A Dual-Step Approach for Implementing Smart AVS in Cars

Bachu Poornima
Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Hyderabad, India | Mahatma Gandhi Institute of Technology, Hyderabad, India
bachupoornima@gmail.com (corresponding author)

P. Lalitha Surya Kumari
Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Hyderabad, India
vlalithanagesh@gmail.com

Received: 15 May 2024 | Revised: 3 June 2024 | Accepted: 6 June 2024

 DOI: https://doi.org/10.48084/etasr.7844

ABSTRACT

The Smart Autonomous Vehicular System (AVS) is designed to combine technologies such as sensors, cameras, radars, and machine learning algorithms in cars. The implementation of Smart AVS in smart cars has the potential to revolutionize the automotive industry and transform the way we think about transportation. In this paper, the implementation of Smart AVS in smart cars includes two steps. Firstly, the architecture is designed using Microsoft Threat Modelling tool. Secondly, with the use of Engineering Software, smart cars are constructed and simulated to verify and validate algorithms related to autonomous driving, path planning, and other intelligent functionalities. Simulating these algorithms in a controlled virtual environment helps to identify and address issues before implementation on physical vehicles. The main advantages of using the proposed model are early detection of vulnerabilities, realistic simulation of sensor inputs, communication protocol testing, cloud integration validation, user interface, and consumer experience, and validation of compliance with security standards.

Keywords-engine control module; GPS; IoT devices; Microsoft Threat Modelling; sensors; smart Autonomous Vehicular System (AVS)

I. INTRODUCTION

Based on the research work done in the domain of autonomous vehicular systems in smart cars, several research gaps have been identified. There is a notable need for a reliable car-following model that accurately describes the longitudinal dynamics of Autonomous Vehicles (AVs) to evaluate their impact on traffic flow [1]. Additionally, the instability of existing longitudinal control systems on level-2 AVs indicates a pressing need for more robust control systems [2]. Furthermore, there is a lack of comprehensive surveys that provide an overview of autonomous car technology, encompassing both technical and non-technical challenges [3, 4]. Addressing these gaps is essential for advancing the development and deployment of AVs. These research gaps in the field of autonomous vehicular systems in smart cars can be addressed using the Threat Modelling tool and simulations in Proteus software. Smart cars are vehicles that incorporate advanced technologies such as Machine Learning (ML) and the Internet of Things (IoT) to improve safety, efficiency, and driver experience. Smart cars use sensors and IoT devices to collect real-time data, enabling them to analyze and respond to changes in their environment quickly. Authors in [5] reported that self-driving Artificial Intelligent (AI) technologies can greatly reduce driver's workload and improve transportation system safety. Proteus software can be used for modeling autonomous vehicles' behavior in various situations, simulating their interactions with other cars and the environment, and improving their performance.

II. RELATED WORK

Over the past decade, there has been significant progress in the development of smart car technologies. Cybersecurity features need to be built into the technology to ensure that the system is secure and safe to use [6].

A. IoT Devices and Sensors

Authors in [7] explored the potential of integrating IoT devices and sensors with smart car systems to improve road safety. Authors in [8] investigated the use of sensors and ML algorithms to detect road hazards and warn drivers in real-time. Authors in [9] explored the use of IoT devices and sensors to monitor vehicle performance and provide real-time feedback to drivers. In [2, 10] semi-autonomous vehicles capable of cloud-based control both with voice commands and through a Web app are demonstrated.

The development and implementation of IoT sensors to improve road safety is discussed in [11]. Authors in [12] explored the use of IoT technology to create a more efficient and responsive traffic light control system. Authors in [13] introduced an advanced approach for enhancing IoT cybersecurity through adaptive threat identification using deep learning in cyber-physical systems. Authors in [14] presented a low-cost and simple distributed sensor model for commercial vehicles. In [15], a driver identification method that considers road shapes and their impact on driving behavior is proposed.

B. Smart Systems

Authors in [16, 17] propose a design strategy that may be used at the architecture design level of AVs that may facilitate the development, analysis and, consequently, safety level. In [18], an efficient obstacle detection and avoidance model based on 2D LiDAR for autonomous mobile robot is proposed. Authors in [19] discussed the basic chronology leading to the development of autonomous cars. Authors in [20] showed that the timing involved in the takeover can be obtained by using a performance-based approach considering human factors. Author in [21] introduced a deep learning approach for detecting malware and software piracy threats.

C. Proteus Software

The use of Proteus software is very useful in carrying out practical learning [22, 23]. Authors in [24] introduced a new simulation software package for microcontroller, Proteus Virtual System Modeling (VSM) for industrial and educational use. The practice of simulation in Proteus in digital teaching can be seen in [25, 26].

D. Spoofing Attacks

Authors in [27] proposed an efficient GPS-free vehicle localization algorithm by exploiting vehicle-to-infrastructure communications. It is an on-board odometer and Inertial Measurement Unit (IMU)-assisted and Single Roadside Unit (RSU)-based approach. Authors in [28] proposed a new approach to detect and handle sensor spoofing attack against automotive radars -a key component for assisted and autonomous driving- by extending multiple beamforming in an automotive MIMO radar. Authors in [29] utilized transportation and vehicle engineering domain knowledge to detect GPS spoofing attacks towards CVs and AVs]. Authors in [30] provided an overview of various authentication schemes proposed over time which are used in 6G IoE-based vehicular communication environment. Authors in [31] investigated security and privacy issues and their solutions for the smart transportation. Authors in [19] proposed a model utilizing machine learning to protect AVs from LiDAR Spoofing attacks.

