IoT-enabled Adaptive Cybersecurity Framework for Autonomous Vehicle Networks

By Dr. Soojin Kim

Professor of Computer Science, Gwangju Institute of Science and Technology (GIST), South Korea

1. Introduction

In the state-of-the-art, the main incentive is to provide secure, privacy-enhanced, authenticated and flexible functionalities of prosumer electric power distribution network by integrating IoT with blockchain technologies [1]. In brief, the high-level architecture of the vehicle-to-vehicle IoT includes in-vehicle communication with connected vehicle I/Os, decision-making intelligent gateway I/Os and gateway ECUs, connected vehicle backbone, service-oriented middleware, IoT smart services and public interfaces. Every node cooperatively offers secure and adaptive communication services using mutual cyber-security confirmations.

The automotive industry is increasingly embracing the paradigm of cybersecurity as a crucial decision-making parameter in the implementation of secure, safe, and dependable automated vehicle technology [2]. Because automotive networks are progressing from your standard CAN to Ethernet, a new milestone has been touched in the evolution, i.e., towards the modern state of in-vehicle communication: connected car architecture, decision-making power of gateways, tension between safety-critical nodes, and more.

1.1. Background and Motivation

In-library configurations and protocols significantly affect automobile security. The intruders exploit system vulnerabilities and inherent blemishes in protocols to escalate a successful cyber-attack. The demand for security in IVN is higher due to existing and future requests. In-Vehicle Networks use various communication protocols in different bus topologies. Classical protocols are an open book to unauthorized intruders through well-known

vulnerabilities like lack of message authentication, message integrity, identity theft, replay attack i.e., if an intruder captures a message, it can change the message or repeat it to the network without any additional authorization.

The automotive industry has undergone a remarkable transformation over the years due to the invasive exploration and application of the Internet of Things (IoT), particularly in modern vehicles. This transformation has paved ways for significant trends, most notably the advent of self-driving cars - a technological augmentation that promises better safety, traffic efficiency, and reduction in travel costs [3]. In recent years, autonomous vehicles (AVs) or smart cars with digital computer systems have been increasingly deployed in various shapes and platforms - making the automotive industry an important consumer of internet services [4]. Owing to their combination of electric, electronic, mechanical, hydraulic, and software systems, such vehicles are considered to be the most complex mechatronic systems in the IoT environment. The introduction of powerful tools poses an augmented risk of cyber-attacks that can lead to catastrophic consequences through remote manipulation [1].

1.2. Research Objectives

This new paradigm is also responsible for dealing with the security and privacy challenges of the connected and autonomous vehicle (CAV) ecosystem, underpinned by the internet of things (IoT) and the need for guaranteed connectivity, between vehicle to vehicle (V2V), between vehicle to infrastructure (V2I), between vehicle to anything (V2X), between vehicle to network (V2N), between vehicle to pedestrian (V2P). At the same time, the security threats are increasing due to all new digitalization trends, the number of connections of the CAV ecosystem, the data generated and transmitted by connected vehicles is huge and its security is equally challenging. That's why we need a robust cybersecurity framework [1].

Recent technological advancements in digital and communication technologies have made mobile Internet applications capable of providing not only in-vehicle and out-of-vehicle infotainment, personalized transport services, and other innovative value-added services on the move, ut also enhanced security in vehicular ad hoc networks (VANETs) in Intelligent Transportation Systems, following the U.S. Federal Communications Commission (FCC) 5.9 GHz Dedicated Short Range Communication (DSRC) frequency allocation and European guidelines for public safety applications over Cellular/Vehicle to Everything V2X purposes. This new paradigm may fulfill the demand of safety, lower risk of road accident by avoiding

accidents, an improved transport system, optimization of traffic light infrastructure, efficient toll collection, route planning, car localization, and even car-to-car orientation and platooning, yielding overall lower vehicle emissions. Moreover, vehicle connectivity technologies can offer value-added, location-based, and personalized services, like private insurance and third-party fleet management, gas station discounting or carsharing end-to-end solutions [5].

1.3. Scope and Organization of the Work

More knowledge-based trust management systems along with the security and privacy provisions have been introduced in References and. A model has been proposed in References to enhance the security and privacy of a vehicular ad hoc network considering the anonymous attacks. A blockchain-based security infrastructure is proposed in References here trust building between entities are dependent on the Past interaction data. Despite of many trust management models and issues presented in References and, the surveys, and stated,lack of comprehensive knowledge-based trust management in IoV.

