iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 **Issue:** V **Month of publication:** May 2025

DOI: https://doi.org/10.22214/ijraset.2025.70603

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue V May 2025- Available at www.ijraset.com

Machine Learning-Based Cyber security in Advanced Autonomous and Connected Vehicles

Nikita Hatwar[1], Tejal Borkar[2], Prashik Lamsoge[3], Vedant Kapgate[4], Anurag Yamnurwar[5], Ashay Wanjari[6]
Information Technology Department PCE Nagpur, India

Abstract: ***The rapid evolution of Advanced Autonomous and Connected Vehicles (AACVs) has redefinedthe future intelligenttransportation,bringingforthsignificantbenefitsintermsofsafety,efficiency,anduserconvenience.However,thisincreasedinterconnectivityhasalsointroducedawiderangeofcybersecuritychallenges.AACVsdependheavilyoncomplexarchitecturesinvolvingElectronic Control Units (ECUs), onboard sensors, and communication protocols such as Vehicle-to-Vehicle (V2V), Vehicle-to-Infrastructure (V2I), and Vehicle-to-Grid (V2G) networks. These components make the system vulnerable to numerous cyberattacks, including GPS spoofing, Replay Attacks, Man-in-the- Middle (MITM) Attacks, Denial-of-Service (DoS) attacks, and unauthorized remote access via Software Defined Radio (SDR) devices like HackRF One.***

Inthisstudy,wepresentarobustmachinelearning(ML)-drivencybersecurityframeworkspecifically designed to safeguard AACVs against these sophisticated threats. Our approach integrates a multi- layered Intrusion Detection System (IDS) combining rule-based filtering with real-time anomaly detection using decision trees, ensemble methods, and Generative Adversarial Networks (GANs). To address data privacy concerns, we employ federated learning techniques that facilitate decentralized modeltrainingwithoutexposingsensitivevehiculardata.

Further,oursystemarchitectureincorporatessecurediagnostics,biometricauthenticationprotocols,and advanced encryption mechanisms to defend against zero-day vulnerabilities and internal threats. Experimentalsimulationsconductedonsynthetic CANbustrafficdemonstratetheproposedmodel'sabilitytodetectandrespondtothreatswithhighaccuracyandlowlatency.

Byleveragingartificialintelligence,thisresearchaimstoestablishanadaptive,scalable,andresilientcybersecurityframeworkthatevolveswithemergingthreats.Ourfindingsunderlinethecriticalroleof ML in enhancing vehicular cybersecurity and serve as a foundation for future innovations in safe, intelligent transportation systems.

Keywords: ***AutonomousVehicles,IntrusionDetection,SoftwareDefinedRadio,GenerativeAdversarial Networks, Machine Learning, GPS Spoofing, Cybersecurity, CAN Bus, Smart Key Attacks, LiDAR Disruption***

I. INTRODUCTION

TherapiddevelopmentofMachineLearning(ML)andInformationandCommunication Technology (ICT) has played a pivotal role in shaping the landscape of Connected Autonomous Vehicles (CAVs). These technological advancements have led to significant improvements in driving efficiency, road safety, and user convenience. However, they have simultaneously introduced critical cybersecurity challenges that threaten vehicle security. Traditional safety mechanisms, such as mechanicallocks,basicencryption,andisolatedsystemdesigns,arenowinadequateinaddressingthe complexities of modern cyber threats. The growing dependence on wireless communication and autonomous functionalities has made these vehicles highly vulnerable to sophisticated cyberattacks, prompting the need for advanced protective measures.

Historically, vehicle security has primarily focused on preventing physical theft and unauthorized access. With the digital transformation of automotive systems, the scope of threats has expanded to include cyber intrusions such as Replay Attacks, Man-in-the-Middle (MITM) Attacks, and Sybil Attacks. These threats exploit flaws in authentication protocols and communication frameworks, enabling attackers to remotely manipulate vehicle operations. Research shows that devices like HackRF One, a Software Defined Radio (SDR), can be used to intercept and replay smart keysignals, thereby bypassing traditional security measures.

Furthermore, the integration ofwireless standards such as Wi-Fi, RF, and Bluetooth has broadened the attack surface. Cybercriminals can target these channels to remotely disrupt vehicle functions, potentially endangering passengers. Sensor systems including LiDAR, radar, and onboard cameras— crucial for autonomous navigation—are also susceptible to adversarial interference. Laser-based attacks, for example, can distort sensor readings, leading to inaccurate object detection and unsafe vehicle behavior. These threats highlight the urgent need for resilient security systems to safeguard sensor data integrity.

