Automotive Security Virtual Exploration Platform for Wheel Speed Sensor Attacks

Kyra Nhat-Thy Vo
Engineering Science Department
Smith College
1 Chapin Way, Northampton, MA 01063
kvo@smith.edu

Bhagawat Baanav Yedla Ravi
Department of ECE
University of Florida
Gainesville, FL 32611, USA
b.yedlaravi@ufl.edu

Mustafa Mohammad Shaky
Department of ECE
University of Florida
Gainesville, FL 32611, USA
mustafa.shaky@ufl.edu

Sandip Ray
Department of ECE
University of Florida
Gainesville, FL 32611, USA
sandip@ece.ufl.edu

2025 IEEE 22nd International Conference on Mobile Ad-Hoc and Smart Systems (MASS) | 979-8-3315-6599-2/25/$31.00 ©2025 IEEE | DOI: 10.1109/MASS66014.2025.00103

***Abstract*—Understanding automotive security becomes more significant as the probability of the average person interacting with an autonomous vehicle accelerates— Yet, only a small group of specialized experts understands the nuances of security in automotive systems. With this paper, we address this knowledge gap by developing an exploration platform that provides hands-on experience with wheel speed sensors (WSS) and their security weaknesses. Unlike previous research that based such exploration platforms solely on hardware or exclusively on virtual reality, this platform combines the two. Users, from students to industry professionals, may experience different wheel speed sensor attacks from the attacker and victim perspectives in a virtual environment built with Unity, a game development engine. The experience uses data from a wheel speed sensor model and a solenoid attacker module coded with Arduino. We describe the development process for this wheel speed sensor exploration platform and demonstrate how it might be used to understand different attack vectors, including a new spoofing attack developed with the platform that allows the attacker to accurately control the wheel speed with a PID controller and spoofed magnetic pulses. The platform serves as a medium for researchers to create and defend against new attacks and as an educational resource to expand knowledge in the automotive security field.**

I. Introduction

Autonomous and driver assistance features in modern vehicles rely heavily on sensor data to operate effectively. These vehicles use technologies such as radar, LiDAR, and cameras to perceive their surroundings, but it is equally vital for them to monitor internal states like position, speed, and acceleration. Wheel speed sensors (WSS) provide real-time data on the rotational speed and direction of each wheel, supporting critical safety systems such as Anti-Lock Braking Systems (ABS), Traction Control Systems (TCS), and Electronic Stability Control (ESC). Wheel speed sensors (WSS) provide real-time data on the rotational speed and direction of each wheel, supporting critical safety systems such as Anti-Lock Braking Systems (ABS), Traction Control Systems (TCS), and Electronic Stability Control (ESC). As autonomous systems reduce the need for constant human oversight, the potential for such attacks only increases. It is crucial for professionals across the automotive industry—engineers, designers, policymakers, mechanics—as well as end users and cybersecurity researchers to understand the mechanics and risks of WSS attacks. While some research exists, this topic remains largely underexplored and under-communicated to the broader public.

To bridge the current gap in awareness, this work introduces a wheel speed sensor (WSS) exploration platform that uniquely integrates both virtual reality and physical hardware to educate users about the role and vulnerabilities of WSS in vehicle dynamics. The platform presents realistic driving scenarios—both benign and adversarial—within a virtual environment built using Unity, a widely adopted and accessible game engine. Unlike systems that rely on synthetic data, this platform uses real-time inputs from a WSS hardware model, offering a more accurate representation of real sensor behavior. The hardware component is developed using Arduino, incorporating two microcontrollers, Hall effect sensors, magnets, a solenoid, a servo motor, and custom 3D-printed parts. This modular and open-source design allows users to easily reconfigure or scale the platform to suit their learning or research objectives. As the platform evolves, it is intended to support remote interaction, with wireless communication between the computer running the Unity simulation and the physical hardware—making it more affordable and accessible by removing the need for users to own the hardware themselves. With its flexible design and hands-on capabilities, the platform serves a broad audience—from students and newcomers to automotive systems, to industry professionals and cybersecurity researchers. By enabling intuitive, real-time exploration of WSS behavior and attack impacts, this paper lays the groundwork for greater understanding and broader

2155-6814/25/$31.00 ©2025 IEEE
DOI 10.1109/MASS66014.2025.00103

education around a critical but often overlooked component of vehicle safety. The novel contributions of this paper are as follows:

- We introduce an exploration platform that uniquely combines physical hardware with a virtual reality (VR) environment, enabling realistic and accurate modeling of wheel speed sensor (WSS) behavior under both benign and attack scenarios.
- The platform is designed to be modular and scalable. Both the VR environment and hardware components—including sensors, actuators, and 3D-printed parts—can be easily reconfigured or extended to meet the specific needs of users, ranging from basic demonstrations to complex research applications.
- This platform serves as an effective educational tool by providing continuous, hands-on learning experiences. Users receive real-time feedback on WSS behavior and attack impacts, making the system accessible and informative for learners, educators, and professionals alike.

The remainder of this paper is organized as follows: Section II provides an overview of wheel speed sensors, their functionality, potential attack surfaces, and a review of related research and exploration platforms. Section III details the development of the virtual environment, outlines the architecture of the proposed platform, highlights its various use cases, and presents a novel attack on wheel speed sensors enabled by the platform. Finally, Section IV concludes the paper.

II. Background and Related Work

A. Overview of Wheel Speed Sensors and Related Attacks

Wheel speed sensors measure the speed each wheel rotates in real time. These sensors provide essential data for various safety functionalities in a vehicle, such as the Anti-Lock Braking System (ABS), Traction Control Systems (TCS), and Electronic Stability Control (ESC). For example, the ABS module uses WSS to detect if one wheel is decelerating more slowly than the other wheels when the driver is braking. If this is the case, the slower wheel has likely lost traction, and the ABS module repeatedly applies and releases brake pressure on that wheel until it gains traction, potentially saving the driver's life. In addition, a vehicle's speedometer displays information collected by the wheel speed sensor. There are two kinds of wheel speed sensors: passive and active. Passive wheel speed sensors consist of a wire wound around a permanent magnet that alters the magnetic field of a toothed tone ring that turns with the wheel [1]. This generates a sine wave analog signal. On the other hand, the more common active wheel speed sensors consist of a Hall effect sensor that reads magnetic pulses from a ferromagnetic tone ring with areas of alternating magnetic polarities. A malicious attacker may generate a magnetic field that affects the data read by the wheel speed sensor, since the hall effect sensor has no way to determine which magnetic pulses are false or true [2]. For example, the attacker can cause a jamming attack by sending magnetic pulses at a high frequency, which can blind the WSS from reading magnetic pulses from the tone ring. Moreover, an attacker could cause a spoofing attack by sending false magnetic pulses alongside the tone ring's true magnetic pulses, causing the WSS to read both values.

B. Relevant Research on Exploration Platforms

A substantial body of research has investigated wheel speed sensors, addressing diverse aspects such as performance optimization and energy harvesting, while also delving into their exploitation for cyber-physical attacks. Notably, Pollny *et al.* [2] utilized an audio amplifier in conjunction with a Helmholtz coil to generate electromagnetic fields at varying frequencies, assessing their impact on electronic stability control via a Hardware-in-the-Loop (HiL) simulation. In a separate effort, Shoukry *et al.* [3] designed an ABS spoofing prototype to facilitate sensor-targeted attacks, highlighting the potential safety implications of such vulnerabilities.

Parallel to these offensive strategies, several studies have proposed detection and mitigation techniques. For instance, Shin *et al.* [4] implemented deep neural networks to identify anomalies indicative of sensor attacks. Similarly, Kang *et al.* [5] developed a predictive model based on historical vehicle state data, introducing a mitigation approach that subtracts inferred attack artifacts from the real-time measurements.

Despite these advancements, existing literature lacks educational resources tailored for individuals newly engaging with vehicular cybersecurity. While Wang *et al.* [6] introduced a benchtop platform to support instructional efforts related to ABS operation, its scope excludes cybersecurity applications. In contrast, educational frameworks have been developed for other vehicular subsystems, such as ultrasonic sensors [7], [8], V2X communications [9], and computer vision modules [10]. Furthermore, Kabir *et al.* [11] introduced ViSE, a digital twin platform designed to facilitate experiential learning in automotive functional safety and cybersecurity. HAWA [1] a table top exploration platform to understand wheel speed sensors explore spoofing and jamming attacks. Nonetheless There has not been a platform that enables virtual exploration of security attacks targeting wheel speed sensor vulnerabilities and their corresponding defense mechanisms.

III. Methodology

A. Overview of Exploration Platform

The exploration platform consists of two primary components: a physical hardware setup and a virtual reality (VR) environment, as shown in 1. The VR environment receives real-time wheel speed data from the hardware, allowing it to incorporate uncertainties that naturally arise in physical systems and accurately reflect the effects of different attacker parameter values. In contrast to previous automotive security exploration platforms that relied on predefined behaviors or simulated inputs, this platform provides a more realistic and dynamic experience by using data from an actual wheel speed sensor (WSS) model [12]. Within the virtual environment, users can interact with the platform from two perspectives: as an attacker, they can tune solenoid parameters to observe

