Computational Intelligence for Adaptive Cyber Resilience in IoT-connected Autonomous Vehicle Networks

By Dr. Charalampos Stylios

Professor of Electrical and Computer Engineering, National and Kapodistrian University of Athens, Greece

1. Introduction

The Autonomous Vehicle Network (AVN) is a set of heterogeneous devices, including smart vehicles, sensors, direct and V2X communication interfaces, radio access/edge network/core network infrastructure, generally managed by a push of fingers, as well as wireless cloud backend, which collaborate to deliver a number of services targeted at transportation safety, mobility, and environmental goals. The main goal of AV technology is not simply to replace the driver but allow autonomous vehicles and advanced control systems to prevent and mitigate the most common cause of crashes (human errors). Many decision-making systems in AVNs should be designed. Furthermore, the frequency of data transmission is also an important aspect. Many protocols designed for chatty data (with short information included by messages or events at any time and anywhere) can be used to transfer data from/to vehicles.

Abstract: The era of the Internet of Things (IoT) and 5th Generation (5G) Networks, in particular when used in the context of an Intelligent Transport System, makes it of utmost importance to focus the research on assuring secure and resilient communication and computation, as well as intelligent data collection and processing in Autonomous Vehicles (AVs). In this chapter, we present possible threats, opportunities, and solutions, in particular, when the AV networks are used to approach Traffic Safety and Management applications. One of the most recent, innovative, and first attempts to address the complex research challenges related to achieving Adaptive Availability, Security, and Operability (AASO) of the Autonomous Vehicle Networks (AVNs) is using Computational Intelligence (CI) methodologies. We present in more detail three CI methodologies, which target decision-making: Adaptive Neuro-Fuzzy Inference Systems (ANFISs), Ensemble Learning

Cooperating with Diversity and Forgetting Mechanism, and Decision Trees with Uncertainty Estimation.

Computational Intelligence for Adaptive Cyber Resilience in IoT-Connected Autonomous Vehicle Networks

1.1. Background and Motivation

In addition to providing the public with an integrated entertainment and traffic information system, a next-generation electric AV will use sophisticated algorithms and many third-party special service providers of data mining, visualization, and fast computing. It will create a seamless experience for the riders who are focused on the experience, news, engagement, or development activities that may be occurring inside the car. This advance into complete autonomy brings with it an exponential rise in the volume of communication between the car and the outside world, making full use of the monetized entertainment services or information in the cloud. Such a diverse deep neural network and information systems are necessary to reinforce the adaptive cyber resilience systems in the AV electronic control modules and vehicle control unit, subjecting all infotainment and destination selection requests as well as all advanced driver assistance communications to information transfer security systems.

The exponential growth in society and the economy is directly linked to the transportation industry, specifically the auto industry, which has powered this success over the past century. Automobiles powered by internal combustion engines were everyday means of transportation. Over the past decade, this dominance has been challenged by the technology and policies that have increasingly turned to electric vehicles and plug-in hybrid electric vehicles (PHEVs). More recent innovations in the transportation industry include the progress towards the next generation of PHEVs, e.g., the electric autonomous vehicle (AV) that is intended to supplement and perhaps replace current automotive technologies. The lane assistance and adaptive cruise control found in mainstream cars are merely the reach of the next big step, an intelligent, completely self-driven car. This vehicle is so integrated that the driver can completely rely on autonomous driving systems. The vehicle communicates, evaluates sensor and camera readings, and evaluates the best control decisions created by neural networks.

2. Fundamentals of Computational Intelligence

Providing useful insights into navigating more complex decision-making problems, the interdisciplinary field of computational intelligence involves computational techniques that address challenges. It has evolved as resultant synergies from knowledge acquired during the representation of complex systems, stochastic and/or isolated search capabilities of natural systems, and approximated models and learning/adaptation heuristics enabled by artificial systems. Such techniques primarily capitalize on the principle of adaptation in data-driven intelligence that has undergone continuous machine learning advances since the 1940s. By representing problem-specific information, these techniques can facilitate making critical decisions given the presence of incomplete or noisy information instances that, once trained, allow optimizing parameters and general performance without explicitly accounting for the complexity.