Another major concern involves GPS spoofing and jamming. Since CAVs heavily rely on GPS for navigation and localization, attackers can manipulate positional data, causing the vehicle to deviate from its intended route or lose navigation capabilities altogether. Such attacks are especially dangerousinreal-timetrafficenvironments, whereaccurate positioningisvitalforcollisionavoidance and route planning.

Addressing these challenges calls for the implementation of cutting-edge security mechanisms. These include modern encryption standards, intrusion detection systems (IDS), and even blockchain-based authentication methods. Additionally, AI-powered anomaly detection can play a crucial role in identifying and mitigating cyber threats in real-time. Collaborative efforts involving automotive engineers, cybersecurity experts, and regulatory authorities are essential to developing robust frameworks that can withstand evolving threats. By taking proactive measures, the industry can ensure the safe and secure deployment ofautonomous vehicles in the coming future.

Additionally, artificial intelligence-driven anomaly detection mechanisms can help identify and mitigate potential cyber threats in real time. Collaborative efforts between automotive manufacturers, cybersecurity researchers, and regulatory bodies are essential to developing robust security frameworks that safeguard autonomous vehicles against evolving cyber risks. By addressing these security challenges proactively, the automotive industry can ensure the safe and reliable deployment of autonomous vehicles in the future.

II. LITERATURE SURVEY

The growing reliance on Machine Learning (ML) and Information and Communication Technology (ICT) in autonomous vehicles has exposed them to increasing cybersecurity risks. Multiple studies have documented various vulnerabilities, such as weaknesses in authentication systems, particularly exploited through Replay Attacks where intercepted signals are retransmitted to gain unauthorized access.Networksecurityassessmentshaverevealedthatcommunicationprotocolslike Wi-Fi,RF,and Bluetooth are prone to breaches, making vehicles vulnerable to remote hacking. Research involving Software Defined Radio (SDR) tools, such as HackRF One, demonstrated that smart key systems operating at 433.92 MHz could be exploited by replaying captured signals to unlock vehicles without authorization.Additionally,laser-basedinterferencewithcamerasensorshasshownthatboth LiDAR and image recognition systems can be manipulated, compromising the vehicle's autonomous navigation capability. These findings underscore the importance of stronger encryption techniques, biometric authentication, and signal verification to secure communication systems. Experiments conducted on vehicle sensors, wireless signals, and smart key transmissions have generated valuable insights to inform more robust cybersecurity solutions. This body ofwork emphasizes the urgentneed for advanced protocols to safeguard autonomous vehicles from cyber intrusions. [1]

DespitethetransformativeimpactofConnectedAutonomousVehicles(CAVs)ontransportation,they remain highly exposed to cyber threats. Research has highlighted significant weaknesses across various sensor systems—LiDAR, radar, cameras, ultrasonic sensors, and GPS—all of which can be compromised through spoofing or jamming. Vehicle communication systems are also vulnerable to Man-in-the-Middle (MITM) and replay attacks, while Sybil attacks illustrate the dangers offraudulent vehicle identities influencing shared traffic data. Further investigations into sensor fusion and malware penetration have revealed weaknesses in infotainment systems and automated decision-makingprocesses.Forensicanalysismethods,suchasdataextractionfromblackboxesandElectronic Control Units (ECUs), have been recommended for tracing attacks and reconstructing incidents. Artificial Intelligence (AI)-based security mechanisms have shown to be more effective than traditional rule-based approaches in threat detection and mitigation. Moreover, both anomaly detection systems and intrusion detection systems (IDS) have proven to significantly improve cybersecurity measures, decreasing the likelihood of successful attacks. These insights reinforce the critical need for robust encryption, intelligent monitoring tools, and effective forensic techniques to ensure the operational safety of CAVs. [2]

Securing AI-powered autonomous vehicles remains a crucial concern as research continues to highlight their vulnerability to cyberattacks. Software-based assessments have revealed that cybercriminals can exploit Wi-Fi-enabled systems to carry out Denial-of-Service (DoS) attacks and gain unauthorized control. Simulations focused on sensor-based hacking have demonstrated that adversaries can manipulate GPS data or disrupt LiDAR signals, causing misinterpretations in vehicle perception.