For secure interactions between devices, SKP (SVC-to-REC Key Pair) based Softwaredefined Security (SD-SEC) model is proposed in References. Lateral communication security threats and vulnerabilities are identified and addressed in Reference that can be exploited in IoV networks. In References and, potential threats of the RAN (Radio Access Network) slicing technology have been discussed for the IoV services and applications with corresponding defense strategies, respectively. A comprehensive survey of 60 articles is carried out to summarize a state-of-the art of IoV trust management schemes to identify challenges and propose future research directions presented in Reference. A trust management framework to provide a beginner IoV network user with much trusted relation parameter between end vehicles, intermediate vehicles, and multiple level Roadside Units (RSUs) is presented in Reference.

An adaptive cybersecurity approach for IoV networks is presented in References?when the number of Wi-Fi authorized receivers is limited. IoT-enabled AVC ecosystem's real-world scenarios and their practical implications have been discussed in References. Interdependencies among security, performance, and trust scoring have been identified by studying existing IoV trust management approaches. An efficient and adaptable IoV trust management approach is suggested to quantify the trustworthiness of vehicles using number of direct and indirect parameters, considering different use case scenarios in References.

2. Fundamentals of IoT and Autonomous Vehicle Networks

It not only systematize the vehicular network attributes and identifies networking challenges in a self-driving network but also provides a basic methodology and design that carefully joins edge computing and IoT for connected and autonomous vehicles. A number of related issues are identified and discussed such as edge computing and IoT-enabled attacks, edge computing and IoT enabled threats mitigation schemes, attributes and networking challenges of IoT-enabled AVs, precision and cost tradeoffs on edge computing, fuzzy based edge learning, cognition, and IoT security for edge autonomy, and safety-centric edge enabled smart autonomous vehicles. To obtain these services, the novel functionalities of the edge computing are identified and adopted in autonomous vehicles, and a predictive mental model based on fuzzy theory was designed and implemented at the author's recent study [6]. The IoT-enabled and secure data acquisition, learning, and efficient cognition is proposed in smart vehicles. Furthermore, the standard summary of IoT-enabled edge cognition for smart vehicles and novel services were also introduced.

The Internet of Things (IoT) is a blend of real and virtual worlds helping in fine decision making with the help of computational intelligence. Autonomous vehicles also use IoT technology to step into the era of smart and autonomous automobiles. Autonomous vehicles are the fifth generation transporting systems consisting of a high end vehicle that can drive and monitor its environment without human assistance. It can be used for different operations like monitoring a map for route guidance or driving a vehicle without driver's assistance. It would be an intrinsic necessity for autonomous vehicles to obtain and analyze the surroundings and environmental data effectively, and taking decisions in real-time for secure networking infrastructure free from vulnerabilities. Therefore, an IoT-enabled adaptive security model is proposed in [7] for smart and autonomous vehicle networks that aims to guarantee secure, resilient, and safe operation of vehicles under these threats. The proposed model not only provides adaptability but also defense against the different types of threat models and an intelligent edge based decision module.

2.1. IoT Technologies and Protocols

The altered versions of industry-standard protocols and new essential protocols have been had to use in the right way with the existing IoT VANET communication channels like Wave2Car or Car2X [8]. These protocols are then adapted for multiple and high-level Dynamic host configuration protocols as a result of the small text information transfer;

Decentralized PKI and public key infrastructure have been proposed for detection, minimum, and communication devices of all the three layers in the context of naming devices for VANET nodes. Where the data with short limits, compression and the identity verification is important elements in and outside the vehicle when it wants to exchange data and information in an AV. So security measures and algorithms running on IoT devices inside an AV are considerable focus.

The inception of the Internet of Things (IoT) as a phenomenon has enabled the interconnection of anything that has computers or sensors with Internet facilities [9]. For autonomous vehicles (AVs), IoT plays a significant role as the AVs required to have IoT devices present in them for routing traffic and locality information. Various other features in an AV are dependent on IoT technologies that require interconnecting the devices in the vehicle with the rest of the network outside the AV. The technology that enables the communication of the sensors, vehicular sensors and actuators is VANET [7]. Short-range communications that are used for eco-routing for vehicle information sharing and vehicle-to-infrastructure (V2I) interfaces are the IoT channels that are inbuilt in the AV. They are used to retrofit the existing infrastructure or perform promotion of Vehicle2Vehicle (V2V) communications. Some usually raised questions about IoT for in AV arduous operations, synchronization of the IoT device, ensuring reliability, preserving data integrity, and security confinements.

