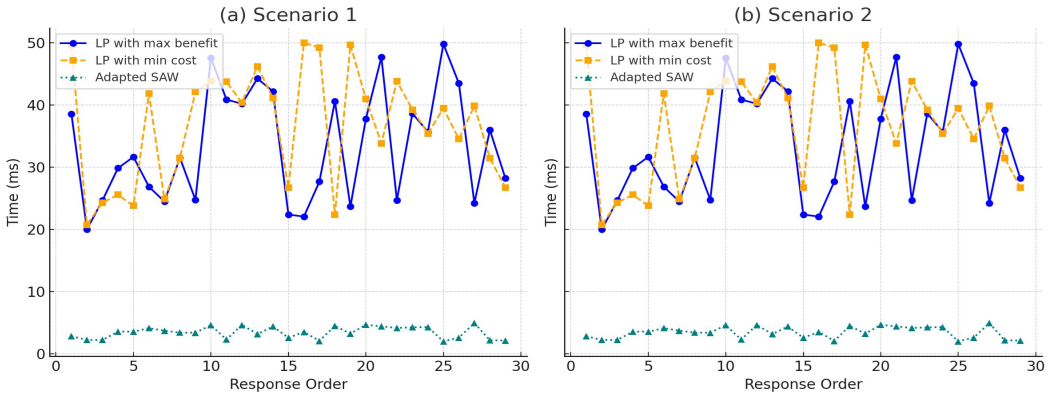


*Figure 5: Assesses parameter adaption in Scenario 1 (top) and Scenario 2 (bottom) for replies picked throughout five rounds using the three selection algorithms if the responses were consistently unsuccessful*

For both scenarios, Figure 3 displays the costs and benefits of each suggested reaction in the order in which the corresponding algorithms apply them. As shown in Figure 3, the number of replies proposed by our proposed IRS varies among scenarios and selection algorithms, even for the same situation. As shown in the figure, a few responses were selected twice. The option to restart the malfunctioning system, for instance, was selected twice. However, it should be noted that several systems were used to determine the answer. In other words, the camera is involved in the first restart and the acceleration control is involved in the second. To no one's surprise, Figure 3 reveals that the most advantageous LP strategy is the one that begins with extremely high advantages. Even the LP that puts a premium on reducing response costs starts off cheap and saves the selection of costlier solutions for later on. Notably, the LP that prioritizes benefit maximization is cost agnostic. But it ensures that the incident response cost will never be more than the breach's impact.

The time required to find a solution by each of the three algorithms is displayed in Figure 4. The response order, not the response index, is shown by the X-axis. The LP methods are slower than the tailored SAW method, as seen in the figure. Because of the need for iterations, the optimal LP method sometimes takes more time, and its offensive replies may fail to meet necessary preconditions. Although it takes somewhat less time, the most cost-effective LP method chooses its conservative answers with fewer precondition checks. All algorithms work well on embedded systems with limited resources.

We ran two sets of data, with five iterations of the outer loop each, to see how different parameters affected the results. For each situation, we ran two sets of iterations; one set of five iterations yielded

consistently successful results, while the other set yielded consistently unsuccessful ones. In Figure 5, we can see the pros and cons of the three selection algorithms' best five answers for each situation, assuming that these answers were always correct. Both test scenarios can be considered genuine, as the results show that the optimized SAW methods and LP perform well with the altered parameters, proving the validity of the parameters. The LP method with minimal cost optimization, however, is inadequate for dealing with variations in response benefit values brought about by parameter alterations. For that reason, it appears that this approach makes discovering optimal answers in autonomous IRS less appealing. In every assessment metric, the IRS performed admirably. Intelligent vehicle cybersecurity can be improved with the help of this system because of its quick and effective response to various attacks.

## 6. CONCLUSION AND OUTLOOK

The suggested Intrusion Response System (IRS) for smart cars is an answer to the urgent demand for strong cybersecurity protocols in the car sector. 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. In order to make the IRS more resilient to new dangers, more study is required in the future, especially in light of the growing autonomy and connection of vehicles. Possible directions for future research include creating industry standards for automobile cybersecurity and incorporating more complex AI-based methods. We also need more research on how well the IRS works in real-world deployments and how well it handles large-scale attacks. Protecting smart cars from the increasing danger of cyber-attacks is a top need, and the proposed IRS is a positive step in the right direction.

## 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] Baddu Naik B, Manam Ravindra, Simhadri Mallikarjuna Rao, Srikanth Kilaru, Madamanchi Brahmaiah, Bezawada Manasa, Muralidhar V "Cyberattack Prevention and Detection in Smart Power Systems Using Deep Learning" Journal of Theoretical and Applied Information Technology, May 2025. Vol.103. No.9, pp. 3934-3944.

[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] 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

[18] Baddu Naik Bhukya, Vutukuri Sarvani Duti Rekha, Venkata Krishnakanth Paruchuri, Ashok Kumar Kavuru and Kadiyala Sudhakar "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, ISSN: 1817-3195, Vol. 101, No.10, pp. 4033 – 4040, May-2023.

[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