Penetration tests on AI-driven decision-making systems have further exposed the susceptibility of these technologies to adversarial inputs that mislead image recognition algorithms and compromise navigation. To combat these risks, researchers propose encrypted communication protocols and electromagnetic shielding techniques, including RF-blocking pouches for smart key protection. AI- basedcybersecuritysystems,especiallythoseusingmachinelearningforreal-timeintrusiondetection, have shown great promise in identifying and responding to attacks. This research highlights the importance of enhanced encryption standards, AI-powered threat monitoring, and multi-layered defense strategies to support the secure operation of autonomous vehicles. [3]

CybersecurityinConnectedAutonomousVehicles(CAVs)continuestobeagrowingchallengedueto the vulnerability of their integrated components. Key sensing technologies—cameras, ultrasonic sensors, LiDAR, and GPS receivers—are all exposed to various threats like spoofing, signal interference, and jamming. Countermeasures such as redundancy, machine learning, and multi-sensor fusion are being explored to address these risks. Likewise, long-range communication technologies, particularly LTE-based V2X systems, are vulnerable to spoofing attacks, malware injection, and privacy breaches, often executed through radio frequency (RF) jamming. Vehicle-to- vehicle (V2V) communication faces specific threats targeting data integrity, authentication, and confidentiality. Although traditional cryptographic and IDS methods are effective against external threats, they often fall short in addressing internal security breaches. To counter these limitations, researchers are examining trust-based models including fuzzy logic, game theory, blockchain, and edge-computing frameworks. While these methods have improved certain aspects of cybersecurity, challenges still persist—particularly in areas such as data privacy, AI integration, blockchain scalability, and system efficiency under high traffic loads. This body of research emphasizes the importance of cloud- and edge-computing models in building resilient cybersecurity infrastructures for CAVs, ensuring both safety and performance. [4]

Aselectricvehicles(EVs)becomemoreintelligentandinterconnected,ensuringtheircybersecurity has become a priority. Core components like batteries, powertrains, electronic controllers, and charging systems are increasingly targeted by malicious entities. Threats include firmware manipulation, unauthorized access to ECUs and telematics, and attacks on public and privatecharging infrastructure. Additional risks stem from supply chain vulnerabilities, where compromised hardware or software can introduce systemic flaws. The communication frameworks within EVs— such as V2V, V2I, and V2G—further expand the attack surface, increasing the need for comprehensive protection. Common threats involve battery mismanagement, software exploitation, and remote access breaches, each posing a risk to both vehicle functionality and passenger safety. In response, researchers recommend robust encryption practices, layered IDS systems, and network security enhancements. Maintaining cybersecurity in EVs also calls for secure Over-the-Air (OTA) updates and continuous industry collaboration. By integrating risk management strategies and promoting awareness, the future of connected electric mobility can be made both safer and more sustainable. [5]

Concernsregardingthecybersecurityof in-vehiclenetworkscontinuetoriseasmultipleaccesspoints remain exploitable. Entry vectors such as OBD-II ports, USB interfaces, keyless entry systems, LiDAR, and CAN bus networks present serious security vulnerabilities. These can be exploited through a range ofattacks including DoS, spoofing, data injection, and replay attacks. One ofthe most significant concerns lies with the Controller Area Network (CAN) bus system, which, due to its lack of encryption and message authentication, is vulnerable to masquerading, eavesdropping, and bus-off attacks.Toaddresstheseissues,researchershaveproposedmachinelearning-basedIDSusing Deep Neural Networks (DNN), Long Short-Term Memory (LSTM), and time-interval analysis to achieve accurate, real-time threat detection.

Complementary cryptographic solutions—such as lightweight CAN authentication,Message Authentication Codes (MAC), and stream cipher techniques—enhance security by mitigating tampering and replay attempts. Comparative studies demonstrate that combining ML with cryptographic defenses leads to better threat detection, system scalability, and secure communication. Datasets derived from real-world CAN traffic, simulated attacks, and live sensor data have been instrumental in training these models. Future work should focus on integrating these technologies further to fortify vehicle cybersecurity against evolving threats. [6]

III. MODELLINGAND ANALYSIS

The modeling and analysis section of this study is developed to simulate, detect, and evaluate cybersecurity threats in Advanced Autonomous and Connected Vehicles (AACVs) using real-time vehicular communication data. The proposed framework is fully implemented within a cross- platform environment utilizing Windows Subsystem for Linux (WSL) on Ubuntu, allowing seamless integration ofLinux-native and Python-based machine learning libraries.