2.2. Autonomous Vehicle Architecture

[10] An autonomous vehicle is a robot that is capable of moving without human input. Vehicles are classed as autonomous because they are capable of sensing their environment and navigating with little or no human input. Many such vehicles are being developed, some of which are ready for testing and deployment. The level of artificial intelligence in autonomous vehicles varies. The physical architecture and the role of sensors, fusion, and heterogeneous sources play a crucial role in achieving a reliable autonomous GPS location.[7] The data flow from autonomous vehicle sensors to autonomous driving ... dynamically contacts heterogenous linked data sources over the Web in order to build up a rich knowledge base about context that is of relevance for the vehicle itself. Autonomous vehicle networks are a key part of Intelligent Transportation System (ITS) and work together in an ad hoc manner to fulfil traffic demands (e.g., an intersection-based autonomous vehicle control system). Research has shown that the performance of autonomous vehicle networks could be very helpful to minimize the collision rate, traffic jam, fuel consumption and result in the saving of

time of all road users. The vehicle could produce and consume a huge amount of data without any interaction of the vehicle owner or driver perspective. Autonomy is achieved through self-regulation and thus the vehicle can provide high efficient and reliable services, in general, without human interaction.[11] Moreover, intrusion in critical mission of an autonomous vehicle has led various consequences as the vehicle is no more able to move or participate in a convoy/pattern until and unless brought back into a normal/mission mode that could be only possible after removal of attacked over some compromise modules or may be by installation of new modules that does not already come under attacked category. All these attacks and intrusions are identified on the bases of the properties of adversaries/hackers to degrade or manipulate with the sensing, decision making and the movement phase of the vehicle. An autonomous vehicle is an important electronic innovation in which the vehicle can run itself based on learned policies and support. There are lots of sensors, systems, and communication modules fitted in an autonomous vehicle that make it an essential social element.

3. Cybersecurity Challenges in Autonomous Vehicle Networks

To address the above-mentioned susceptibility in autonomous vehicle networks, we design a cybersecurity framework to protect against perceived malicious behavior [11]. To develop the proposed framework, we specifically identify and categorize the current cybersecurity challenges affecting the autonomous vehicle network. We also identify these challenges based on different levels of autonomous vehicles (L1–L5) and propose a feasible cybersecurity framework capable of deterring against diverse attacks generally relevant in the ecosystem of AV networks. The cybersecurity framework will make autonomous vehicles safe and trustworthy, such that it can be utilized in different mission-critical domains where certain risk factors exist. Therefore, the proposed cybersecurity framework can be used in vehicle-to-vehicle, vehicle-to-infrastructure, and vehicle-to-everything communication in emerging networks and towards a level 5 smart city.

Autonomous vehicle networks are prone to diverse cyber threats, including hacking, privacy breaches, network congestion, service theft, and data manipulation. Therefore, it is important to design a robust cybersecurity framework to overcome the associated security mechanisms and enable safer and more secure autonomous vehicle networks [12]. Automotive systems consist of multiple electronic control units with different network architecture types. Securing

autonomous vehicles against cyber-related threats is becoming increasingly challenging. Hacking, privacy breaches, network congestion, location tracking, service and data manipulation are threatening autonomous vehicles [3]. Furthermore, fully autonomous vehicles rely on embedded systems and wireless technologies, such as 4G Long Term Evolution (LTE) and 5G, to maintain network and internet connectivity. These innovative technologies introduce new vulnerabilities and open up novel attack vectors. Robot Operating System (ROS) Manipulation, LTE jamming, and Motion Control manipulation are malicious acts that are harmful to autonomous vehicles. As a result, the vulnerability of autonomous vehicle networks is becoming a serious impediment to the wider adoption of autonomous vehicles in different domains.

3.1. Vulnerabilities and Threats

In autonomous vehicle networks (AVNs), multiple security threats put considerable tension on network-operations. In general, identity theft aims at user participants, device hijacking is targeted at the hardware, and various data theft is inclined towards exchanging shared- and non-shared information across device-border semantics. Apart from the security threats like brute force attacks to hack user-components, miscellaneous malware, spyware, back-door attacks and network-level threat such as, jamming, wormhole and fragmentation attacks are to be concerned about. Moreover, security problems may also infect data accuracy, integrity and reliability and then possibly induce financial vulnerabilities and consequences. Despite theoretical assertions, these security vulnerabilities materialize in an easy-to-use vehicle ecosystem platform (like CAV) due to open data sharing and automated authority delegations.