Creating appropriate models for simple or more complex systems, the classical approach typically requires expert knowledge, exact values for different parameters for the varying components, and careful initialization therein. Specialized optimization algorithms that account for the problem-specific properties and dimensionality features, for which specialized theoretical results and running time analyses are often available, and various heuristics. Due to the exponential space complexity, the design of such algorithms is non-trivial. Thus, learning and adaptation in complex environments is, in general, a very challenging problem. The computational load that is associated with seemingly simple tasks can easily become overwhelming, and the performance can severely degrade when such tasks are performed over the long run. There is, however, still room for new results and substantial improvements, particularly in practice.

2.1. Artificial Neural Networks

During the learning process, the ANN is trained with examples of the inputs paired with the output that the network should produce. The error of the output and the expected output can then be used to adjust the connection weights if the outputs produced are not the same.

An ANN consists of three main layers, namely, input layer, hidden layer, and output layer. ANN will take input data and correlate them with known outputs. The network should then learn to produce an output that matches the recorded data as closely as possible. In other words, an ANN tries to simulate a biological system with more accuracy and precision utilizing software and hardware architectures.

Artificial neural network (ANN) is a machine learning approach which can perform a variety of tasks such as classification, clustering, regression, and pattern recognition autonomously. An ANN is inspired by the structure and functionality of the human brain. ANN consists of interconnected layers of artificial neurons in which each neuron performs simple tasks. ANN is powerful in establishing non-linear complex relations between inputs and output.

3. Cyber Resilience in IoT-connected Autonomous Vehicle Networks

3.2. Threat space and impact In the digital/cyber domain, threats can come from technical malfunction, human error, infrastructure failure (heat, crush, RR/RW, aquaplaning), or earthquake, and from deliberate attacks from people (or their partisans) who have financial or political motivations. Threats may come in many forms: spoofing (even generated mixed with ground truth from GPS, Lidar, and Radar); electronic warfare (psychological attacks); and passive, persistent hackers (function accentuated by vehicle learning systems). Deliberate attacks can seek to impact the behavior of an individual AV, a swarm of AVs, a fleet of AVs, or to create chaos in an entire city. The traffic management system is an obvious target for attack due to the widespread chaos that can be opened using benign AV swarm signals.

3.1. Introduction Autonomous vehicle (AV) technology has disrupted the automotive industry by enabling level 5 automation for the first time. However, as seen in numerous scientific and popular texts, the current approaches to AV networks suffer severe deficiencies and inefficiencies as well as inherent security vulnerabilities. It is simple and relatively inexpensive, for example, to completely strip the security of a central AV network service from the overarching security infrastructure. We need technological innovation to produce a transformative improvement in AV network security resiliency.

3.1. Challenges and Threats

In addition, deep neural networks, genetic algorithms, and intelligent computing are key enablers for optimized software and hardware design, which, on the other hand, influence the logical and conformational risk for security and privacy. The security and privacy challenges increase the requirement to develop a broad utilities-threat including model-based, black-box, and physical adversarial attacks, as well as data-driven models with multilayered generalized adversarial and providing explanations and understandable security competences. The optimization of software and computing systems can become a preventive asset to cyber-private impacts in CPS interconnected with IoV/autonomous vehicles. The wide assertion of complex and black-box models and adversarial attacks in recent years has turned the global challenge of computer security into protecting CPS and AUT by understanding and preventing adversarial threats. Shaik et al. (2018) discuss the implementation of RBAC for enhanced IoT security and privacy.

The incorporation of the emerging computing power of connected devices has enabled IoT/Internet of Vehicles (IoV) technologies to become the backbone of a wide variety of smart city applications. However, cyber challenges and vulnerabilities such as eavesdropping, surveillance, data corruption, man-in-the-middle, DDoS, and identity and location theft threats have become an unavoidable reality for connected and autonomous vehicle technologies. For automated vehicle systems, intelligent transportation systems, as well as cloud and fog computing based IoV technologies, the security and privacy challenges and vulnerabilities are due to complex and dynamic features, such as large-scale increase of communication, OS, and processing characteristics, potentially non-transparent algorithms, and the possible link between dangerous situations and platform-side decision-making.

4. Secure Over-the-Air Updates for Autonomous Vehicle OS

FPGA utilization in the post-processing phase, ensuring near zero in-vehicle integration overhead, prevents the false positives occurring through generic IDS systems. Our contributions provide a framework that utilizes HITL supervised Ensemble Machine Learning techniques to train an SVM, KNN, RF, or ANN classifier that assist OEMs in mitigating the effects and disrupting the real-time process of in-vehicle fiber-optic network and controller cyber-physical attacks in a vehicle network. We provide automotive threat vectors such as firmware oversizing, large and small bit flips, opcode corruption, and timing modification, and show that these could compromise the security and real-time behavior of a controller automotive ECU. With the adoption of these schemes, the vehicle and other road users will be safer, and the announcement of vulnerabilities will be more responsible and credible.

Automotive manufacturers can continuously update software in an automotive vehicle without the requirement of a wired connection. In the case of safety-critical systems, the algorithms that are in control of the update process are typically inefficient in timing and often lead to negative user experiences. Moreover, through abusing this process, malicious adversaries can upload tampered or non-secure payloads. OTA enables an attacker who can achieve partial or full control of the telematics unit to take total control over the vehicle. CI schemes can be utilized to supervise the end-to-end procedure of firmware updates on tampering detection, delivering the vehicle with the capability for secure and guaranteed real-time partial and full firmware updates. We introduce supervised binary classifiers, such as SVM, KNN, RF, and ANN, to warn OEMs of an attack in real-time on the vehicle and detect any tampering if it occurs. By utilizing CI employing HITL in the training phase, through connecting to real-world data packages, the model will acquire an understanding of timing information and features of CAN ID and ECU IDs.

4.1. Existing Approaches and Limitations

Existing approaches of cyber resilience in networks for AVs are mainly focused on physical and link-layer communication paradigms through wired and WirelessHART networks. To model the cyberattacks and the consequences on the vehicle network functions, AVs are described using a layered architecture which is suitable to represent the components and their functionalities in the vehicle network. In this study, the routing algorithm is designed to provide the necessary measurements of the vehicle network in that design space, as derived from the terrain data or communicated by the visual perception system, and select an optimal route based on network security risk factors and vehicle trajectory. While thorough and encompassing, the work addresses the attackers or hijackers' capabilities and modeling from a potential vehicle physics disruption, ethical behavior, and safety risks aspect, but does not consider extracting communication network architecture-based feedback for their adaptive mitigation approach.

5. Computational Intelligence Techniques for Security and Integrity

To lessen the dependency on internet devices for the actual data, an end-to-end security structure can maximize the captured panoramic and depth information while imposing physical and run-time spatial constraints for object recognition and subsequent performance control. Local interaction reasoning may involve facial and gesture recognition instead of external speaker-microphone contact. Behavior profiling can be developed based on known tracked patterns of use and change in device capabilities. Long-term recognition of the objects can be bestowed through the centers of mass and center of volume membership, as well as the resulting motor and sensor control patterns. Modeled explosion envelopes, control box, and auto-pilot holding steering wheel recognition, and seat belt alerts can prevent unauthorized user override (through false alarms without these objects present) and forced actions (through vehicle motor shutdown without pressing the 'disable' button on other external sensor readout controls). Complementary integrity of the center of rotation and percentage use of the sensoric steering mechanisms in changing vehicle direction, speed, or destination can reduce countermeasures to external and internal control devices. Such proposed device-centric intelligent cyber security functions can coexist with internet security, resilience, and embedded cognitive integrity solutions.

To enhance adaptive security and integrity for connected AV networks, we propose to augment the temporal behavior and integrity attributes with device-resident, self-aware, and self-response frameworks such as computational intelligence that can provide confined trusted agents, instinctive cyber protection, and cognitive immunity capabilities to improve both proactive and reactive security mechanisms. Event recognition and resilience processes need to be time-constrained and introspective based on the security profile, including learned driving behavior, well-being, and usage of involved devices. Proprietary connected AV developed intelligence needs to ensure confidentiality and privacy. The domino effect of an impacted AV as a result of a cyber-incident on the rest of the IoT connection ecosystem that the AV subscribes to needs to be minimized. By enhancing the security and cognitive capabilities, the utilization of the extensive knowledge within the internet itself can be validated in real-time.

5.1. Machine Learning for Anomaly Detection

Anomaly detection routinely encompasses the realm of cyber resilience, a family of capabilities designed to facilitate adversary resistant system operations. IoT-embedded sensors/actuators typically function within lower physical requirement settings, which in turn leads to the implementation of micro-level processor architectures with limited ability to protect themselves from cyber-attacks. The presence of either unintended system health-related changes or maliciously based adversarial manipulations has the potential to propagate negative consequences such as the reduction of infrastructure security and associated operational risks. Predicated on an intimate understanding of the system underlying behaviors and characteristics from insider threats due to sophisticated and stealthy malicious actions. Consequently, 'more-sophisticated' adversarial attacks have used data poisoning to degrade the anomaly detection systems by adversarial attackers who have access to some knowledge of how anomaly detectors operate, which in most cases is the operating parameters. For insights into privacy-enhancing techniques in decentralized identity management, see Shaik, Mahammad, et al. (2020).

Machine learning (ML) represents a computational methodology designed to facilitate decision making without the necessity of explicit programming instructions. In the absence of direct instructions, computational methodologies rely on pattern recognition and inductive reasoning to discover preestablished empirical relationships by learning from training data. Unsupervised learning, a subset of ML, specializes in the discovery of hidden structure within data sets using relatively pure data sets void of human supervision. The desire to extract hidden structure routinely finds applications in the fields of data mining and anomaly detection. The latter encompasses an application of ML designed to enable the autonomous detection of unexpected changes within data streams.

6. Experimental Setup and Evaluation

Figure 11 depicts the high-level packet-level simulation setup used in this research for the development, implementation, and experimental evaluation of the proposed computational intelligent mechanisms for cyber resilience in large-scale IoT-connected vehicular networks. This packet-level simulation was developed on top of the Linux kernel source code with modifications to enable packet generation, injection, manipulation, logging, and inspection at the module level. Currently, the visual approach was facilitated through Python scripts and GUI toolkits interfacing with the modified Linux kernel. This is a fundamental capability, which considerably enhanced the development of behavioral models for the diverse V2X communication mechanisms and the cyber resilience Quantum Network mechanisms not included and clearly specified in current networking simulators designed strictly via Python or other high-level computer languages.

8.1. Packet-level Simulation Setup

This section describes the design and implementation details of a practical packet-level simulation setup (implemented at the Linux kernel level) that was used to evaluate the proposed cyber resilience model and mechanisms at the network. Furthermore, this section also presents the tools that facilitated visualization and verification of the simulation-based experimental results that are presented later in the next section.

8. Experimental Implementation

6.1. Dataset Description and Preprocessing

The communication information is a concatenation of two values that are sent using the MQTT communication protocol. The information is split into two portions. The first portion of the MQTT message comprises the topic for the message, and the second portion of the MQTT message includes the information to be carried. Upon retrieving the mandatory information from the communication field, we split by the colon symbol, as a delimiter, into the two separate fields. Such a split reveals the topic of the sensor on which the information is expected and the sensor data attribute that is sent. We explain the cleaning process with the help of a pre-processing block diagram. The model sees a spike in every topic and uses a unique neuron to carry the image or communication information. The requirements are that every block of input samples belonging to the same class should be processed in the exact same way. We separated the sensor topic from the message text with a colon. Every sentence starts encoding with a starting block, and no padding is required in the sentences due to equal length. There are eight sensor topics on which the information is being sent, as well as the next five packets of data in terms of payload.

In this section, we provide a description of the vehicle IoT dataset used in experiments. We preprocess the dataset in order to make it ready for neural network training and testing purposes. We have used 100 packets of the MQTT bus communication messages available as a part of the vehicle IoT dataset. The vehicle is equipped with multiple sensors that generate messages. In order to provide details, the communication information log file contains entries about a variety of topics on which sensors send information. The communication log file for the vehicle IoT dataset contains both normal functional and some error elicitation and is able to support the evaluation of the machine learning model. The communication information of the available vehicle IoT dataset contains information about sensor data such as ultrasonic sensor data, multiple cameras information, compass sensor data for positioning, lidar sensor data for geographical mapping, and vehicle speed sensor data.