The modular designensures that the system can support both virtual simulation setups and future deployment on physical hardware platforms.

A. VehicularCommunicationSimulationwithpython-can

To accurately emulate intra-vehicle communication, this study employs the python-can library to generate and simulate Controller Area Network (CAN) traffic. This setup creates virtual CAN messages that represent standard vehicle operations such as braking, steering, and sensor data exchange. To evaluate the framework's robustness against cyber threats, simulated attack scenarios— such as Replay Attacks, Denial-of-Service (DoS), and ID spoofing—are introduced into the communication stream using script-controlled message floods and tampered payloads. All message transactions are recorded in log files, which are subsequently used for analytical processing and training of machine learning models.

B. DeepLearningImplementationwithTensorFlow

Tomodelthecomplextemporalbehaviorof CAN-basedvehicularcommunication,deeplearning techniques are implemented using TensorFlow. The primary components ofthe architecture include:

- LSTMNetworks,whichareutilizedtocapturesequentialpatternsanddependenciesinCAN traffic over time.
- Autoencoders, applied for unsupervised anomaly detection by learning compact representations of normal communication patterns.
- Convolutional Layers, used for identifying spatial features in reshaped binary streams extracted from payload data.

TensorFlow's GPU-accelerated computation is enabled via the CUDA-compatible backend available throughWSL,whichoptimizestrainingperformance.Hyperparametertuningisconductedusing grid search techniques and early stopping criteria based on validation loss to ensure optimal model accuracy and efficiency.

C. DataHandlingandFeatureEngineeringwithpandasandNumPy

Raw CAN traffic logs are preprocessed and structured using the pandas library, enabling fast extraction of metadata such as timestamps, message identifiers (IDs), and Data Length Codes (DLCs). The NumPy library is used to compute a set of high-dimensional numerical features necessaryforrobustanomalydetection.Thekeytransformationsinvolvedare:

- MessageFrequencyVectors:Thesemeasurethenumberofmessagestransmittedper IDover defined time intervals.
- Inter-messageTiming:Thiscalculatesthetimedifferencebetweenrepeatedoccurrencesofthe same message ID.
- Payload Entropy: Entropy metrics are used to quantify variability within data fields, helping to identify spoofed or abnormal sensor readings.
- Bit-LevelPatternRecognition:Payloadsareconvertedintobinaryformattofacilitatethedetection of injected faults and irregular bit patterns.

Thisfeatureengineeringpipelinetransformsunstructured CANbusdataintostandardized,numericaltensorssuitableformachinelearning-basedthreatdetection.

D. RationaleforUsingWSLwithUbuntu

Windows Subsystem for Linux (WSL) offers a lightweight, virtualized Linux environment that enables researchers to run native Linux tools directly within a Windows system. This setup allows users to:

- Execute specialized Linux-based tools like python-can, tcpdump, can-utils, and iproute2 without dual-booting or using virtual machines.
- AccessandmanipulatebothLinuxandWindowsfilesystemsconcurrently,simplifyingcode sharing, log management, and debugging processes.
- Maintain a unified development environment for Python, TensorFlow, and CAN bus simulationtools, promoting consistency and ease of replication across different systems.

UbunturunningunderWSLprovidesastable,flexibleplatformforscripting,automation,andendtoendtestingofintrusiondetectionmechanismsanddataprocessingworkflows.

IV. CONCLUSION

The integration ofMachine Learning (ML) and Information and Communication Technology (ICT) in Connected Autonomous Vehicles (CAVs) has significantly revolutionized the transportation industry by enhancing operational efficiency, improving safety, and offering user-friendly solutions. However, these technological advancements have also brought forth critical cybersecurity challenges, leaving autonomous vehicles increasingly vulnerable to cyberattacks such as unauthorized access, signalspoofing,sensormanipulation,andremotehacking.Thisstudyunderscorestheurgentneed for robust and intelligent security frameworks to mitigate such threats.

Through comprehensive analysis, this research has examined multiple vulnerabilities within CAV systems, including weaknesses in authentication mechanisms, exploitation of smart key systems, security gaps in wireless communications, and GPS spoofing attacks. It has also highlighted the risks associated with the compromise of sensor-based perception systems, emphasizing the importance of securing LiDAR, radar, and camera inputs against adversarial manipulation. Addressing these risks, the study aims to propose advanced cybersecurity models that ensure reliable and safe functioning of autonomous vehicles.