E. The Threat Modelling Tool

Authors in [32] provide a threat modeling approach for VANET networks using the PASTA threat model process focusing on AI attacks Authors in [1] propose a robust threat analysis and risk assessment framework with mathematical modeling to identify cyber-physical threats to AV perception systems that are critical for the driving behaviors and complex interactions of AVs in their operational design domain. Authors in [33] propose a nature-inspired algorithm for threat modeling in AVs.

The main contributions of the current research paper are:

- The Architecture of Smart AVS in cars is designed with the Microsoft Threat Modeling tool.
- Smart cars are constructed and simulated with the help of Proteus Software.

III. THE PROPOSED MODEL

Figure 1 shows the proposed Smart AVS model.

A. Design and Architecture

The design includes the following sub modules: sensor zone, cloud zone, in-vehicle information, consumer zone and communication protocol.

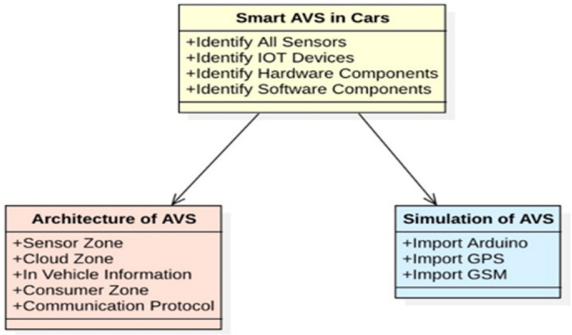

Fig. 1. Proposed model of Smart AVS in cars.

Sensor Zone: This zone includes all the sensors mounted on the vehicle, such as cameras, LiDAR, radar, ultrasonic sensors, etc. The Sub-Modules included in this zone are Camera Module, LiDAR Module, Radar Module, and Ultrasonic Module.

Cloud Zone: This zone involves the off-vehicle infrastructure, where data is processed, and decisions are made. The Sub-Modules included in this zone are Cloud Servers, Data Storage, Decision-Making Algorithms.

In-Vehicle Information: This module includes the internal systems and components of the vehicle, such as the onboard computer, control systems, and the Human-Machine Interface (HMI). The Sub-Modules included here are Onboard Computer, Control Systems and HMI.

Consumer Zone: This zone involves the interaction between the vehicle and external entities, such as mobile apps, remote control systems, and other user interfaces. The Sub-Modules included are Mobile Apps, Remote Control Systems, and User Interfaces. Unauthorized Access to Mobile Apps, Remote Hijacking, Social Engineering Attacks on Users, Unauthorized Access to User Interfaces are threats which occur in this zone.

Communication Protocol: The communication protocol module involves the methods and protocols used for communication between different modules and with external systems. The Sub-Modules included here are Vehicle-to-

Vehicle (V2V) Communication, Vehicle-to-Infrastructure (V2I) Communication, and External Communication Interfaces. Man-in-the-Middle Attacks, Communication Interception, Spoofing of Communication Signals, Protocol Exploitation are the threats which occur in this module.

These threats can be visualized and analyzed with the Microsoft Threat Modelling Tool. It can also generate reports that help the development and security teams communicate with each other.

B. Simulation of AVS

The working process of Smart AVS in cars involves several steps. A detailed overview of the implementation process follows. Figure 2 shows how, with the use of Proteus Software, smart cars are constructed and simulated. The possibility of error is less in software simulation than in a practical circuits.

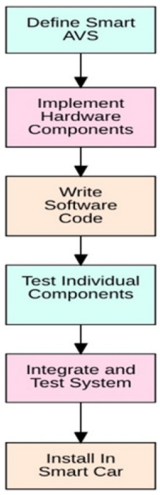

Fig. 2. Implementation process overview.

C. Simulation Methodology of Smart AVS

- Design the architecture of the Smart AVS system, including the hardware components (e.g. Arduino Uno, sensors, microphones, speakers) and software components (e.g. speech recognition algorithm, NLP algorithm).
- Implement the hardware components of the system in software, including the Arduino Uno and any necessary sensors or actuators.
- Write the software code for the Smart AVS system. Use appropriate programming languages and libraries.
- Test the individual hardware and software components of the Smart AVS system.
- Integrate the individual components into a complete system and test its functionality and performance.
- Install the Smart AVS system in a smart car, ensuring that all components are properly connected and secured.
- Perform thorough testing of the Smart AVS system in real-world driving scenarios to ensure its reliability and safety.

IV. RESULTS AND DISCUSSION

A. Design Phase

The architecture of the system can be understood and visualized using the design phase of the Threat Modelling Tool. The Data Flow Diagram (DFD) in Figure 3 is a common technique used during this phase to represent the flow of data within the system. To represent all the components in the DFD, stencils are used. Stencils are graphical elements or symbols for representing all the zones to indicate components or services that are hosted in them. Potential security risks must be considered while designing the architecture. The common threats linked to various components and communication channels are identified using this tool (Figure 4).