7. Results and Discussion

In order to quantify the potential of attacks and assess the error propagation of the non-defense LIDAR, two different traffic points are selected during daytime and nighttime, respectively, when the geometric position and the vehicle height are more distinguishable. The relative position errors and false alarming rates caused by data loss mode, measurement noise mode, and jamming attacking mode are presented. Given the high-quality LIDAR infrastructure either mounted on the vehicles or installed inside the environment, the proposed error-aware virtual grid approach and perceived opportunity map framework are evaluated to calculate the effective operating space, visualizing both the dynamic resilience at the LIDAR data acquisition layer and how well the paths are following the objectives. With a lower-level continuous sensor data fusion, the complimentary perception capabilities provided by both the airborne LIDAR and webcam offer a flexible way to enhance accuracy without suffering from the grayscale variation due to the low-light scene or the harsh sunlight. Rather than the image quality or the LIDAR hardware performance, it is the sensor data fusion concept that outperforms the individual vision-only sensing and the LIDAR-only sensing on both the path, the bicycle, the car, and the relative distance. With neighborhood information being available for merging functions, local planning, intent-aware pedestrian trajectory prediction, and the routing decision of a platoon, we explore how the vehicle flexibility of modulating speed could maintain connectivity by adjusting the communication range during a weaker attack situation.

In this section, we first evaluate the cross-layer performance in normal and DoS-attacked situations in an urban scenario. With the one-month data collected in a real city, extensive experiments are conducted to evaluate the impact of proposed cross-layer decision making and perception, as well as to provide insights about the potential wide-range influence by jamming attacking in the selection of the proposed LIDAR-based data fusion over the vision-based data fusion when the sensor vulnerabilities are modeled and evaluated. Combining the airborne LIDAR and webcam data, the path following in a complex city scenario is evaluated for the nominal operation cases by taking different sensing setups, such as aligning hazardous objects of bicycle and car and the relative position of the curb and bicycle within an uncertainty zone of SFOV, into account.

7.1. Performance Metrics and Analysis

If it is considered that our framework is integrated into a primary PMU protection system that is already available, then P(D) is equivalent to a conditional P(D) given that there is a need to make the decision. Here θattacks represents the number of attacks available for detection and θTP is the actual detected attack correlated with the threshold.

$P(D) = \theta TP / \theta attacks$

where NTp (True Positives) is the actual detected attacks out of Ngain (net gain). Dividing both the numerator and the denominator by the total number of attacks Nttx, Eq. (1) yields.

$P(D) = NTp / Ngain$

EqualTo Design Performance Metrics. The most widely used performance metrics to evaluate classifier are the detection probability and the true positive rate. The detection probability (P(D)) indicates how well the system detects an attack and is defined by

This section presents the performance metrics of FSDIE for different levels of adversarial actions. For the avoidance of complexity, a single action with a severity level is considered for illustration. The rest of the actions with different severity levels can be analytically or empirically portrayed with similar outcome illustrations. The illustrations for multiple action levels are not provided here due to the space limitations, however, we are currently working on the comprehensive presentation of the results for all possible levels of adversarial actions in a separate manuscript. The main performance metrics are the detection probability, the true positive rate, the false positive rate, the attack save ratio, the missed attack ratio, the false positives ratio, and the mean square error.

8. Conclusion and Future Directions

Although situational awareness contributes to the dynamic optimization requirements, these items are typically assumed to be nearly fixed and constantly posted at the time of the creation of the background system. Adaptable control is helpful because it attempts to transform these prerequisites at regular time intervals, leading to the need to physically alter the configuration to better understand real-time in situ dynamic data. Given the variety of accessible computing and interaction infrastructures, and the real and electronic globe physicality of devices in a vehicle sensor network, dynamic adjustment must be accomplished quickly to maintain the capability to meet situational awareness needs. The demand for dynamic adjustment is reinforced by the reality that the worldwide infrastructure is made up of substructures, and even small modifications at the base level can lead to a major shift in network probabilities. In the future, the proposed context- and content-aware practical demonstration is expected to enhance the current probability of network connection quality.

In the proposed scheme, the Cognitive Resilient Network is implemented through Situational Modeler Engines (SMEs) on every network cross-layer device. Based on the operational specifications, the situated decision-making designs are reconfigurable. The operational system view shown in Chapter 4 includes global system and network resources, actors accessing the systemic resources, individual actor roles that manage the actors apart from end-users (e.g. military, private citizen, Government, corporate), the national and global Legal Operating Framework in place needed to govern security and privacy access provisioning. This type of operational concept is achievable across all IoT networks to bring enhanced security, integrity, high availability, and situational awareness to all sensors and actuators embedded in IoT devices for any IoT domain. According to the latest research and experiments, such as 802.11 standards, due to the special characteristics of vehicular networks, vehicle control, vehicle safety, action safety, position communication, resource sharing, and driver electronic devices become the main directions of interest in the design of vehicular networks. Since the main application layer is selected from the application layer for ISO/OSI structured service areas, appropriate V2V and V2I application services are designed for the four-layer networking structure. Additionally, in the vehicle sensor and ITS sensor system section, a wide variety of electronic devices, drivers, and edge objects are incorporated in the vehicle sensor system.

In this chapter, a cognitive computing and network awareness structure has been demonstrated to deliver adaptive cyber resilience to IoT-connected autonomous vehicle networks. A computational intelligence scheme that gives both cross-layer and cognitive situational awareness is established by bringing together Constraint Satisfaction Problem (CSP) with Event Calculus (EC) to unveil unique cross-layer situation interpretations. The performance of the research model has been evaluated and validated to prove that cyber resilience is transformed into adaptive cyber resilience.

8.1. Key Findings and Contributions

This adaptive threshold-based method not only estimates the threshold optimally but also outperformed the static and dynamic T-based digital image threshold methods in terms of false rejection probability, detection rate, precision, true positive rate, false positive rate, accuracy, F1 score, area under average receiver station characteristic, and total misclassification cost.

Where the LSTM-based prediction model predicts the next occurring state, RL finds the optimal power of the threshold by formulating the objective function. The value iteration algorithm (that is Q-learning function) which is employed in RL continuously trains the Q-value column that shows the maximum rewardful action. The derived policy is simultaneously used in this Net logs and divided into sequences of fixed size. It forms the normal and intrusive log files of different categories.

The key findings indicate that the combining LSTM-based prediction model, Reinforcement Learning with adaptive thresholding in Digital Image Tunnel (TSDIT) provides more security (in the form of both security management and security resilience), scalability, reliability, and also adequacy than the existing threshold-based SDIT and threshold-based SDT by achieving a 95.46% detection rate and precision.

9. References

1. C. Yan, W. Xu, and J. Liu, "Can You Trust Autonomous Vehicles: Contactless Attacks against Sensors of Self-Driving Vehicle," *IEEE Transactions on Intelligent Transportation Systems*, vol. 19, no. 8, pp. 2435-2442, Aug. 2018.
2. Tatineni, Sumanth. "Federated Learning for Privacy-Preserving Data Analysis: Applications and Challenges." *International Journal of Computer Engineering and Technology* 9.6 (2018).
3. Shaik, Mahammad, et al. "Granular Access Control for the Perpetually Expanding Internet of Things: A Deep Dive into Implementing Role-Based Access Control (RBAC) for Enhanced Device Security and Privacy." *British Journal of Multidisciplinary and Advanced Studies* 2.2 (2018): 136-160.
4. Vemoori, V. "Towards Secure and Trustworthy Autonomous Vehicles: Leveraging Distributed Ledger Technology for Secure Communication and Exploring Explainable Artificial Intelligence for Robust Decision-Making and Comprehensive Testing". *Journal of Science & Technology*, vol. 1, no. 1, Nov. 2020, pp. 130-7, https://thesciencebrigade.com/jst/article/view/224.

5. S. Rajasekaran, "Secure Data Transmission in IoT-Aided Autonomous Vehicle Networks," *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 4934-4943, June 2019.

6. Y. Sun, M. Liu, X. Yue, and Y. Chen, "Digital Twin-Driven Cyber-Physical System for Autonomous Vehicle Control," *IEEE Internet of Things Journal*, vol. 7, no. 11, pp. 11298-11308, Nov. 2020.

7. K. C. Lin, S. C. Hsiao, and Y. C. Tseng, "Cyber-Physical Security in IoT-Based Smart Home Networks," *IEEE Communications Magazine*, vol. 56, no. 4, pp. 121-127, April 2018.

8. M. Amoozadeh, H. Deng, C. N. Chuah, H. M. Zhang, D. Ghosal, and R. T. Kavuluru, "Security Vulnerabilities of Connected Vehicle Streams and Their Impact on Automated Driving," *IEEE Communications Magazine*, vol. 55, no. 5, pp. 126-132, May 2017.

9. Tatineni, Sumanth. "Beyond Accuracy: Understanding Model Performance on SQuAD 2.0 Challenges." *International Journal of Advanced Research in Engineering and Technology (IJARET)* 10.1 (2019): 566-581.

10. Shaik, Mahammad, et al. "Enhancing User Privacy in Decentralized Identity Management: A Comparative Analysis of Zero-Knowledge Proofs and Anonymization Techniques on Blockchain Infrastructures." *Journal of Science & Technology*1.1 (2020): 193-218.

11. Vemoori, Vamsi. "Comparative Assessment of Technological Advancements in Autonomous Vehicles, Electric Vehicles, and Hybrid Vehicles vis-à-vis Manual Vehicles: A Multi-Criteria Analysis Considering Environmental Sustainability, Economic Feasibility, and Regulatory Frameworks." *Journal of Artificial Intelligence Research* 1.1 (2021): 66-98.

12. J. Liu, X. Zhang, Y. Zhang, and W. Xu, "Security in Autonomous Driving: Threats and Countermeasures," *IEEE Wireless Communications*, vol. 26, no. 4, pp. 30-36, Aug. 2019.

13. L. Zhang, X. Chen, and H. Chen, "Adaptive Intrusion Detection in Autonomous Vehicle Networks," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 8, pp. 7433-7443, Aug. 2019.

14. T. Zhou, W. Wu, and W. Wei, "Privacy-Preserving Authentication Scheme for Internet of Vehicles," *IEEE Transactions on Intelligent Transportation Systems*, vol. 21, no. 4, pp. 1605-1614, April 2020.

15. A. Boukerche and Y. Ren, "Energy-Efficient Data Fusion Techniques for Reliable and Secure Communication in IoT-Based Intelligent Transportation Systems," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 10, pp. 11699-11711, Oct. 2020.

16. F. Javed, M. K. Afzal, M. Sharif, and B. Kim, "Internet of Vehicles (IoV): Challenges and Solutions," *IEEE Access*, vol. 7, pp. 173623-173651, Dec. 2019.

17. H. Peng, W. Zhuang, and W. Zhang, "Research on the Cybersecurity of Connected and Autonomous Vehicles: Focusing on Two Key Problems," *IEEE Network*, vol. 34, no. 5, pp. 197-203, Sept. 2020.

18. R. Hussain and S. Zeadally, "Autonomous Cars: Research Results, Issues, and Future Challenges," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 2, pp. 1275-1313, Secondquarter 2019.

19. S. Ahmed, M. S. Hossain, G. Muhammad, and K. H. Kim, "Trust-Based Fusion for Intrusion Detection in IoT-Based Intelligent Transportation Systems," *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 3, pp. 1573-1584, March 2021.

20. X. Liang, J. Zhao, L. Qian, and X. Shen, "Enabling Reliable and Secure IoT-Based Autonomous Vehicles," *IEEE Transactions on Dependable and Secure Computing*, vol. 17, no. 6, pp. 1378-1391, Nov.-Dec. 2020.

21. P. Hu, L. Li, Y. Chen, M. Cheng, and S. He, "Secure and Efficient Data Transmission for Intelligent Vehicular Networks," *IEEE Transactions on Intelligent Transportation Systems*, vol. 21, no. 5, pp. 1900-1912, May 2020.

22. H. Song, L. Zhao, and C. Zhu, "Privacy-Preserving Data Aggregation in IoT-Enabled Smart Vehicles," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 7594-7603, Oct. 2019.

23. M. Gerla, E. K. Lee, G. Pau, and U. Lee, "Internet of Vehicles: From Intelligent Grid to Autonomous Cars and Vehicular Clouds," *IEEE World Forum on Internet of Things (WF-IoT)*, pp. 241-246, March 2014.

24. R. Liu, Z. Zhao, X. Zhang, and J. Zhao, "A Lightweight Intrusion Detection System for Autonomous Vehicle Networks Based on ELM," *IEEE Access*, vol. 8, pp. 204331-204341, Nov. 2020.

25. W. Gao, T. Jiang, L. Hu, and J. Wu, "Edge Computing for Autonomous Driving: Opportunities and Challenges," *IEEE Network*, vol. 32, no. 6, pp. 108-113, Nov.-Dec. 2018.

26. K. Mershad and H. Artail, "Finding a STAR in a Vehicular Cloud," *IEEE Intelligent Transportation Systems Magazine*, vol. 5, no. 2, pp. 55-68, Summer 2013.