The contributions of this work include the development of ML-powered intrusion detection systems (IDS), the application of encryption techniques, the exploration of blockchain-based authentication, and the implementation of anomaly detection using AI models. These mechanisms enable real-time threat monitoring and proactive defense against potential intrusions in vehicular networks. The deployment of intelligent security layers allows CAVs to dynamically identify, assess, and neutralize attacks, reducing the likelihood of system failure or accidents caused by cyber threats.

Lookingahead,thefindingspresentedinthispaperprovideafoundationforfutureresearchfocusedonadaptiveAIbasedsecuritysolutions,quantumresistantencryptionprotocols,andblockchainintegratedidentityverification.Furthermore,advancinghybridlocalizationtechniquesthatcombine GPS with alternative systems may reduce vulnerability to spoofing and jamming. Collaborationamongautomotivemanufacturers,cybersecurityspecialists,andpolicymakerswillbeessentialtoestablishgloballyacceptedsecuritystandardsforautonomousvehicles.

In summary, this research supports the long-term vision of secure, dependable, and scalable autonomous mobility. By advancing intelligent cybersecurity frameworks and integrating real-time AI-based threat detection, the industry can ensure the responsible deployment ofautonomoussystems while building public trust in smart transportation technologies. The continued evolution of defense mechanisms, coupled with proactive regulatory involvement, will be crucial in protecting future mobility ecosystems from emerging cyber risks.

V. ACKNOWLEDGEMENTS

We would like to express our deepest and most sincere gratitude to Dr. Mrs. Nikita R. Hatwar, Assistant Professor, Department of Information Technology, for her constant encouragement, expert guidance, and invaluable mentorship throughout the duration of this project. Her profoundknowledge, insightful suggestions, and constructive feedback played a pivotal role in shaping our understanding of the subject and ensuring the successful execution of this research. Her availability and patience, even during challenging phases of the project, were instrumental in helping us stay on track and motivated.

Our heartfelt thanks also go to Prof. Mrs. Mrudula M. Gudadhe, Project Coordinator, for providingus with the opportunity to undertake this research project and for her consistent support and encouragement throughout its various stages. Her faith in our capabilities and her timely advice ensured that we had access to the necessary resources and direction to explore innovative ideas and stay committed to our objectives.

We are profoundly grateful to our parents for their unwavering support, both emotionally and financially, which has been the backbone of our academic journey. Their constant reassurance, patience, and belief in our potential gave us the strength to persevere, even during difficult times. Without their support, this achievement would not have been possible.

Special thanks are due to our teammates for their dedication, enthusiasm, and exceptional teamwork. The collaborative spirit, mutual respect, and determination shared among us greatly contributed tothe completion of this project. Each member's unique strengths, ideas, and efforts were essential in overcoming obstacles and achieving our collective goals.

Lastly, we are grateful to the academic community and all the researchers whose work we have referred to during the course of this study. Their contributions have inspired and informed our own efforts. This project has been a truly enriching and transformative experience, and we hope it adds value to the field and serves as a stepping stone for future research in vehicle cybersecurity and intelligent systems.

REFERENCES

[1] S. I. Jung and S. D. Ho, "A Study on Hacking Attacks and Vulnerabilities in Self-Driving Cars with Artificial Intelligence," in Proceedings of the PAUL Math School Conference, Goesan-gun, Chungcheongbuk-do, Republic of Korea, 2023.