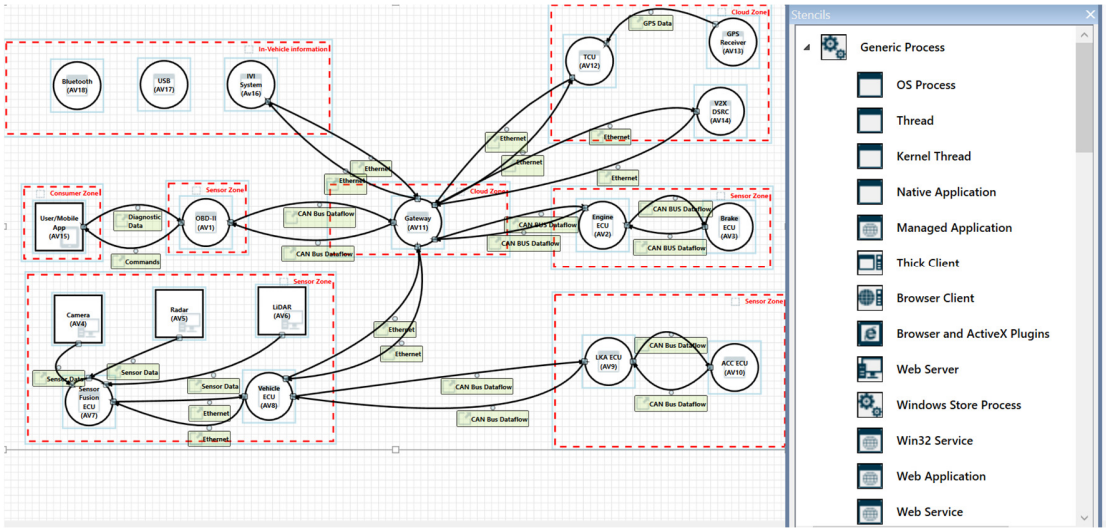

Fig. 3. DFD of the proposed Smart AVS system in cars using stencils.

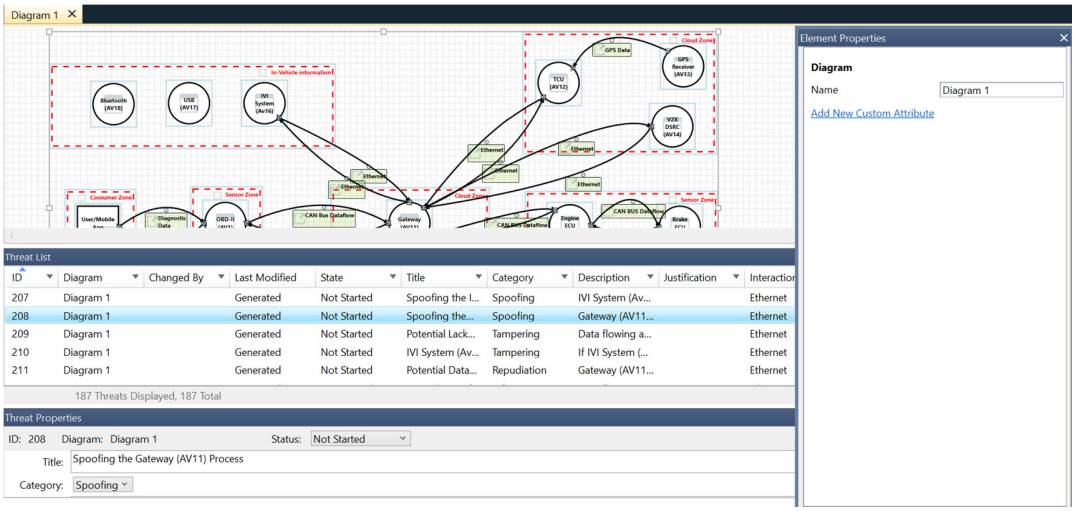

Fig. 4. DFD of the proposed Smart AVS system in cars with threat list and properties.

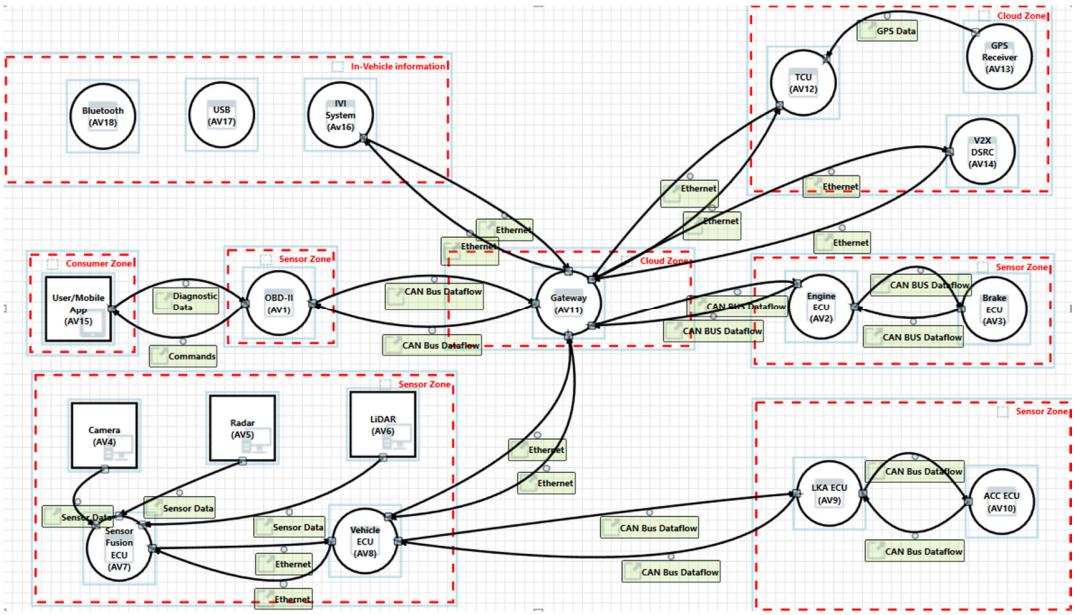

Fig. 5. Architecture of the proposed Smart AVS system in cars.

Figure 5 gives the clear representation of the architecture of the proposed Smart AVS system in cars. This architecture also reveals and illustrates security boundaries between different zones. For example, the communication between the internal vehicle systems and external servers could be a security boundary. The next step after designing the architecture is to simulate and test the electronic aspect of Smart AVS that involves hardware components, such as microcontrollers, sensors, and actuators.

B. Working Results

The design of the electronic circuitry of the Smart AVS was constructed in Proteus as shown in Figure 6. The construction included placing components like microcontrollers, sensors, and actuators on the virtual breadboard. Arduino UNO Microcontroller was selected from the library and placed on the virtual breadboard. Sensor and actuator components were added to the circuit and connected to the Arduino Uno.

When the left indicator was turned on, as in Figure 7, the wheels on the left side of the vehicle will begin to rotate at a different speed than the wheels on the right side. This is because the AVS system is designed to activate the turn signal and initiate a turn when the left indicator is turned on. The system achieves this by using sensors and computer algorithms to control the steering and braking systems of the car, which in turn control the rotation of the wheels. As the left wheels rotate faster than the right wheels, the car begins to turn in the direction indicated by the left indicator, allowing the driver to navigate the road safely and smoothly. Overall, the rotation of the wheels in a Smart AVS system when the left indicator is on is a critical component of the system's ability to provide safe and efficient automated driving. When the right indicator of a

Smart AVS in is turned on (Figure 8), it triggers a signal to the onboard computer that initiates another series of actions. One of these actions involves the rotation of the wheels on the right-hand side of the car. This is accomplished through the application of power to the motor of each wheel, causing them to turn in a synchronized manner. As the wheels turn, they provide the necessary force for the car to safely change lanes or make a turn to the right. The AVS system is designed to ensure that the turning radius and speed of the car are optimized for the given situation, providing a smooth and efficient driving experience for the driver and passengers. When the backlight indicator of a Smart AVS system is turned on (Figure 9), it typically indicates that the system is active and functioning properly. The exact function of the Smart AVS system and the meaning of the backlight indicator will depend on the specific make and model of the smart car.

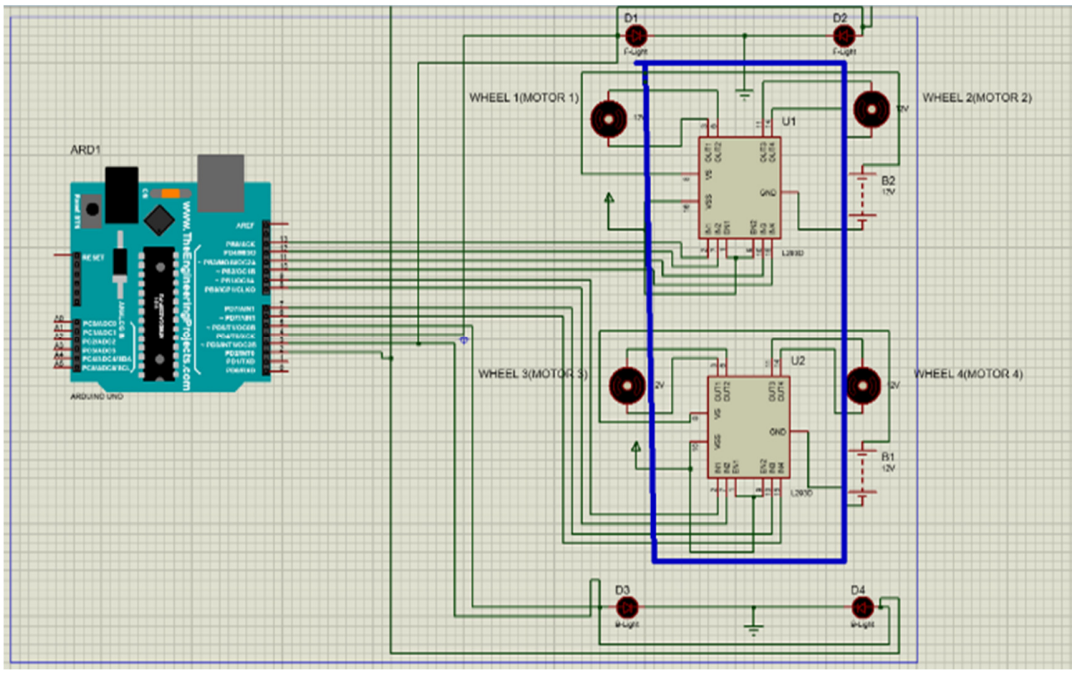

Fig. 6. Implementation of the proposed smart AVS system in smart cars.