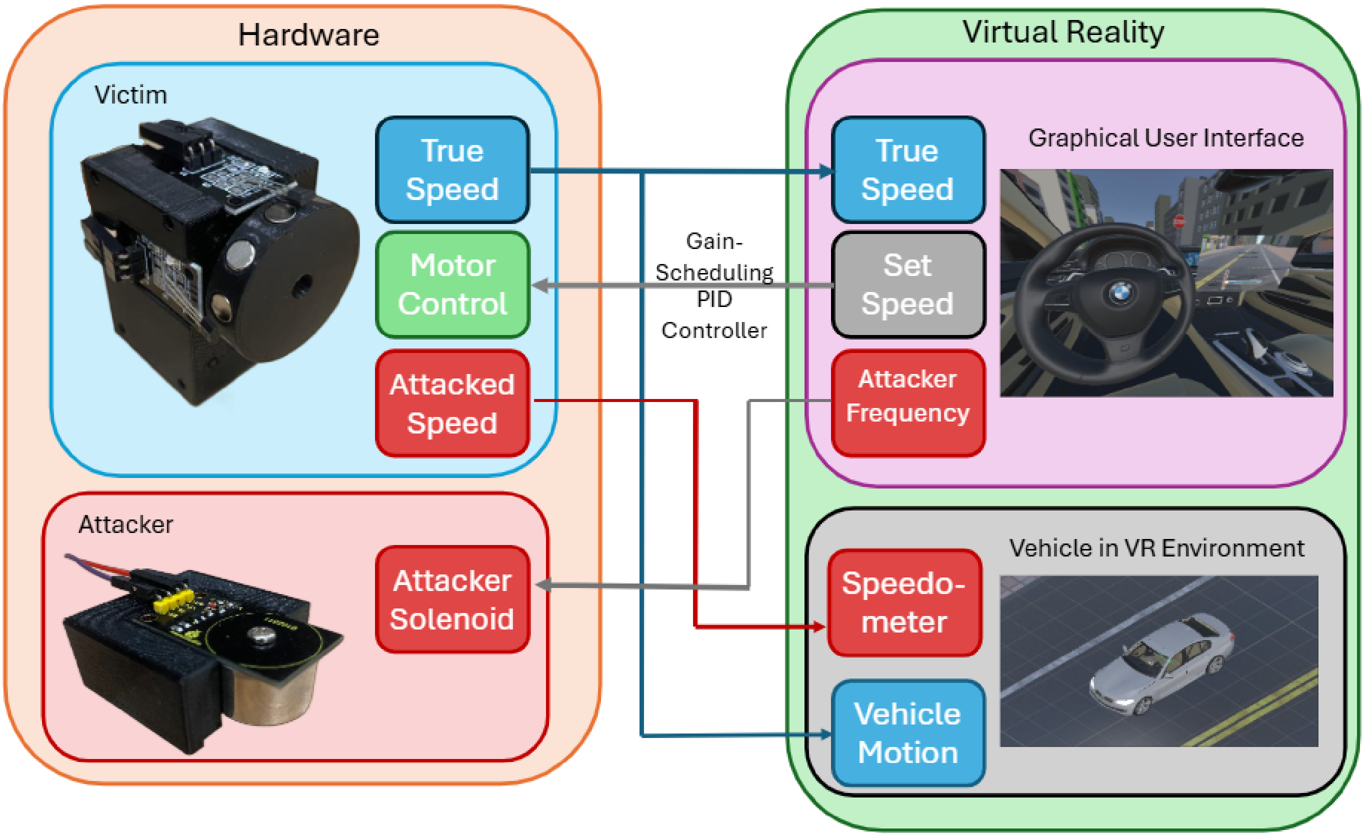

Fig. 1. Architectural Diagram

the impact on the sensor and vehicle behavior, and as a victim, they can operate the vehicle and experience how attacks affect its performance and response in real time. This dual-role interaction enhances user understanding of WSS vulnerabilities and their implications on vehicle safety.

B. Requirements for Exploration Platform

The exploration platform was designed with accessibility, flexibility, and scalability as core requirements to support a wide range of users—from beginners to advanced researchers. To make the platform approachable for users with limited knowledge of automotive systems or cybersecurity, the virtual reality (VR) environment provides an interactive, hands-on experience. Users can explore wheel speed sensor (WSS) behavior by adjusting parameters and observing realistic attack scenarios. A graphical user interface (GUI) delivers real-time feedback on attack outcomes, enhancing user understanding and engagement. At the same time, the platform is built to support more advanced use cases, including security research and the development of new attack or defense strategies. To enable this, both the hardware and software are modular, reconfigurable, and cost-effective. The VR environment was developed using Unity, a widely supported game engine available in a free edition. The hardware component relies on Arduino, a popular open-source electronics platform, and uses the Oculus Quest 2 headset for immersive interaction. Together, these choices ensure the platform is accessible, educational, and extensible for a diverse range of users.

Fig. 2. Reconfigured Victim and Attacker Modules

Fig. 2 demonstrates how the hardware may be reconfigured. The original design was modified so that a solenoid and third hall effect sensor could be snapped onto the wheel speed sensor. With this new configuration, the attacker can now measure the wheel's current speed, which the user could use to explore different attack methods.

C. Victim Module and GUI Interaction

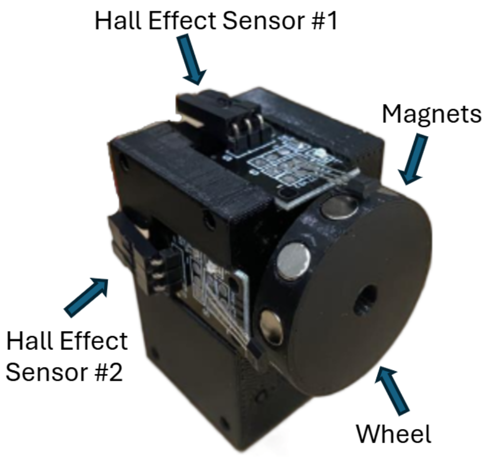

Fig. 3. Victim Module

The victim module shown in Fig. 3 consists of a 3D printed stand, a servo motor that controls a wheel embedded with ten magnets evenly spaced on the rim, and two hall effect sensors which detect magnetic pulses. The first hall effect sensor measures the current wheel speed based on the time taken between detecting two consecutive magnets. The user may attack this hall effect sensor, which will affect the wheel's motor control. The second hall effect sensor measures the ground truth wheel speed– the attacker cannot manipulate its readings.

As depicted in the architectural diagram, the user sets the speed in the GUI, which is sent to the physical victim module. Using Arduino IDE, the servo motor controlling the wheel utilizes a gain-scheduling PID controller to reach the set target speed.

PID Controller Equation:

$$u_n = K_p \cdot e_n + K_i \cdot \sum_{i=0}^{n} e_i \cdot \Delta t + K_d \cdot \frac{e_n - e_{n-1}}{\Delta t}$$

Where:

- u_n: Control output at time step n
- e_n: Error at time step n (e.g., difference between current speed and set speed)
- e_{n-1}: Previous error (from time step $n-1$)
- K_p: Proportional gain
- K_i: Integral gain
- K_d: Derivative gain
- Δt: Time interval between measurements

A gain-scheduling PID controller was selected for the victim module's control system because PID controllers are common in both autonomous and manually driven vehicles. Abdallaoui notes that PID feedback control is a popular strategy in the automotive vehicle industry [13].

The PID controller was tuned using the trial and error method. Initially, all the gain parameters were set to zero.

TABLE I
GAIN SCHEDULING PID PARAMETERS BASED ON SET SPEED

Set Speed (RPM)	K_p	K_i	K_d
0-10	0.1	0.3	0.05
10-20	0.08	0.2	0.05
20-40	0.5	0.45	0.05
40-60	0.55	0.8	0.05
50-70	0.6	1.2	0.05
80-100	0.65	1.7	0.05

The proportional gain was increased until the current wheel speed start oscillating. The integral gain was increased to correct steady state error, until the current speed reached the set speed. Finally, the derivative gain was increased slightly to reduce small oscillations. Gain-scheduling was used because different gain parameters were more effective for different set speed ranges. For example, the proportional gain value of 0.65 would've caused extreme oscillation with a set speed of 10 RPM, but little oscillation if the set speed was 90 RPM.

D. Attacker Module and GUI Interaction

The attacker module shown in Fig. 4 consists of a solenoid, a 3D printed stand, and hall effect sensor. The user can set the attacker frequency, or frequency of magnetic pulses emitted by the solenoid, from the GUI in the VR environment.

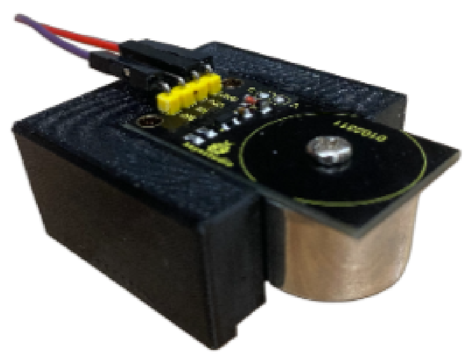

Fig. 4. Attacker Stand and Solenoid

The attacker module connects to the top of the victim module and sends these malicious magnetic pulses to hall effect sensor 1, the hall effect sensor measuring the current speed for the victim's PID controller. As such, the user can manipulate the victim's wheel speed by making the victim believe its speed is slower or faster than the true speed. This attacked speed is displayed on the speedometer of the vehicle in the VR environment. In effect, the user will experience how a wheel speed sensor attack results in falsified speedometer values.

E. True Speed and GUI Feedback

The second hall effect sensor on the victim module measures the true speed the wheel is turning. The ground truth speed will be displayed on the GUI. If there is a difference between the true speed and attacked speed, the GUI will provide feedback to the user that the attack was successful. In addition, the true speed governs how fast the vehicle travels in the virtual environment. The virtual environment shown in Fig. 5 and Fig. 6 was designed to help the user gauge if the true speed differs from the speedometer readings. The evenly spaced streetlights offer landmark-based true speed estimation for the user. In addition, the buildings alternate from gray to light-colored at evenly spaced intervals as another marker for speed estimation. Fig. 5 shows one of the sections of the road that is straight. It is expected that the user performs attacks in this region. Fig. 6 shows the entire track with gentle curvature to let the user prepare for the next trial of attacks.

Fig. 5. Looped Road Virtual Environment with Streetlights and Buildings for Speed Estimation

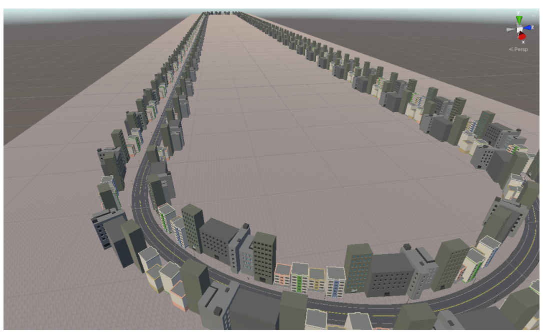

Fig. 6. Complete Looped Road Virtual Environment

IV. Case Studies

The platform allows users to experience three primary scenarios: benign, jamming, and spoofing. While these represent the core categories, users can explore a wide range of outcomes by varying parameters such as speed and frequency. These scenarios and their effects are further illustrated through detailed case studies.

Benign Scenario: In a non-attack or benign scenario, the hardware allows users to experiment with different wheel speed values to explore how these inputs affect drivetrain control. During this phase, the induced speed is set to 0 rpm, indicating that no attack is occurring, as the attacker solenoid remains inactive. To build a foundational understanding of the wheel speed sensor's normal behavior, a scenario is examined where the wheel speed is held constant at 50 rpm and the induced speed remains at 0 rpm. With the solenoid deactivated, users observe a stable speed reading of 50 rpm, confirming the absence of any interference. Users are encouraged to test a range of wheel speed inputs and monitor the corresponding feedback outputs; importantly, the deviation stays at zero as long as the attack mechanism is not activated.

Jamming Attack Scenario: A jamming attack or blinding attack is a type of denial-of-service (DoS) attack that effectively blinds the wheel speed sensor, making it unable to detect any rotation. On the platform, this results in the sensor reading 0 rpm, indicating that it perceives the wheel as completely stationary. This effect can be triggered by exciting the attacker solenoid at a very high frequency—for example, by setting the induced speed to 1000 rpm. In this state, the solenoid acts as if it's continuously on, producing a strong magnetic field that overwhelms the signal from the actual tone wheel. As a result, the sensor detects no variation in the magnetic field and falsely assumes the wheel isn't moving. The system reacts by increasing the throttle in an attempt to reach the expected speed, which causes the wheel to accelerate beyond the platform's safety limit of 100 rpm, reaching up to 110 rpm.

Spoofing Attack Scenario: Spoofing attacks are a type of sensor deception where false signals are used to mislead the system about actual conditions. In the case of wheel speed sensors, an attacker can send either random or fixed fake signals, causing the sensor to misread the wheel's speed. Using the platform, this can be demonstrated in two ways: if the attacker sends a signal that makes the sensor believe the speed is lower than it actually is (for example, showing 20 rpm when the true speed is 50 rpm), the system responds by increasing throttle, causing the vehicle to speed up beyond the intended rate. On the other hand, if the attacker sends a higher fake speed signal, such as 70 rpm, the sensor receives both real and fake signals, interprets the speed as too high, and reduces throttle, causing the vehicle to slow down below the target speed. In both cases, the sensor's perception is manipulated, leading the vehicle to behave incorrectly—either speeding up or slowing down unnecessarily.

Through the above scenarios, users gain insight into how a wheel speed sensor operates and generates vehicle speed measurements, as well as what actions an adversary might take to manipulate or control the vehicle's speed. The VR environment further provides a realistic depiction of how such attacks would appear in practice.

V. Conclusion

As the adoption of autonomous and connected vehicles accelerates, gaining a deeper understanding of automotive cybersecurity—especially at the sensor level—becomes increasingly important. This paper addresses the educational and research gap in this space by introducing a novel exploration platform that integrates real-world hardware with a virtual environment to simulate and study wheel speed sensor (WSS) behavior under both benign and attack conditions. The platform, developed using Arduino-based hardware and a Unity-built virtual environment, offers a scalable, reconfigurable, and immersive experience. The virtual environment not only visualizes the impact of various attack vectors but also provides users with a highly relevant, hands-on learning opportunity in a safe and controlled setting. By enabling users to explore spoofing, jamming, and other forms of sensor manipulation from both attacker and victim perspectives, the platform enhances understanding through active participation. Furthermore, its accessible design allows users—from students and educators to researchers and industry professionals—to engage with real-time data and experiment with modifications at both the hardware and software levels. With future plans for remote connectivity and scalability, this platform serves as a foundational tool for advancing education and research in automotive cybersecurity.

Acknowledgements: This work was partially supported by NSF Grants REU-2150136 and SATC-2221900.

REFERENCES

[1] B. B. Y. Ravi and S. Ray, "Hands-on exploration and learning platform for automotive wheel speed sensor attacks," in *2025 IEEE International Conference on Consumer Electronics (ICCE)*, 2025, pp. 1–6.

[2] O. Pöllny, A. Held, and F. Kargl, "On the manipulation of wheel speed sensors and their impact in autonomous vehicles," in *2020 IEEE Intelligent Vehicles Symposium (IV)*, 2020, pp. 1530–1537.

[3] Y. Shoukry, P. Martin, P. Tabuada, and M. Srivastava, "Non-invasive spoofing attacks for anti-lock braking systems," in *Cryptographic Hardware and Embedded Systems-CHES 2013: 15th International Workshop, Santa Barbara, CA, USA, August 20-23, 2013. Proceedings 15*. Springer, 2013, pp. 55–72.

[4] J. Shin, Y. Baek, Y. Eun, and S. H. Son, "Intelligent sensor attack detection and identification for automotive cyber-physical systems," in *2017 IEEE Symposium series on computational intelligence (SSCI)*. IEEE, 2017, pp. 1–8.

[5] L. Kang and H. Shen, "Attack detection and mitigation for sensor and can bus attacks in vehicle anti-lock braking systems," in *2020 29th International Conference on Computer Communications and Networks (ICCCN)*. IEEE, 2020, pp. 1–9.

[6] B. Wang, "Design of teaching platform for abs wheel speed sensor," in *Journal of Physics: Conference Series*, vol. 2187, no. 1. IOP Publishing, 2022, p. 012004.

[7] B. B. Y. Ravi, M. R. Kabir, N. Mishra, S. Boddupalli, and S. Ray, "Autohal: An exploration platform for ranging sensor attacks on automotive systems," in *2022 IEEE International Conference on Consumer Electronics (ICCE)*. IEEE, 2022, pp. 1–2.

[8] J. Carter, B. B. Yedla Ravi, M. R. Kabir, and S. Ray, "Poster: Efficient exploration of automotive ranging sensor attacks," in *Proceedings of the Twenty-Fourth International Symposium on Theory, Algorithmic Foundations, and Protocol Design for Mobile Networks and Mobile Computing*, ser. MobiHoc '23. New York, NY, USA: Association for Computing Machinery, 2023, p. 589–591. [Online]. Available: https://doi.org/10.1145/3565287.3617986

[9] D. M. Prakash, B. B. Y. Ravi, S. Boddupalli, and S. Ray, "Vecaep: A hands-on exploration platform for vehicular communication attacks," in *2023 IEEE 97th Vehicular Technology Conference (VTC2023-Spring)*. IEEE, 2023, pp. 1–5.

[10] V. S. Gireesh Chamarthi, X. Chen, B. B. Yedla Ravi, and S. Ray, "Exploration of machine learning attacks in automotive systems using physical and mixed reality platforms," in *2023 IEEE International Conference on Consumer Electronics (ICCE)*, 2023, pp. 1–4.

[11] M. R. Kabir and S. Ray, "Vise: Digital twin exploration for automotive functional safety and cybersecurity," *Journal of Hardware and Systems Security*, pp. 1–12, 2024.

[12] R. Owoputi, M. R. Kabir, and S. Ray, "Ive: An immersive virtual environment for automotive security exploration," *Immersive Learning Research-Academic*, pp. 468–480, 2023.

[13] S. Abdallaoui, H. Ikaouassen, A. Kribèche, A. Chaibet, and E.-H. Aglzim, "Advancing autonomous vehicle control systems: An in-depth overview of decision-making and manoeuvre execution state of the art," *The Journal of Engineering)*, vol. 2023, 11 2023.