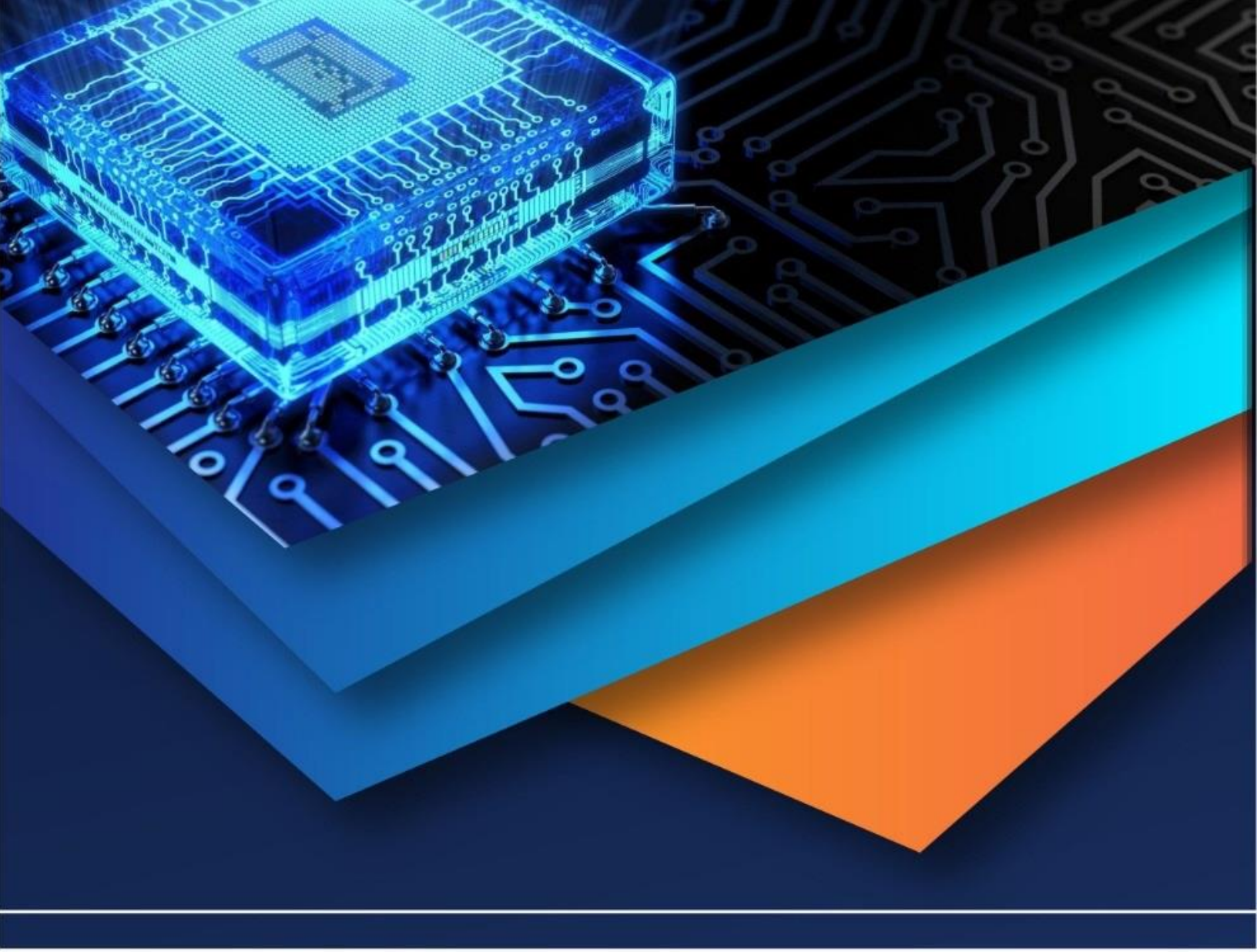
[2] I. Durlik, T. Miller, A. Łobodzińska, E. Kostecka, and Z. Zwierzewicz,"Cybersecurity in Autonomous Vehicles—Are We Ready for the Challenge?" Maritime University of Szczecin, Szczecin, Poland, 2023.

[3] P. Sharma and J. Gillanders, "Cybersecurity and Forensics in Connected Autonomous Vehicles: A Review of the State-of-the-Art," University at Albany – State University of New York, Albany, NY, USA, 2023.

[4] M. D. Mwanje, O. Kaiwartya, M. Aljaidi, Y. Cao, S. Kumar, D. N. Jha, A. Naser, and J. Lloret, "Cybersecurity Analysis of Connected Vehicles," Nottingham Trent University, Nottingham, UK.

[5] P. S. Devanandanan and R. B. Rengarajan,"Cybersecurity in an Electric Vehicle: A Comprehensive Review Paper," International Research Journal of Modernization in Engineering, Technology and Science. DOI: 10.56726/IRJMETS56581.

[6] R. S. Rathore, C. Hewage, O. Kaiwartya, and J. Lloret,"In-Vehicle Communication Cybersecurity: Challenges and Solutions," Sensors, vol. 22, no. 16, p. 6679, Sep. 2022. DOI: 10.3390/s22176679.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY