Cognitive Threat Detection Systems for Autonomous Vehicle Networks

By Dr. Pierre Bourque

Professor of Geomatics Engineering, Laval University, Canada

1. Introduction

The deep neural system is practicable entity for a variety of standalone pattern recognition and classification systems that use low complexity in the case detection task and largely accounts for the state-of-the-art in effectively many real-world problems. Another requirement of the different AI-powered classes based on the learning techniques are participating into focused conditional phrases and serves against learning models. The accidental driver, driver assistance, and automated vehicles will expect to allow secure cooperation against the communication and decision making for safeguarding the individual and society and promote cue and environmentally friendly driving. The physical (and nonphysical) addresses of these threat signals give precautions against the smart engineers and professionals to realistically design an entire protected ecosystem in the automatic vehicle subsystems. The core of this survey article is based to focus on the state-of-the-art in autonomous vehicle and connected drone security mechanisms and their key assessment through this document, such as 6G technologies and systems and application assignment, and the prohibiting the cyber-physical impacts between incoming dives in local and public domain performances.

In the modern automotive domain, autonomous vehicles, have evolved from connected vehicles and conventional vehicles to exchange safety messages (beaconing) and speed and heading information to enhance road safety by minimizing human error out of the automobile. In recent years, intelligent autonomous vehicle networking applications have become popular infrastructure of a blend of smart transport schemes to provide connected vehicle features based on intelligent transportation systems, which deliver infotainment while multi-model transportation and improve traffic safety. Moreover, vehicles that are not simple nuances are integrated as flying automobiles, drones and off-road and watercraft applications,

among different utilization. Each intelligent vehicle application has a tough design requirement that combines significant security techniques in its architectural considerations.

Vehicles are complex cyber-physical systems with numerous controllers and components evolved to provide a large scope of services ranging from safety and ride comfort to infotainment and convenience functions. The integration of such a wide variety of functionalities and electronic equipment into the standard automotive network architecture renders them more prone to security attacks. Since 2010, cyber-attacks against vehicles have gained considerable attention because inter-vehicle communication schemes are being progressed in many industrial nations as an important transmission method for recognizing cooperative intelligent transportation systems. Autonomous and intelligent autonomous vehicles are perceived as possible ways to control the vehicle in the automotive paradigm.

Cognitive Threat Detection Systems are advanced technologies designed to identify and mitigate potential risks and threats. These systems utilize artificial intelligence and machine learning algorithms to analyze vast amounts of data in real-time, enabling organizations to proactively detect and respond to potential threats to their networks, systems, and data. By continuously monitoring network traffic, user behavior, and system logs, cognitive threat detection systems can quickly identify any suspicious activities or anomalies that may indicate the presence of a threat. This proactive approach allows organizations to take immediate action to prevent or minimize the impact of a potential security breach. With the increasing sophistication of cyber threats, cognitive threat detection systems are becoming indispensable tools for organizations of all sizes and industries to safeguard their digital assets and protect against both known and emerging threats. By leveraging the power of artificial intelligence and machine learning, these systems provide a comprehensive and proactive defense against cyber threats, helping organizations stay one step ahead of cybercriminals.

1.1. Background and Significance

We propose the Cyber Attack-Aware Integration Algorithm (CAIA) to serve as an input filter for a multi- sensor fusion system and perform robustly against all mentioned attacks. Both nature-aware spoofing attacks and an array of stealthy cyber-attacks were used for testing. We also used six different multimodal integration algorithms from the literature to evaluate their sensitivity to sensor spoofing and stealthy cyber attacks on the sensors. We will have concluded these with a brief description of the next steps in CTS for connected autonomous

vehicles which involves developing a scenario based taxonomy of attacks. In the immediate future we are transforming this information to a deep learned model that will be embedded in a new sensing module. [1] The input filter will be also incorporated back in the fusion module after categorically classifying the spoofing and cyber-attack type. This new test bed of multi-sensor modal spoofers and stealthy cyber attackers will then be fully replayed to ascertain the robustness of the CAIA. Subsequently, the presented paper has introduced a comprehensive review of the existing defense-less technologies of the networked connected autonomous vehicles from the view point of strings, binary and object (point cloud) spoofing attacks.

Security and safety should be the primary concerns in autonomous and connected vehicle systems. Cyber-attacks like Spoofing, Stale Data Injection, Stealthy Denial-of-Service and Sybil Attack can lead to either direct loss of dollars or loss of life. In this paper, we review the existing security mechanisms designed for the technologies associated with networked connected autonomous vehicles. We also emphasize the pivotal role of multi-sensor integration that itself forms its vulnerabilities to cyber-attacks. The decisions of an autonomous vehicle depend critically on the input sensor data that maps the physical world. The result of integrating data from explicit sensors takes the form of a form of an informed abstraction, a Virtual-HD Map. [2] Therefore, faked sensor data can be used for Stealthy False-Data Injection, Ego Vehicle Nuisance-Denial of Service (DenIAL), Ego Vehicle Stealthy Spoofing and Local Dynamic False Data Injection attacks. The Stealthy Denial-of-Service attack can easily convert into a more damaging attack because all involved testing vehicles also test various forms of data rejection. This rejection can become stealthy if brute force testing is used and the input data has no randomness. While the importance of stealth in cyber-attacks has been well appreciated in the literature, dynamic stealthy attacks which can switch their mode dynamically for purposes of obfuscation and robustness is not generally considered.

1.2. Research Objectives

Our cognitive system will handle datasets with label noise, so it is robust in corrupt and Byzantine adversarial settings. Since different attacks can have similar affect, we will develop methods for attack functional replacement, this means we will build robust models that are accurate in adversarial attacks. We will develop methods that adjust the robustness of our

model based on available dataset feedback data in an automated, seamless manner. It is important to maintain autonomy and reduce human intervention in our system security. Automatically estimating a model's autonomic assistance and stopping adversarial attacks might require proving mathematically that 'no legitimate substitute for a human needs to be involved' while defending against specific attacks. Our methods will differ by AV functionality as well as attacks. Essentially, this means that our method will handle all these according to needs while thwart adversarial attack. Building upon the study by Sadhu (2023), which investigates the integration of SSO and OAuth for secure patient data access in healthcare applications, this research explores the security and user convenience enhancements achieved through this integration on AWS GovCloud.

Our vision to balance security and autonomy within Jay will have several components:

Nowadays, collaborative infrastructures provide massive benefits that will allow introducing autonomous vehicles and other uses cases in the future. However, on the other hand, they present attack vectors: this infrastructure may be employed for attacking vehicles, thus blocking traffic, performing privacy theft, and lowering the security level of the widely deployed and highly trusted connected car technology. This study presents a risk analysis of the fully autonomous vehicle's communication infrastructure to meet and increase the security level of connected autonomous vehicles.[3] "A Systematic Survey of Attack Detection and Prevention in Connected and Autonomous Vehicles" By Seyed Farid Shahab Nazari, Marianthi Theocharidou, Dimitrios Serpanos. Connected and autonomous vehicles (CAVs) use advanced driver assistance systems (ADAS) and vehicle-to-everything (V2X) communication systems to share real-time information about the road and provide passengers with a safe and comfortable driving environment. However, the traffic density is increasing each day, leading to high traffic congestion which requires improvements to the road-utility network. CAVs and electric motor companies are increasing, getting benefits from this, and motor companies and researchers have designed autonomous vehicles to connect with other vehicles and even to smart city infrastructure to increase road utility and reduce traffic congestion and accidents risks. Frequently connected vehicles provide the possibility to safely maneuver through intersections to eliminate the necessity of stopping the vehicle; besides the ability to communicate with the AV system to send it to EV charging stations for recharging. This kind of communication is crucial to make the cars smart enough to copy with normal or adversarial electromagnetic noise. Perturbed or corrupted automatically generated sensor

feedback data can lead to AV crashes or malfunctioning requiring developer's tremendous cost and time for reducing the width-connected vehicle technologies more critical that automatically generate feedback data.

[4] "Risk Analysis Study of Fully Autonomous Vehicle" By Mahmudur R. Khan, Kevin Foster, Daniel Mendez, Kusum L. Ailawadi, CEmgleby Payne, CamIG tchcol. Autonomous vehicle technology is rapidly advancing due to increasing demand and public interest. Autonomous vehicles are able to both – physically and digitally – communicate with other advanced infrastructure elements. Nevertheless, by being part of larger cellular and distributed communication systems, this represents a new attack surface, exposing these systems to digital security related risks. Following the insights of Reddy, et al. (2023), who explore the integration of generative AI in CRM systems, this study utilizes their data-driven framework to enhance content personalization.

1.3. Structure of the Work

The vision of connected vehicles also known as intelligent transport systems (ITS) allows the introduction of both safety and non-safety applications by using vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I) and vehicle-to-everything (V2X) communications. However, the reliance of these applications on communication technologies, such as Wireless Ad-hoc Network (WANET) and DSRC, brings several security threats to the infrastructure and vehicles, which if not resolved, can pose serious threats to the safety of individuals and traffic flow. However, information security is crucial to establish trust between vehicles that establish network. Likewise, the lack of confidence in the distribution of information will affect traffic management and harm national traffic management and vehicle-to-vehicle safety communications. This introduces a new process that conflicts with the other normative goals in vehicle-to-everything (V2X) communication and with the conventional approaches safety communication technology. Therefore, the straightforward application of traditional security solutions such as secure encryption for confidentiality, secure hash algorithm for integrity and verification in these environments has numerous problems. Hence, security solutions cannot simply be used in V2X environments without the development of new security technologies that consider the features and threats of vehicular ad-hoc networks (VANET). Security Relevant Incidents and External Events (SRIEE) are those events that have a negative impact on the threat and hazard analysis. This work emphasis on mobile Unmanned Aerial Vehicles

(UAVs) supporting autonomous connected cars provide an alternative approach for V2X safety mechanisms with V2X communication link. [5]

The work in hand proposed a deep learning framework based Intrusion Detection method for two-wheeled electric vehicle battery systems. The method proves effective in detecting various cyber-attacks such as Denial of Service (DoS) to battery PCM and BMS; such as tampering with temperature, state of charge or state of health sensor information of the battery PCM or BMS at vulnerable nodes or making the motor execute a racing condition by attacking the data packets. The paper is structured as follows: Section 2 reviews the literature and Philips the research gap and research questions. Section 3 describes the Proposed Intrusion Detection Model. Section 4 explains the experiment results and analysis. Finally, Section5 concludes the paper. [6]

2. Fundamentals of Autonomous Vehicle Networks

Vehicular ad hoc networks (VANETs) have recently attracted significant attention due to their ability to provide application services such as traffic safety, traffic management and infotainments. As a result of these values, proposed VANET architectures have been designed and built to address several outlined functional and non−functional requirements, however, the proposed architecture are typically not guaranteed to be intrinsically secure. The practical threats that often occur include sniffer, routed attacks, message dropping, traffic analysis and active attacks [7]. This has made securing secure communication inter−vehicles and AVN communication from both network layers to vehicular applications more crucial in the transport domain. Consequently, this paper uses a novel approach of using Petri Nets (PNs), which are high level Petri Nets (HPNs) as the mathematical model to build SECurable and KNowledge empowered System(s) (SECKS).

Autonomous vehicles (AV) are promising to significantly reduce traffic accidents, commuter time, and transport costs, while increasing vehicle fuel efficiency, usable road capacity and utilization of vehicle assets. The increase in road safety could be enabled through inter−vehicle cooperative systems, which include advanced driver assistance systems (ADAS), collision avoidance (CA), and vehicle platooning. Nevertheless, through technical and security issues induced due to vehicle and infrastructure communication, the security of transportation systems is threatened [8]. This domain has not been conclusively addressed by scholars yet from the security and privacy vista of vehicle communication. All the works are

based on traditional security mechanisms, cryptography, and authentication. This domain lacks threat assessment (TA) models, autonomous vehicle network (AVN) and vehicular ad hoc network (VANET) gateway security and privacy. Consequently, the domain is under−developed in comparison to the emerging threat challenges.

2.1. Definition and Components of Autonomous Vehicle Networks

[9] With the increasing bandwidths of the next-generation mobile and wireless technologies, new safety applications will be realized that are currently not possible. The concept of new mobility services is developing where traditional methods of services are exceeding their boundaries. It is proposed to create a network consisting of two layers, namely the physical network and the service network for CAVs. The physical network provides infrastructure reliability of CAVs by allowing continuous communication between N-BSs. On the other hand, the service network ensures that the services are multimodal and that the stop-and-go behavior of the user is better automated [3]. Satisfying these requirements on a wide range of target characterization will support the development of security services specific to CAVs.[6] A disruption of the computer network in autonomous vehicles commonly exhibit attacks. To begin with, Denial of Service attacks (DoS) block access to resources in the vehicle. Some DoS attacks can be permanent, DDoS, and other can target groups of users. Unlike DoS, Man in the middle (MitM) attacks targets interaction between vehicular nodes. They listen to share fitting information with a source and tries to intervene themselves by relaying incorrect share installing them to act wrongly. As with the wide development of computer networks contagion of malware has now extended to automotive systems. As soon as a malware slips into a vehicular system implicated in a crash, the car entrance of supportive functions is risked.

2.2. Challenges and Vulnerabilities in Autonomous Vehicle Networks

Modern automobiles necessarily include connectivity abilities, and thus car cybersecurity seeks to achieve five security goals: Confidentiality (we have to avoid data tampering), Integrity (check summed and encrypted systems should automatically discard data hence tampered), availability (absence of interruption of service), privacy (to avoid the possibility that an external player eavesdrops what a personal connected car is doing), and safety (we shall avoid a tampering leading to critical faults) [6]. The set of electronic systems that manage the car's operation may be attacked using traditional cyber-attacks. Some examples of possible

exploited vulnerabilities are the car data exchange framework, WiMAX, communication services like 3G-LTE, nal automobile buses such as CAN, V2I communication, ECUs mutual communication, supply chain security, and car network dierent devices. Car to car communication is another macro-topic. Only direct communication between vehicles is available in VANETs and much has been written on this topic. On the contrary, cloud-to-car and cloud-to-roadside are now the examples of V2I. This is why in a vehicle of our interest we have access to ve "external security levels": the Digital Terrestrial Networks (DTNs or terrestrial communication infrastructure), ISP (Internet Service Providers), service providers, and a cloud ecosystem in which Car2Cloud aspects in transparency are composed with data analysis and offered service and/or applications [2]. Additionally, apart from classical known exploits and vulnerabilities (e.g., vulnerability in a given protocol, misconfiguration due to patch absence or pressure in updating, exploitation of poor error handling), in a connected vehicle it is possible to introduce specic signed vulnerabilities; this is the case where the software system is highly dependent on potentially intrusive automotive communication protocols and vehicle data processing. In effect, such system's intrusion data stream could be carefully tempered with a specic purpose, such as simulating an anomaly (falsication) in the car real behavior. Just simulating a car breakdown (e.g., defective sensor) would already be annoying, but an adversary vendor might be able to design a much more subtle compromise, preventing a safety-critical fault from blinking on the dashboard as if sensors and actuators were real.

Cognitive Threat Detection Systems for Network of Autonomous Vehicle Networks: 2.2. Challenges and Vulnerabilities in Autonomous Vehicle Networks

3. Cognitive Threat Detection Systems

Acubi is mounted on each on-board unit (OBU) in the intelligent transportation system (ITS) and evaluates the threat scenario that the OBU faces by considering the communication modules it resolves. Acubi is based on self-organizing maps (SOMs) combined with intrusion detection systems (IDSs). Acubi learns abnormality patterns in varying environments. Finally, there are cognitive attackers who employ different threats based on the severity of a threat scenario. We evaluate the false positive rate, false negative rate, and time overhead effect of Acubi in communication environment modeling [9].

Cognitive threat detection systems (CTDS) can detect threats with low false positive, false negative, and time overhead rates. Threat detection refers to identifying malicious communications in networks by identifying discouraged or forbidden behaviors. Here, we focus on cognitive threats that involve communications targeting vulnerabilities in the vehicle's computing hardware, software, or behavior [10].

3.1. Definition and Principles of Cognitive Threat Detection

In this article, the general principles of a cognitive framework for threat detection in autonomous vehicle ADAS and connected infrastructure are summarized. It is discussed how the framework provides very accurate threat detection rates and a huge reduction in processing time by synthesizing three different hierarchical perception blocks. The hierarchical approach allows us to integrate preknowledge available directly in the system, flowing from the advanced driving assistance system (ADAS) and safety measures in the car and within the infrastructure onto fast deep-learning decisional blocks, performing out-of-peception-threat detection. The same blocks ensure very less-systematic false alarm responses, by not alarming too quickly when it comes to actually-thresholded contextual safety-tolerance threats. Lastly, out-of-context threat stemming from unknown attacks or showing various signature deformations at the ADAS level will pass towards system learning, to have a behavioural adaptation of safety measures in place. [10]

Cognitive threat detection can help detect system attacks even when the operating environment is not previously known. [5]Cognitive threat detection is the process of detecting and discriminating objects, signals, and attacks and threats against connected autonomous systems, taking into account the interactions such systems have within their complex, dynamic, and unpredictable traffic environment. Different from traditional threat detection systems, which are based on detection and discrimination of single attacks one by one, cognitive threat detection system tries to recognize very different and unknown attacks and then take actions accordingly.

3.2. Types of Threats in Autonomous Vehicle Networks

The controller is also vulnerable to persistent attacks going unmitigated for a longer timespan than its scheduled reset [11]. The attackers directly focusing on victim sensors under autonomous on-board networks execute signal substitution attacks disregarding unsuitable

angles and velocities, possibly tampering with Dynamic and Static Vehicle Stability Control (VSC) systems in the direction of arbitrary offsets unwanted by the control software. Code-offenders can also manipulate measurement infusions by modifying perception, discrete, and continuous-time Kalman filters.

The attack targets vehicle networks either by sniffers or loaders of malicious messages, which can originate from a compromised sensor or an external interceptor at a vehicular network's access point as the vehicle's wireless interface [12]. In such cases, an attacker might maneuver the car by wrongly appropriating body control units (BCU) and electrically-controlled brake units (EBB) other than by tampering with onboard position sensors. Unlike external adversaries, it is conceivable for an internal adversary to obstruct the accuracy of sensors that intend to reach the attacker-controller level of inverses of the dynamics obeying the Heart-In-the-Loop (HIL) scheme [13].

3.3. Role of Machine Learning and Artificial Intelligence

Current machine learning-based models need a significant amount of labeled data to accurately detect security threats across autonomous vehicle networks. This necessity can lead to problems where collision attacks or multi-pronged hacks that include an intrusion followed by a misbehavior affecting the model's behavior are indistinguishable. Recent research has addressed this via a reinforcement learning (RL) model guidance that makes use of a limited set of labeled data to effectively pre-train the big model before it is applied. This compensates for the major drawback of RL which is its sample complexity, thus allowing for the learning of deep RL models with a reduced number of samples. [14]A few critically essential criteria are identified that must be looked for when selecting a machine learning-based approach for developing a cyber-physical threat detection system. It is addressed that the algorithm selected must be well-suited for implementation on resource-constrained devices, handle temporal dependencies inherent in the data, and transparently explain the detection outcome. Furthermore, a list of possible future threats is identified and it is suggested that mitigations be deployed in advance to minimize the impact of such threats. Therefore, the cyber attack problems that AI applications should be addressing in DMS-based systems are stated. There are potential AI-associated solutions, including cautious data augmentation, mixup approach, and counterfactual samples-based anomalous detection, quick AI interpretations and

transformations of input for labeling adversarial samples during training, AI explainable models, and learning bias models. [15]

4. Existing Threat Detection Technologies

The development of robust and real-time threat detection systems for autonomous vehicles becomes the current need. The state-of-the-art and cutting-edge threat detection and correcting technologies have been discussed in our study. Moreover, with industrial use applications, some promising techniques such as sensor-based, communication-based attack detection and correction, different algorithm-based trust development, some secure and robust key management and unit fault detection, tracking, and isolation systems have also been presented. All these technologies aim to improve the base connectivity, numerous error detection, falsification of data and messages detection, protocol-based attack detection through stochastic signal processing, information sharing and routing request, propulsion systems and fault security. The most complex obstacle avoidance is discussed to ensure communication and sensor-based technologies secure the vehicle's operation. The leading industrial systems pioneer the advanced vehicle experiments and robotics companies' active tests maintaining open access for public use analogous to the coordination of advanced sensor technologies. This facility is capable of providing the multidisciplinary test facilities according to the favor of national and international requirements regarding insurance measures, risk assessment, operation insurance, threat anticipation, defense, and monitoring system requirements.

In the contemporary era of technology, vehicles and other vehicles' systems are interlinked in intelligent networks to make the best utilization of resources, minimize the accidents through active safety, and facilitate real-time noncritical information to improve travel. However, the network-induced threats are the primary concern for developers to ensure secure operation of such autonomous vehicle networks . As the autonomous vehicles are equipped with advanced sensors, embedded computers, advanced algorithms, and communication technology, these vehicles become the carrier of traditional vehicle safety linear threat, sensor-specific threats, and open protocol and communication technology threats. These threats can significantly compromise the safety of passengers and more significantly, road users and traffic.

4.1. Traditional Approaches

A number of cyber threat detection systems have been introduced in the relevant literature. Such systems use anomalies to detect and report on attacks on a vehicular network [16]. In contrast with traditional literature, our approach considers the unknown as a class similar to the known known. There are no relevant limitations against the solution or solutions used, and provide information or knowledge related to network communications in a welldecisive way. Some of the key sources of cyber security vulnerabilities in intelligent transportation systems include Electronic Control Units (ECUs), telematics units, cellular and satellite receivers, Wireless Access Points (APs) and In-Vehicle Networks (IVNs). The state-of-the-art IDSs proposed for IVNs indeed exhibit several shortcoming and limitations. These limitations include considering known cyber-attacks only, detecting anomaly cyber-attack only, relying on manual intervention and expensive computations, and scope limitations that require IDSs to be implemented elsewhere in the network. There is no need for a priori knowledge about known cyber-attacks and anomalous communication patterns in the network 8 cf.

The solution for cyber-physical systems security is multifaceted, including diverse strategies like encryption, intrusion detection and response strategies, and anomaly detection systems [2]. The most commonly deployed cyber security tactic is edge/endpoint cryptography which requires a cryptographic key—whether symmetric or asymmetric—to produce a secret codes mandated in the communication between nodes and antecedently, the system users. Encryption is a mutation of character strings by means of an encryption algorithm and a key, so that the original data is not discernible without the recovery of the encrypted data via a corresponding decoding key or code. Traditional cryptographic schemes, however, do not authenticate the originality and integrity of the data that are being communicated. This limitation may be resolved by utilizing hashing functions. In next generation intrusion detection and response methodologies, file-less threat detection and isolation, which count on machine learning, are surpassing the traditional honeypotting and signature-based strategies. Despite the number of its participants or the pattern of the communication traffic, the intrusion detection and response methodologies are implemented as an interactive or a machine learning algorithm that can diagnose and block malicious entities and activities [6].

4.2. State-of-the-Art Technologies

The security of connected and/or autonomous vehicles (CAVs) is being considered as a critical aspect as the vulnerabilities they expose are targeted by cybercriminals who can then

remotely manipulate a vehicle posing a potential risk to human lives. This article aims at reinforcing the importance of adopting deep learning in IDS development for CAV systems. This is because the issue of creating efficient and resilient machine-learning-based IDS algorithms is strongly linked to the trade-off between security threat mitigation and fleet-performance constraints which are tackled by the authors with the proposed machine-learning schemes. Indeed, solutions dedicated to IDS in CAV scenarios are typically based on decision tree-collaborated approaches to single-branch deep learning. The aim is also to remove the need for programming the distribution of anomaly features during model implementation, as well as protecting the robustness of the model against attack representations – two aspects which are crucial in a realistic CAV scenario [17].

This work reviews some of the latest technologies and methodologies that can be adopted to detect and mitigate threats in autonomous vehicle networks and presents in detail two state-of-the-art (SOTA) algorithms for its implementation, i.e., the interval-valued fuzzy approach and the modified extension theory approach. The interest in security research and development (R&D) has therefore been triggered by the fact that threats to connected and autonomous vehicles (CAVs) may lead to serious consequences in transport, citizen safety, human lives and the national economy [18]. The vulnerability and risk assessment for CAV systems must be multidisciplinary and accounted for during the design, engineering and development stages. Notably, CAV threats can be categorized as either direct (e.g., malfunction of an object-detection sensor) or indirect (e.g., altering the decision-making mechanism of an autonomous vehicle) in nature. The intrusion detection system (IDS), in this scenario can be seen as an important complement to the existing cybersecurity methodologies. IDS is designed to automate early malware detection, identification, and classification in order to assist CAV focused – embedded designers with cost-effective open-source defence [2].

5. Design and Implementation of Cognitive Threat Detection Systems

The device at the edge manages the main intelligence and computing functions and acts as a cognitive unit deployed on the buses of the vehicles [2]. The edge network is in charge of vehicle monitoring. Several vehicles create and manage a cooperative vehicle network, which has also been enriched with sensors at the edges. The first part contains multiple mechanisms, such as robot-operating system (ROS), dedicated control unit (DCU), and middleware (MM). The middleware is in charge of collecting and combining signals from sensors and the

corresponding vehicle's nodes that contain basic electronic control units (ECUs). The recent version of the MCUs allows the nodes to directly serve their signal to the edge network, to their application processors, and the comparable neural network of the vehicle. Additionally, the digital twin and machine-learning elements are deployed to enhance the DT and traditional machine-learning (ML), Iterative Neural Prediction, and Reinforcement Machine-learning Reinforcement Learning (RL).

In order to effectively detect threats to autonomous vehicles, we designed an AI-driven cognitive system that operates in two levels: devices at the edge and the cloud [3]. In the first level, a combined machine learning and digital twin (DT) system learns from the dynamics, conditions, and processes the vehicles and its environment. Once trained, the DT is deployed to predict the most probable behavior of the vehicles, surrounding vehicles, infrastructure, and, overall, the transportation network. In case of unclear or unusual situations, the DT triggers potential alerts and informs the network. When several alerts are raised in the system, then the most probable threat vectors are communicated. In the second level, a neural network with well-tuned hyperparameters for the Cognitive Engine of the classical Model-Predictive-Control (MPC) architectures is deployed. The learned detections of the first level are used for potential object detection, and the neural engine infers whether the conditions in the environment are threatening (e.g., low adjust, malicious access). When this is the case, the cognitive engine triggers the distributed threat detection mechanisms.

5.1. Architecture and Components

The cyber protection system proposed for control units of atonomous vehicles untangles key issues like security-related state estimation and security-aware trajectory planning. Attacks against autonomous or connected cars opens up a lot of safety and security vulnerabilities. These dire scenarios, first liken the system's feature into legal, software, security and safety aspects and subsequently voice the potential impact in terms of violation of the system's cyber and safety availability alike [19].

A cognitive cyber protection system has been proposed as a solution to the protection of critical infrastructures relying on autonomous systems, such as vehicles, energy grids, and buildings [5]. This system is based on reinforcement learning and recurrent neural networks, whose policy networks are responsible for the investigation of possible threats over time; these are dynamically personalized by the recurrent part, which makes the whole system

adaptive to unpredictable environments and potential adversarial dynamics. Capabilities and diverse architectures of deep learning in defense, smart defense, and adversarial defense capable of such architectures to increase the cyber secure system performance [6].

5.2. Data Collection and Processing

Threat detection during human-computer interaction (HCI) leverages not only system-focused data like requests or delivery data, but also user-focused data like the user's decision-making or intention data. Sometimes, a threat such as a malware attack or misbehavior may be detected and handled by using user-focused data and usually terminated for safety reasons, but its dynamic-level effects can still be observed after termination, e.g., heavy CPU usage, spiky power consumption, or out-of-band network traffic, and these can be detected only via HCI! The latter is the focus for the proposed approach, and the task is to generate a feature set using user-driven HCI data from 12 data sources while carrying out several DNN-based analysis tasks which should lead to feature selection/cleaning in the related databases. Notice that there are many non-CK fingerprints; we have taken account of this during the feature engineering. Finally, we enhanced the current version of our driver-monitoring model to explore the driver-involved threats in the vicinity of vehicular networks [15]. In this article, we discuss real-time mechanisms to identify and counter cyber-attacks on CAV systems in an Infrastructure-to-Vehicle (I2V) communication environment. We identify different attack types that could take place on the V2I communication system. We observed the trajectories when an attack is launched into the V2I communication systems with different Digital Ecosystem IDs (DEIDs) and also with different Data Paket Data Units (PTK and GTK) (PDU and GDU). In verification, the approach proposed hope to provide a robust detection mechanism by which V2I communication is made tamper-proof. This work deals with the transition of the origin of an attack on the connected CAVs. We have studied the transition of normal V2I communication to an intruder attack. We consider a particular group of V2I communication system as reference and then a test case is created where we randomly check different types of tampering with respect to it [17].

5.3. Model Training and Evaluation

In conclusion, a suitable model should be adapted for our deep learning model. Additionally, as freely available, multivariate datasets of cyber-attacks on IoT devices are not available, UGR'16 and CICIDS2017 are employed to investigate the proposed deep learning algorithm.

Also, the suggested ensemble model with U-Net style as multi-level temporal-spatial shallow net sequences and LSTM for the final stages is evaluated with two diverse remedy datasets.

[12]In research, original unimodal and multimodal models have shown robustness and effectiveness in the application on coinjecture attacks, while the one based on the depth temporal-spatial network (DTN) has demonstrated superior anomaly detection when compared to similar IoT data. Attackers mainly inject their individual attack records that are different from normal ones. The forensics results show that four of the DTN bands show clear inconsistency between normal and selective attacks. As a result, the depth temporal-spatial network is vulnerable to overfitting of the training set, which is one reason for the failure of the DTN model in target attack detection.[20]Since IoT and 5G networks have not yet been fully identified and utilized in autonomous vehicles, a new concept of LTE-Vehicular (LTE-V) is proposed to provide vehicular service through the existing 4G LTE network. The article focused on identifying vulnerabilities and security attacks for modern connected and autonomous vehicles through several relevant literatures of recent years and suggested recommendations, such as guaranteeing safety and clearing responsibilities of the participants. We provide a comprehensive summary of the most significant vulnerabilities and attacks on different parts of connected and autonomous vehicular systems, this includes attacks on external communication and on-vehicles systems. Then, we briefly discussed the implication of the vulnerabilities and threats, and then proposed a model for a secure system design and responsibility assignment for better safety. Consequently, this survey intends to present current security issues in spare categories including external communication interfaces, communication protocols, on-vehicle domains, software and hardware, and enabler technologies. Finally, we shed a philosophy-based argument about how security responsibility might be constructively divided among stakeholders in the connected vehicular domain that would guard a fair and faultless participation in the security of connected vehicular systems.

6. Performance Evaluation and Case Studies

Protecting Intelligent Transportation Systems (ITS) against various cyber related attacks is extremely challenging given their high computational demands and reaction times. Cyber Threat Detection and Prevention Systems (C-ADAS) based on AI/ML models are used for inspecting and monitoring the networks for deviations. In authors have presented novel

methodologies for securing communication networks and explored hostile scenarios under which autonomous cars are liable for change in their driving directives. In, C-ADAS acquires the dynamic traffic density and behavioural model using Recurrent-Neural Network (RNN) and another RNN block undertakes the potential Western Union cyber-physical incident based on these inputs. If decision-maker detects an injury report, C-ADAS does not accept cruel control action. For studying the future stage of connected and cooperative transportation, we are broadly considering scenarios with the capability of enforcing collision prevention/engagement between participants actively. In this way, using a road junction case study various vehicular observations are provided to cloud-connected ambience. [21]

A practical implementation of C-ADAS is generally based on testing it with various vehicular movement and threat generation scenarios. In this work, two real-time vehicular communication scenarios have been sketched out. In Fig. 10 the cases of two cars moving on roads with arrival times at three different traffic light-controlled road junctions are presented. The primary motive of creating this scenario is to analyse the performance of C-ADAS both in the presence and absence of cyber-physical attacks. The position of the target car C2 (in black) is tracked by the EGO vehicle C1 (in blue) using RTK-GNSS. The dynamically changing differential distance is used by C-ADAS to role out cooperative control action as an anti-terrorist expertise.

article_id: 872a1f2e-776c-4f16-b89e-885667529623 article_id: 934507dd-3d5e-4d47-9964-31660871cbf8

6.1. Metrics for Evaluation

While evaluating some tasks like lane detection the mean Intersection over Union (IoU) or heading estimation on records of a dataset are manly talking about model's performance on labeled portions of the dataset, which can clearly address the quality of the perception performance for these tasks, evaluating the perception object detection systems by standard metrics like approximate percentage of False Positives: FPs = 1 − Precision, or False Negatives: FN = 1 − Recall, are not enough in order to ensure that if there are any perception errors in the trajectory, the later task does not observe any miss-decisions. Even if a perception system could detect all obstacle objects correctly in the frames, the planner actuation after these misdetections can increase violation of high-level safety constraints like keeping the safety distance or avoiding sudden maneuvers. We refer to this important safety-critical topic as

Perception Safety Constraint Violation which means that there are no incorrect obstacles detections and unexpected obstacles are not in the predicted regions for the future according to the tracking results but a safety-critical maneuver is expected sometime in the future, and then it is missed that the control-code has an internal conflict between the different monitoring blocks, e.g., dynamic obstacle tracking (spatio-temporal conflict) and internal map (interaction-awareness problems) also the prediction block (temporal problem). The inverse or in the case of standalone obstacle perception are considered as constraining driving maneuver violation in planned space. The common performance reporting metrics are quoted from 2021: IoU (Intersection of Union) - IoU > 0.5 is counted over the groundtruth bounding box area as True Positives, and other truth objects are counted as False Negatives, Precision = True Positives / (True Positives + False Positives), Recall = True Positives / (True Positives + False Negatives) [22].

Increasing attention is paid to the autonomy of vehicles. Many systems are simultaneously working on different subtasks, including the system for safe stopping. They evaluate short-term comfort (e.g., jerk values) and comfort in a longer time horizon (e.g., maintenance of a comfortable safety distance). As future work, more quantitative assessment methods should be adapted and utilized within the architecture. Also important are longitudinal and transversal comfort aspects, because influencing one aspect can have negative effects on the other. It can also contribute to one metric showing good values in the respective comfort aspect, but agree with the other metrics. Also, higher model uncertainties are to be considered, e.g., vehicle models with significant longitudinal slip and lateral vehicle motions. The mentioned comfort aspects and assessments are mainly considered for the longitudinal use case, but also are of relevance for the towed case with perspectives on transversal forces and their influence on stability [7].

6.2. Case Studies and Real-World Applications

The same HTIDS system architecture, concepts and implementations approaches can be easily adapted and deployed in any other kind of autonomous and semi-autonomous mobility, e.g., at assisting systems in V2H systems or to secure the railway system. Eventually co-created values and disruption: currently, more research and networking to foster innovation-based implications are necessary. The increasing use of autonomous systems is expected to make their security and dependability crucial in the near future. It is necessary to consider new

distributed learning-cybersecurity methods to reduce the malware on such devices and a further development of a standard on vehicle security, taking into account the perspective of the blockchain and the Cloud to guarantee the data privacy. Also of particular importance is the integrated cyber-physical security, with constructive malware-based attacks for cyber-risk assessment and hypothesis generation over different elements of a vehicle that maps observed vehicle electromagnetic pulses (electromagnetic propagation and potential radiation) to hypothesis which were instructions for Peripheral Devices (PDs).

Reliable threat detection and mitigation paradigms can enhance the overall security and robustness of AVNs. In this context, this section presents a few real-world applications involving cognitive threat detection systems. European Horizon2020 project "Safe and (Cyber-) SECURE (Semi-) Autonomous Driving (SECREDAS)" focuses on connected and automated mobility and presents the application of Cognitive Threat Detection framework for securing the automated parking scenario. Leveraging the Vehicle-to-Everything (V2X) communication capability, a subscription-based semi-autonomous Use Case was identified that allowed it for simulating different attack scenarios. Multi-Source Information Fusion (MSIF) model integrated the environment sensors and V2X communication inputs to make the risk judgement. A threat monitoring module was designed to capture and control the malignant attacks. A Deep Learning Pass Prediction model is trained on the generated inputs data from the CU, RU, and AIs and the system was tested in diverse car-parking use cases without any noticeable deterioration in performance.

7. Challenges and Future Directions

One can note that in-vehicle communication protocols have their exclusive characteristics and tend to exploit real-time processing methods by which detection of security threats can be unexpected and difficult. Such aspects of security threats in in-vehicle networks are highlighted in. Known security threats in controller area network have been shown together with possible machine learning methods for ID-attacked using a multiclass support vector machine. Key man-in-the-middle attacks in local interconnect network are depicted with attention on identifying such forms of attacks for design of secure in-vehicle communications. On the other hand, cyber security and privacy attacks on FlexRay network have been delineated and effective IDS features for the network are exhibited. Connection-oriented attacks are of the main problem types on Secure On-board Communication, where the authors

propose four types of connections for attacks in the network and are supported by several features of fraudulent and secure connections.

Nowadays, modern communication technologies are employed in order to provide an end-to-end environment to vehicles for offering advanced safety, infotainment, and convenience applications [18]. Such systems are open and have to deal with novel threats that can be based on security and privacy attack forms. It has been shown that strict availability, confidentiality, and integrity are put at risk, but a notable risk associated with connected vehicles is road safety. In [3], the authors offer a comprehensive survey of different cyber threats related to automotive industry including, both in-vehicle and inter-vehicle communications. It is evidenced that attacks such as key-less car theft can have safety consequences. Security measures, like IDSs and cryptography methods, cannot stand-alone protect connected vehicle networks and it is argued that DNN and machine learning are needed [6]. The advent of autonomous vehicle technology has also realized the need for secure inter-vehicle communication mechanisms. 'Automated Waterway Path Adjustment' is introduced in this article beside which having a future look for inland waterway autonomous vehicles is also discussed. The article also sheds highlights on proposed methodologies with corresponding algorithm illustration.

7.1. Ethical Considerations

The automotive industry and affiliated legal and decision current instances are not exceptions among those which may become more efficient in adaptation of smart time-complex management, while creating extensive and multi-level data processing algorithms for engineering support in enabling of safety. In our research, we concentrate on two main topics: potential risk influences of these cooperating characteristics and from them what kind of ethical dilemma of data processing should be conceived. It seems quite evident that inherent dangers and legislative ethical-legal questions of the cooperational actions of automated driving systems are inseparably ignorable as the brief review of standards already reveals. No decision or proposal about supporting or refuting some trend is yet possible. However, if contemporary challenges and consequences are not recognized and thought about, then it may significantly delay the cooperation with other necessary research directions [7]. Interactions of such corporations may kick-start a new type of deep relations and research which may be re-categorized as an Integrated Networking Science.

Autonomous vehicle networks could present all of these aforementioned dangers and threats on an even larger scale, posing significant threats that may have an impact on both overall traffic safety and societal cybersecurity. There are no general-purpose, widely researched frameworks and standards available concentrating on protecting autonomous vehicle networks from internal and external "dual-use" threats [20]. Threat detection algorithms designed to filter out potentially dangerous situations (that are not explicit attack behaviours) must generate low false-negative (low blocking) and low false-positive (low nuisance) classification results. Threat detection and autonomous vehicle network protection legal and ethical issues are investigated jointly in a wider perspective in the chapter, but in this section, threat assessment algorithm ethical considerations studied are especially analyzed. The capabilities provided by the developing and application of artificial intelligence have broad spectrums. The motivation of numerous enterprises for utilizing AI methods and technologies in various types of applications is on the rise [23].

7.2. Scalability and Adaptability

The state of cognitive communications for future mobile networks presented the vision, key communications drivers, and general principles of cognitive communications for 5G and beyond networks. Because of the advanced, dynamic adaptability and any number of networking scenarios including satellites, ground networks, sensor networks, IoT, and more, cognitive optimization was designed for the management of the entire networking system to achieve the management goals optimally. The current honeypots and intrusion detection tools were specifically designed to secure computer systems by luring and capturing the intruders. Therefore it is not suitable for the connected and autonomous vehicles system. Digital Twin (DT) systems work as digital clones of operational objects, providing an interface between real-world entities and their computer-based models. DW3D (DT-Wireless) is a recent paradigm shift in the area of emerging wireless networks, due to the fact it can represent the operational environment in the wireless network of interest. Therefore, it can offer more efficient design spaces, scalability, and adaptive mechanisms.

The scalability of cognitive systems is closely related to the adaptation ability of the cognitive systems in different environments[^2268367a-6d52-4c70-ac51-ee84bc536d54][^9d753ac3-bb35-4d84-9824-a7a2fe7622da]. Considering this, A. Gulliver discussed two taxonomy and pertinence of cognitive radio spectrum management mechanisms, Release First and Listen

First models. In order to accommodate diverse requirements and achieve human-like cognitive computing capabilities, cognitive optimization: a general framework of integrating cognitive computing with optimization methods, is proposed on the basis of the research development of cognitive technologies and optimization. Information technology has been evolving from digital to smart environments, smart platforms, and now to cognitive systems, based on context-awareness, reasoning, and prediction for the users behind the smart entities.

7.3. Emerging Technologies

The last 10 µm critical two-stage defenses in defending blurring, altering, and imitation attacks, defending false reclaim as well as Data Message syntax analysis defenses are designed and innovated. Also, a critical tricky defense against crypto breaking attacks is elaborated. In this paper, multi-sensors are used to detect new attack symptoms. Data, derived from each sensor, is then comprehensively analysed through Bayesian methods, to produce the true sensor output. Detecting a CAM key changing message in order to keep random broadcasting addresses, messages from the central unit (CU), by any attack can force IVi[/sub] to keep a message history and observe the real operation of the AI CU when there is no key changing. If the 979 tms new 8fuassic application in use, none can eavesdrop or pretend to get the token. [18]

Quantum cryptography, together with a new X.509v3 model, can also enhance security in VANET cloud computing environments. Given the key length strength of quantum cryptography, it can be used to generate trusted Public-Key Infrastructure (PKI) listed addressing, which can be authenticated by the in-vehicle unit (IVU) and roadside unit (RSU), cryptographic organizations, placed and registered in the light weighted cloud PKI together with new 5G networks asymmetrical AES key management system which are used in emerging protocol data unit (PDU). The PDU encrypts the vehicle's big data header and establishes random PKI authenticated scheduling together with custom ID list addressing. Non-Radio Regularity (NR) with adaptive semi-random domain-coordination and MX350 paper with intelligence are used to hide critical witness International Mobile station Equipment Identity (IMEIs), and IMSIs that can be tracked in base stations, RSUs,among clouds by the unauthentic third party.

8. Conclusion and Recommendations

Therefore, further research is essential for the actuation, sensor, boundary, and traffic layers to reach a such generic analysis result as in communication sublayers. Thereby, generic studies such as the one by Bhat et al. can be seen as the foundation while this chapter extends them by fine-tuning them to communication layer communication technologies after systematic identification. Moreover, it is notable to mention that the chapter did not involve any special security attacks based on innovative physical mechanisms or unconventional network communication technologies at the sensor layer [24]. Through proper use of advanced techniques for encrypting IoT protocols or new commonly established standard protocols or after the successful adoption of a comprehensive Intrusion Detection System, the proposal for a cognitive solution with these concerns would also be a further research in the scope of the chapter. Similarly, solutions based on AI technologies on the CPU or the hardware level, which would be added as future research, benefit not only from conventional network-based defense possibilities but also from further generic attacks that are very advanced far from the pure cyber-physical attacks on in-and outgoing information.

At the end of the day, 61 selected attack scenarios of the traffic, boundary, sensor, computation and communication layers of a vehicle were considered when presenting the cognitive threat vectors. For the most part (with a few exceptions), the given scenarios assumed the compromise of network communication. With that, the machine learning-trained and fixed-rule-based solutions proposed in this chapter for detecting cybersecurity threats in the V2X communication system and V2I communication system were primarily focusing on network communication vulnerabilities [20]. As a conclusion, they highlight just the network communications vulnerabilities of a V2X environment as possible causes for potential anomalous attacks. And indeed, the same can not only be said for the considered network layers but also for all the attack vectors of the significantly broader and more generic V2X layer spectrum. In this way, several other communication layer security research works analyzed in the systematic mapping study as well.

Cognitive Threat Detection Systems for Autonomous Vehicle Networks

8.1. Summary of Key Findings

This chapter presented the design of cognitive threat detection systems for cyber-physical systems enabled by autonomous vehicles, showing the focus in sensing and communication technologies. A cognitive threat detection system has been designed for cyber-physical

systems related to autonomous vehicles, for mitigating the security and privacy threats discussed in the previous sections. By maximizing the joint potential Obstacles/Cyber threats (OC) perceived by the drone and computing the entropies associated with these obstacles and cyber threats, the mission plan of an autonomous drone will be computed. The objective is to ensure that the perceived obstacles and detected cyber threats maximize the mission entropy, so that the final strategy takes the drone through regions of the greatest benefit (in terms of micro-satellite data) while avoiding known obstacles, as well as areas in which cyber threats have been detected. The proposed architecture raised new financial challenges and, specifically, the consequent requirement posed by the availability of financial resources significant for the calibration of the model logistic operations that must be carried out within the logistic operating regions, by the competence of the autonomous vehicles for dynamic decision-making each time aiming to respond optimally to the needs connected to economic prioritizations [4].

Autonomous Vehicle Systems are at a significant threat from cyber-attacks, mainly due to their connectivity and the sheer complexity of automotive systems in general. To mitigate these threats, a number of measures can be hesitated including strengthening cybersecurity of the car's software, implementing defense mechanisms for systems that support the vehicle, and providing cybersecurity protection(s) for V2X devices and skilled programs, so as to ensure the safety and security throughout the process of autonomous driving [2]. Due to promising benefits from the deployment of last-mile transportation automation supported on autonomous vehicles may pose the integrity and potential accuracy of the data being used that may impinge considerably on the security and privacy of services and thus users' personal data. Another challenge associated to adversary threats, taking actions directly on the drone to fulfilling its intended mission with highly attractive implications [5].

8.2. Recommendations for Future Research

Guaranteeing security in Autonomous Vehicle (AV) environments is a cumbersome mission that requires costly and time-consuming risk analysis and threat detection stages to maintain security for road users while still obeying the autonomy of the AVs [4]. This mission can be lightened if we detect and analyze threats as early as they appear in the system using the cognitive features of the AV nodes [10]. Various digital video streams are produced by different parts of the AV networks. These social distractions include texting, e-mail (such as

reading or responding to), social networking (Facebook, Twitter, Instagram, day managing applications, social games, etc.), watching videos, selfies (Snapchat, videos, Instagram, etc.), browsing (news, websites, etc.), or other. The classification of driving-relevant risks as AV drivers engaged in these social distractions, and based on the type of distraction's scenes captures, such as road, windscreen, dashboard, or rear view, is introduced in this work. In this study, the challenging problem of detecting cyber threats in autonomous vehicles is investigated. The novelty of the research rely on differentiating the vehicle's internal threats, such as fake messages, from social-driving related distractions, such as driver's normal talking. The first level of the proposed system is based on Modulation Identification using Power Spectrum (MIPS). The second level of the system is based on the learning model according to the average duration of variations between two equal objects. The robustness of the system was tested using a data collection of five different variants of a previously created dataset. Test results show an accuracy rate of 98.64%. The study focuses on eight different driving relevant risk types occurring at different rates in the dataset. For all of the driving relevant risk types, confusion matrices, categorization performances, and Receiver Operating Characteristic (ROC) graphics are also given.

References:

1. Sadhu, Ashok Kumar Reddy. "Enhancing Healthcare Data Security and User Convenience: An Exploration of Integrated Single Sign-On (SSO) and OAuth for Secure Patient Data Access within AWS GovCloud Environments." *Hong Kong Journal of AI and Medicine* 3.1 (2023): 100-116.
2. Tatineni, Sumanth. "Applying DevOps Practices for Quality and Reliability Improvement in Cloud-Based Systems." *Technix international journal for engineering research (TIJER)*10.11 (2023): 374-380.
3. Perumalsamy, Jegatheeswari, Manish Tomar, and Selvakumar Venkatasubbu. "Advanced Analytics in Actuarial Science: Leveraging Data for Innovative Product Development in Insurance." *Journal of Science & Technology* 4.3 (2023): 36-72.
4. Selvaraj, Amsa, Munivel Devan, and Kumaran Thirunavukkarasu. "AI-Driven Approaches for Test Data Generation in FinTech Applications: Enhancing Software

Quality and Reliability." *Journal of Artificial Intelligence Research and Applications* 4.1 (2024): 397-429.

5. Katari, Monish, Selvakumar Venkatasubbu, and Gowrisankar Krishnamoorthy. "Integration of Artificial Intelligence for Real-Time Fault Detection in Semiconductor Packaging." *Journal of Knowledge Learning and Science Technology ISSN: 2959-6386 (online)* 2.3 (2023): 473-495.
6. Makka, A. K. A. "Optimizing SAP Basis Administration for Advanced Computer Architectures and High-Performance Data Centers". *Journal of Science & Technology*, vol. 1, no. 1, Oct. 2020, pp. 242-279, https://thesciencebrigade.com/jst/article/view/282.
7. Pelluru, Karthik. "Enhancing Security and Privacy Measures in Cloud Environments." *Journal of Engineering and Technology* 4.2 (2022): 1-7.
8. Tatineni, Sumanth, and Naga Vikas Chakilam. "Integrating Artificial Intelligence with DevOps for Intelligent Infrastructure Management: Optimizing Resource Allocation and Performance in Cloud-Native Applications." *Journal of Bioinformatics and Artificial Intelligence* 4.1 (2024): 109-142.
9. Prakash, Sanjeev, et al. "Achieving regulatory compliance in cloud computing through ML." *AIJMR-Advanced International Journal of Multidisciplinary Research* 2.2 (2024).
10. Reddy, Sai Ganesh, et al. "Harnessing the Power of Generative Artificial Intelligence for Dynamic Content Personalization in Customer Relationship Management Systems: A Data-Driven Framework for Optimizing Customer Engagement and Experience." *Journal of AI-Assisted Scientific Discovery* 3.2 (2023): 379-395.