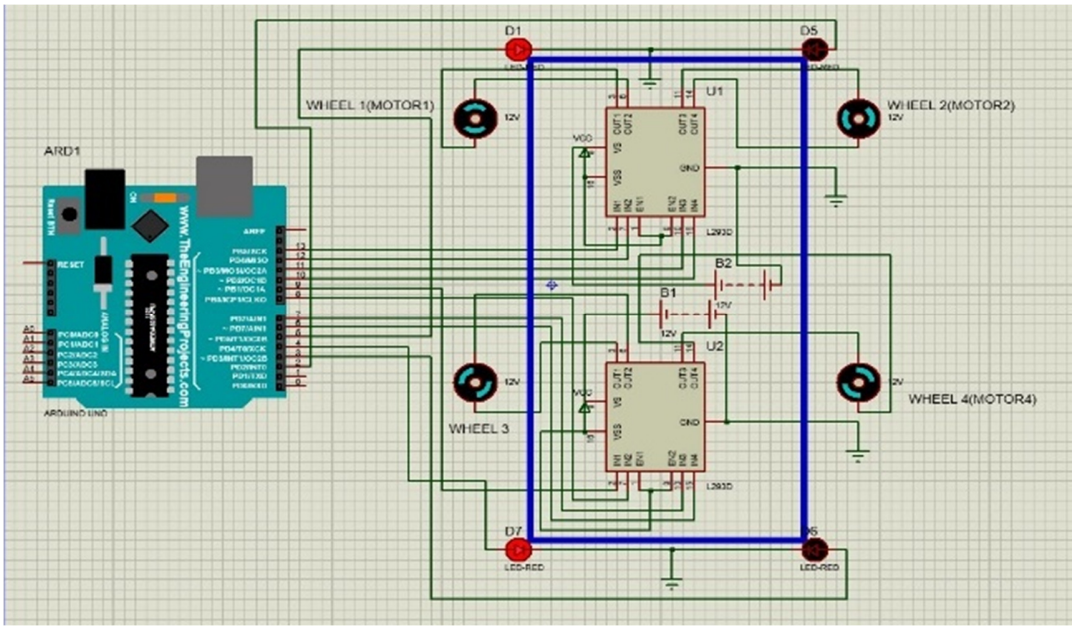

Fig. 7. Rotation of wheels of the Smart AVS system when the left indicator is ON.

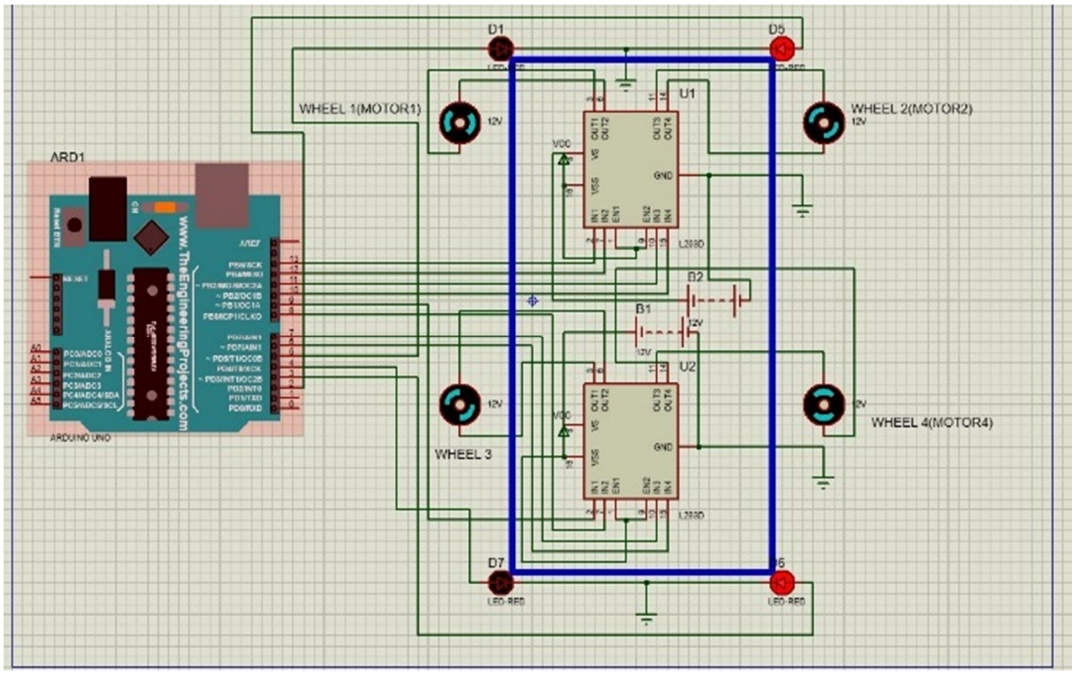

Fig. 8. Rotation of wheels of the Smart AVS system when the right indicator is ON.

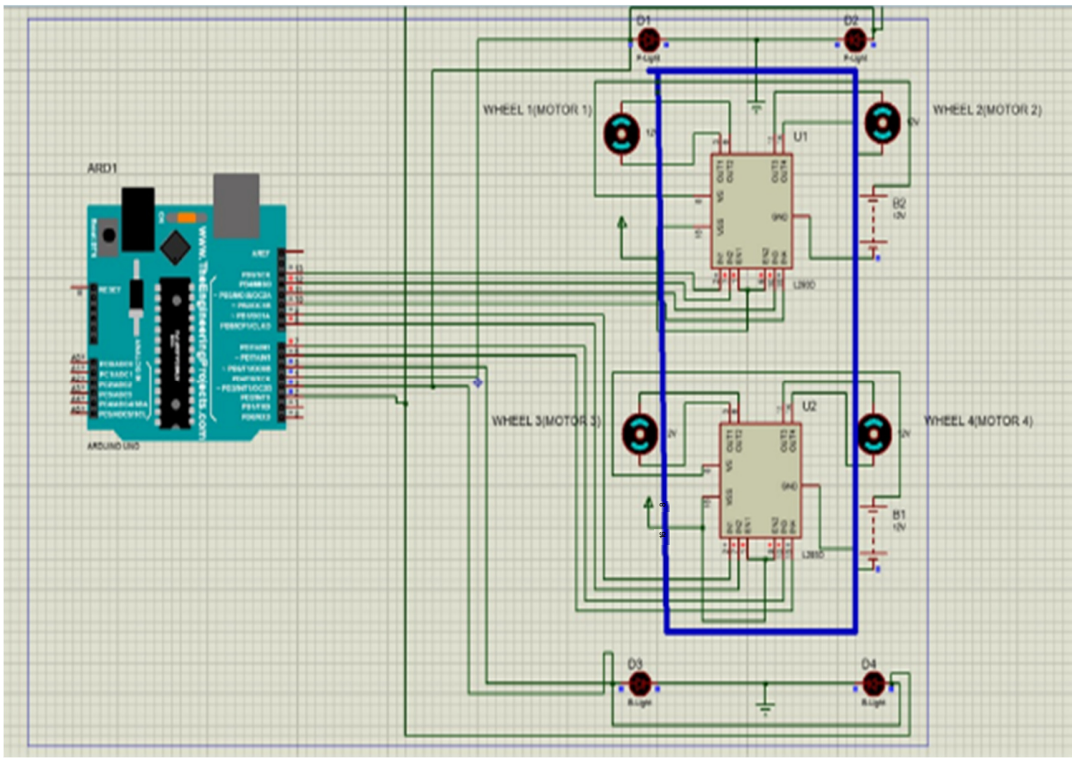

Fig. 9. Rotation of the when the back indicators is ON.

This smart indicator system serves as an example of how modern technology can automate and streamline routine driving tasks, resulting in safer and more intelligent transportation in the future. The vehicle responds smoothly and precisely, lowering the need for human assistance and improving overall comfort while driving.

C. Benefits

The following are the primary benefits of utilizing Proteus software, particularly with an Arduino Uno, to implement the proposed Smart AVS architecture:

- Testing and Simulation: With Proteus, all the parts of the Smart AVS system are modelled and the system's functionality without using the actual components can be tested.
- Time and Money Saving: Proteus's ability to simulate the Smart AVS system can save money and time compared to creating tangible prototypes. With virtual hardware, one can quickly iterate through the design, make modifications, and test various scenarios. These speeds up development and lessens the need for expensive components in the initial phases of the system.
- Early Problem Identification: Early problem detection aids in the development of a more dependable and effective system, regardless of whether the issues are caused by software logic or hardware connections.
- Monitoring and debugging in real time.
- Combining Arduino Development with Integration: This environment allows to write and upload Arduino code directly to the virtual Arduino Uno. Working on the software and hardware components in one cohesive environment is made possible by this integration, which also speeds up the development process.
- Graphic Illustration of the proposed circuitry.
- Testing Hardware-in-the-Loop (HIL): Proteus also facilitates HIL testing, which enables the virtual system to be connected to the actual hardware elements. This gives a more accurate picture of the finished system by allowing verifying how the simulated and real hardware interact.
- Convenience: The convenience of the Smart AVS system could be evaluated based on factors such as the time saved by the driver, the reduction in stress associated with driving, and the overall ease of driving.
- Safety: The safety of the Smart AVS system could be evaluated based on the system's ability to prevent accidents and reduce the risk of injury to drivers and passengers

This software is useful for modeling the hardware components of the Smart AVS system, but it is crucial to remember that its main emphasis is on microcontroller and electronic simulation.

V. CONCLUSION AND FUTURE WORK

In this paper, the Smart Autonomous Vehicular System (AVS) is implemented in cars through a two-step process by adopting the combination of cutting-edge technological design and advantageous engineering application. Firstly, the Microsoft Threat Modelling Tool was used to carefully craft the architecture of the Smart AVS. This allows for a thorough analysis of potential security threats and vulnerabilities. By incorporating security considerations into the system's design from the beginning, this strategic approach paves the way for a safe and resilient autonomous vehicle environment. Secondly, the Smart AVS is put into practice by means of engineering software, which allows for the accurate construction and simulation of smart cars in addition to their conceptualization. The integration of sensors, microcontrollers, communication modules, and cloud functionalities, among other system intricacies, can be dynamically explored in this step. Potential problems and improvements are found through simulation, which helps to improve the Smart AVS implementation.

The realization of the Smart AVS vision in smart cars involves a comprehensive approach, characterized by the seamless integration of specific design using the Microsoft Threat Modelling Tool and hands-on engineering in dedicated software. This two-step procedure prioritizes security, functionality, and innovation, ensuring not only the stability of the autonomous vehicle system but also laying the groundwork for future advancements in smart car technologies. The future work can include the analyzing of various threats which occur in the system by generating a Threat Report.

REFERENCES

[1] S. Ghosh, A. Zaboli, J. Hong, and J. Kwon, "An Integrated Approach of Threat Analysis for Autonomous Vehicles Perception System," *IEEE Access*, vol. 11, pp. 14752–14777, 2023, https://doi.org/10.1109/ACCESS.2023.3243906.

[2] H. Zhou *et al.*, "Review of Learning-Based Longitudinal Motion Planning for Autonomous Vehicles: Research Gaps Between Self-Driving and Traffic Congestion," *Transportation Research Record*, vol. 2676, no. 1, pp. 324–341, Jan. 2022, https://doi.org/10.1177/03611981211035764.

[3] B. Padmaja, C. H. V. Moorthy, N. Venkateswarulu, and M. M. Bala, "Exploration of issues, challenges and latest developments in autonomous cars," *Journal of Big Data*, vol. 10, no. 1, May 2023, Art. no. 61, https://doi.org/10.1186/s40537-023-00701-y.

[4] M. Buehler, K. Iagnemma, and S. Singh, *The DARPA Urban Challenge: Autonomous Vehicles in City Traffic*. Berlin, Germany: Springer, 2009.

[5] A. Swief and M. El-Habrouk, "A survey of Automotive Driving Assistance Systems technologies," in *International Conference on Artificial Intelligence and Data Processing*, Malatya, Turkey, Sep. 2018, pp. 1–12, https://doi.org/10.1109/IDAP.2018.8620826.

[6] A. Naik, "The Use of Artificial Intelligence (AI) in the Automobile Industry," *International Research Journal of Modernization in Engineering Technology and Science*, vol. 4, no. 7, pp. 3968–3971, 2022.

[7] S. Jha, N. Jha, D. Prashar, S. Ahmad, B. Alouffi, and A. Alharbi, "Integrated IoT-Based Secure and Efficient Key Management Framework Using Hashgraphs for Autonomous Vehicles to Ensure Road Safety," *Sensors*, vol. 22, no. 7, Jan. 2022, Art. no. 2529, https://doi.org/10.3390/s22072529.

[8] O. V. Bitkina, J. Kim, J. Park, J. Park, and H. K. Kim, "Identifying Traffic Context Using Driving Stress: A Longitudinal Preliminary Case Study," *Sensors*, vol. 19, no. 9, Jan. 2019, Art. no. 2152, https://doi.org/10.3390/s19092152.

[9] D. Wang, D. Chen, B. Song, N. Guizani, X. Yu, and X. Du, "From IoT to 5G I-IoT: The Next Generation IoT-Based Intelligent Algorithms and 5G Technologies," *IEEE Communications Magazine*, vol. 56, no. 10, pp. 114–120, Oct. 2018, https://doi.org/10.1109/mcom.2018.1701310.

[10] J. A. Solorio, J. M. Garcia-Bravo, and B. A. Newell, "Voice Activated Semi-Autonomous Vehicle Using Off the Shelf Home Automation Hardware," *IEEE Internet of Things Journal*, vol. 5, no. 6, pp. 5046–5054, Dec. 2018, https://doi.org/10.1109/JIOT.2018.2854591.

[11] K. Pretz, "MIT Professor's IoT Sensors Make Roads Safer - IEEE Spectrum." 12 Nov. 2023, https://spectrum.ieee.org/mit-professor-iot-sensors.

[12] M. A. Hamad, A. El Hajj, R. A. Z. Daou, A. Hayek, and G. A. Haidar, "Advanced IOT Traffic Light Control System," in *Fifth International Conference on Advances in Computational Tools for Engineering Applications*, Zouk Mosbeh, Lebanon, Jul. 2023, pp. 69–75, https://doi.org/10.1109/ACTEA58025.2023.10193999.

[13] C. Atheeq, R. Sultana, S. A. Sabahath, and M. A. K. Mohammed, "Advancing IoT Cybersecurity: Adaptive Threat Identification with Deep Learning in Cyber-Physical Systems," *Engineering, Technology & Applied Science Research*, vol. 14, no. 2, pp. 13559–13566, Apr. 2024, https://doi.org/10.48084/etasr.6969.

[14] S. J. Subhan, T. Avinash, and S. Thirumal, "Driver's Safety Management System for Commercial Purposes using IoT," in *7th International Conference on Communication and Electronics Systems*, Coimbatore, India, Jun. 2022, pp. 334–339, https://doi.org/10.1109/ICCES54183.2022.9835894.

[15] J. Lee, M. Kim, S. Park, J. Choi, and Y. Hwang, "Driver Identification for Different Road Shapes Using Vehicle IoT Sensing Data," in *IEEE International Conference on Consumer Electronics*, Las Vegas, NV, USA, Jan. 2021, pp. 1–5, https://doi.org/10.1109/ICCE50685.2021.9427668.

[16] C. B. S. T. Molina, J. R. de Almeida, L. F. Vismari, R. I. R. Gonzalez, J. K. Naufal, and J. Camargo, "Assuring Fully Autonomous Vehicles Safety by Design: The Autonomous Vehicle Control (AVC) Module Strategy," in *47th Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshops*, Denver, CO, USA, Jun. 2017, pp. 16–21, https://doi.org/10.1109/DSN-W.2017.14.

[17] R. Passerone *et al.*, "A Methodology for the Design of Safety-Compliant and Secure Communication of Autonomous Vehicles," *IEEE Access*, vol. 7, pp. 125022–125037, 2019, https://doi.org/10.1109/ACCESS.2019.2937453.

[18] D. Ghorpade, A. D. Thakare, and S. Doiphode, "Obstacle Detection and Avoidance Algorithm for Autonomous Mobile Robot using 2D LiDAR," in *International Conference on Computing, Communication, Control and Automation*, Pune, India, Aug. 2017, pp. 1–6, https://doi.org/10.1109/ICCUBEA.2017.8463846.

[19] M. R. Hadiya, "A Review paper on Development of Autonomous Vehicle," *International Research Journal of Engineering and Technology*, vol. 6, no. 1, pp. 445–449, 2019.

[20] H. J. Kim and J. H. Yang, "Takeover Requests in Simulated Partially Autonomous Vehicles Considering Human Factors," *IEEE Transactions on Human-Machine Systems*, vol. 47, no. 5, pp. 735–740, Nov. 2017, https://doi.org/10.1109/THMS.2017.2674998.

[21] K. Aldriwish, "A Deep Learning Approach for Malware and Software Piracy Threat Detection," *Engineering, Technology & Applied Science Research*, vol. 11, no. 6, pp. 7757–7762, Dec. 2021, https://doi.org/10.48084/etasr.4412.

[22] A. R. S. Arif, A. Nuriyanis, A. Hendartono, E. Sirait, F. S. Kurniawan, and C. O. Putri, "Analysis of The use of Proteus Software as a Practical Learning Support," *International Journal of Engineering and Applied Technology*, vol. 7, no. 1, pp. 30–39, May 2024, https://doi.org/10.52005/ijeat.v7i1.96.

[23] S. Jumini, E. Trisnowati, and D. Dahnuss, "Proteus as a virtual simulation to improve readiness and process skills in laboratory experiment," *Journal of Physics: Conference Series*, vol. 1517, no. 1, Dec. 2020, Art. no. 012074, https://doi.org/10.1088/1742-6596/1517/1/012074.

[24] B. Su and L. Wang, "Application of Proteus virtual system modelling (VSM) in teaching of microcontroller," in *International Conference on E-Health Networking Digital Ecosystems and Technologies*, Shenzhen, China, Apr. 2010, vol. 2, pp. 375–378, https://doi.org/10.1109/EDT.2010.5496343.

[25] D. Cika and D. Grundler, "Proteus Virtual System Modelling used for microcontroller education," in *33rd International Convention MIPRO*, Opatija, Croatia, Dec. 2010, pp. 1034–1038.

[26] T. Jiang-Bo and Z. Jin, "Experimental Instructional Design of MCU Based on Proteus and Teaching Resource Pool," in *2nd International Conference on Artificial Intelligence and Education*, Dali, China, Jun. 2021, pp. 132–136, https://doi.org/10.1109/ICAIE53562.2021.00035.

[27] S. Ma, F. Wen, and Z. Wang, "An Efficient GPS-Free Vehicle Localization Algorithm Using Single Roadside Unit and Receiver," in *International Conference on Networking and Network Applications*, Xi'an, China, Oct. 2018, pp. 310–313, https://doi.org/10.1109/NANA.2018.8648764.

[28] P. Kapoor, A. Vora, and K.-D. Kang, "Detecting and Mitigating Spoofing Attack Against an Automotive Radar," in *88th Vehicular Technology Conference*, Chicago, IL, USA, Aug. 2018, pp. 1–6, https://doi.org/10.1109/VTCFall.2018.8690734.

[29] Z. Yang *et al.*, "Anomaly Detection Against GPS Spoofing Attacks on Connected and Autonomous Vehicles Using Learning From Demonstration," *IEEE Transactions on Intelligent Transportation Systems*, vol. 24, no. 9, pp. 9462–9475, Sep. 2023, https://doi.org/10.1109/TITS.2023.3269029.

[30] P. Kohli, S. Sharma, and P. Matta, "Secured Authentication Schemes of 6G Driven Vehicular Communication Network in Industry 5.0 Internet-of-Everything (IoE) Applications: Challenges and Opportunities," in *2nd International Conference on Mobile Networks and Wireless Communications*, Tumkur, Karnataka, India, Dec. 2022, pp. 1–5, https://doi.org/10.1109/ICMNWC56175.2022.10031781.

[31] N. Alsaffar, H. Ali, and W. Elmedany, "Smart Transportation System: A Review of Security and Privacy Issues," in *International Conference on Innovation and Intelligence for Informatics, Computing, and Technologies*, Sakhier, Bahrain, Nov. 2018, pp. 1–4, https://doi.org/10.1109/3ICT.2018.8855737.

[32] K. M. A. Alheeti, A. Alzahrani, and D. Al Dosary, "LiDAR Spoofing Attack Detection in Autonomous Vehicles," in *IEEE International Conference on Consumer Electronics*, Las Vegas, NV, USA, Jan. 2022, pp. 1–2, https://doi.org/10.1109/ICCE53296.2022.9730540.

[33] I. Jemal, O. Cheikhrouhou, and M. A. Haddar, "IoT DOS and DDOS Attacks Detection Using an Effective Convolutional Neural Network," in *International Conference on Cyberworlds*, Sousse, Tunisia, Oct. 2023, pp. 373–379, https://doi.org/10.1109/CW58918.2023.00065.