[13] [11] The current cybersecurity framework is not entirely compatible with the emerging IoT environment and leaves with several vulnerabilities [14]. The primary reason is the growing number of connected devices that continuously produce a significant amount of data. Moreover, for an intelligent system and network, data sharing and providing on-demand or automated connectivity facilitates the exploitation of the system structure. Hackers exploit the integration of complex systems and IoT. Additionally, privacy threats to the Autonomous vehicle networks (AVNs) encompass risks to operational relations between the distinct components in an AV, various interactions of AV-systems across a public road, changes in the service lifecycle, potential data theft, device hijacking, unauthorized payment methods, as well as personal data of connected citizens. Thus, trust and collaboration pursuit among the

command, control, and managing units and human-driven road-users have been propounded to be several of the security problems in non-traditional use-cases such as autonomous shared mobility (SH-autonomy), supply-chain information exchange, health data, distributed energy management, smart-city, swarm-robotics, edge intelligence, specifics on the coverage-area, AR/VR and beyond.

3.2. Existing Cybersecurity Solutions

The key to cybersecurity is not adding stronger locks on the gate but making the attackers face the bear once they are inside [15]. However, there are currently no known high-quality metrics for evaluating the robustness of cybersecurity measures in an end-to-end approach. Although there is a range of measures available in the literature, including simulation, mathematical attacks, penetration testing, and self-play, research indicates that the polar nature of attacks in automotive cybersecurity often reduces the effectiveness of these typical evaluation metrics [11]. Security and intruder detection improvement enabled by IoT in A-CySeF has never involved user devices. [8]. Many cybersecurity solutions have been developed all targeting different security attributes of the network and vehicles, such as intrusion detection, intrusion prevention, and data authentication. Each of these solutions is designed for an isolated security attribute and works in silos but fails to address security needs throughout the lifecycle of a vehicular network. Cross-layered security solutions have seen significant success in recent years. However, these solutions still fail to adapt to evolving threats and escape the bear once the gate is wide open.

4. IoT-enabled Adaptive Cybersecurity Framework Design

As autonomous vehicles are soliciting increasingly wide acceptance as a topic of interest in both academic and industrial landscapes, it is strongly believed that publicly accessible estimates and reconstructions should always be based on consistent scientific and practical approaches. In an effort to address key uncertainties and stimulate industry involvement in security research of autonomous vehicles, this article emphasizes on the preparation of a risk analysis methodology. The approach centers around the concept of cooperative, intelligent transportation systems to facilitate the automotive industry to implement the benefits of vehicle-to-vehicle, vehicle-to-infrastructure and vehicle-to-other communications. Following this methodology, an ad-hoc risk analysis study of the introduction of fully autonomous vehicles in the Dutch urban and non-urban areas and highway traffic was conducted,

suggesting a level of quantitative and qualitative risk estimates for a variety of security threats related to direct communication and interactions between autonomous interconnected vehicles. The conducted risk analysis study has led to a set of prioritized security threats and a call for the industry to address key security problems with specific countermeasures and ETSA standards.

In spite of technological advancements, the contemporary world is vulnerable to cyber-attacks due to its highly wired infrastructure. With the advent of Internet of Things, the cyber threat becomes more vulnerable to a variety of attack vectors. This article articulates the deployment of cloud computing and machine learning to develop an autonomous, artificially intelligent antivirus framework for vehicles aiming to combat cybersecurity threats. Specifically, the study demonstrates the integration of cloud computing, machine learning, Android security, and security vulnerabilities to create an artificially intelligent system that enhances the security of connected vehicles through various mechanisms, including analyzing of artificial intelligence and machine learning models, big data collection, feature transformation, cloud computing, business intelligence, risk analysis tables, hidden and undetectable processes, and response. Subsequently, the neural network mechanism related to TCP and User Datagram Protocol-based AAA anesthesia modeling and cyber-attack modeling is used to to train and test the proposed framework.

4.1. Key Components and Architecture

The cyber-physical vehicle security framework is developed by implementing high-secure communication and control modules. In a secure in-vehicle network, various parts of a vehicle require secure communication and control. It is essential for electronic control units (ECUs to be updated, and for the connected smartphone/advisor to enable the updated ECUs to communicate and process secure transactions in real time. The high honesty in terms of data and communications security with both drivers and cars is necessary for healthy communication within internal and external systems. Based on the designed architecture for mobile devices and the infrastructure proposed in the "IoT system for network interaction and control", cyber systems and their interfaces are used within vehicles, between vehicles and systems, and between controllers and AVs located at a base [4].

Sensors and embedded components in autonomous vehicles (AVs) are performing secure real-time navigation and control, and high-level security algorithms. In AVs like automated

cars and flying devices, it is impossible to handle such critical tasks in a single integrated computing environment. Most sensors and components of the target vehicle are connected to IoT devices for communication and control purposes. With a high processing capability and an array of sensors, drones and autonomous cars are considered mobile computing and sensing environments. For safe transportation and traffic control, AVs also use communication and broadcasting components. The new architecture formulated constitutes a software, hardware, and secure data communication, thus making it is possible to support various networks, sensors, and devices in the IoT environment [9].

4.2. Machine Learning and AI Techniques in Cybersecurity

The work presents an AI-and-ML-based MI-FWIDS security solution that effectively manages security threats targeting advanced vehicular networks as a novel and efficient architecture for enhancing the security of high-level system operations. The detailed two-phase mechanism developed for MI-FWIDS consists of a layered security architecture where both successful and failed requests are managed using appropriate AI-based monitoring science. The security enhancements across the entire vehicular and infrastructural chain and the trade-off between MI-FWIDS security effectiveness and computational complexity were analyzed through extensive long-term simulation scenarios mimicking driving situations and current and future intelligent transport system exploitation. Then, unfortunately, the fast and unpredictable velocity of mobile nodes makes it impossible to apply these existing models to security applications.

In recent years, the use of machine learning and other AI techniques has shown strong potential for implementation in the cybersecurity of networks which are subject to typical attacks and various types of cyber-physical security threats [3]. For instance, a security framework based on AI reporting to identify advanced security threats that targets your vanet with high precision [9]. Particularly, in wireless VANETs, requiring robust security schemes that directly protect system functionalities, such as autonomous driving, quality of service for communicating cars, coordination of infrastructural units rather than just detecting security violations created at the edge nodes of the network, which is the focus in most current research. The authors of set the novel tradeoff between the high accuracy of security detection and the low overhead required by the same security scheme using advanced AI [16].

5. Implementation and Evaluation

The cryptographic model of the Platooning as well as the definitions of the abstracted SCV-type-based Abstract Platooning and the evolution of a platoon are the simplified versions from [a full version of the paper will be published in Personal and Ubiquitous Computing] [17].

Both of the given road mobility instances simulate two continuous flows of vehicles, which start and end in specific geographical regions of the simulated city. The data was generated using the Vehicle Trace and Mobility (TraffikLab) series, which is primarily based on traffic data from the Swedish Transport Administration (Trafikverket), here and after referred to as the SLO-Traces'12 and SLO-Traces'14, and provide complete vehicle trajectories. The traffic flow is generated by means of inserting and removing vehicle traces every 300 s, for every 100 s of summed up simulated time. The traffic flow rate is thus either 3 or 2.5 vehicles/ s. Randomly chosen vehicle traces are deleted and inserted in lists that simulate entering or leaving the simulated area, lists at a fixed time delay.

In this section, we provide the experimental settings and procedure used for the IoT-ACAV security adaptation experiment, followed by the performance evaluation and analysis based on the experiment. The data sets and messages for the vehicular communication were generated using road mobility instances from the Galileo repository and will be made publicly available. A municipal setting was simulated by running SUMO in the periodic fashion, assuming different traffic flow. The collected data was processed to simulate dynamic changes of traffic flow [18].

5.1. Prototype Development

The platform generates a signal for the EDR component when it detects a wrong behavior of certain vehicle architectures, like a car2vehicle device or a cyber-physical component such as the gateway with the ignition status. The KPI Service is implemented on a dedicated architecture, and it is able to communicate with other architectures and with the vehicles. In case of an anomaly detection, the KPI service sends all the details to the Event Handler for further investigation. In order to effectively manage the entire system, there is also a Metadata, which contains the KPI definition details, and Access Control List mechanisms that manage the access to REST and MQTT interfaces. The Metadata Service communicates with all the

other services to keep an updated status of all the status and relevant information about the KPI [19].

The developed security framework, depicted in Section 3, has intermediate components acting as security barriers that communicate via the PubSub system. The security services that are available via these barriers, namely intrusion detection and prevention, and security auditing, are performed from the physical, network, vehicle bus and architectural levels. Domotics applications on the in-vehicle network may provide intuition about the user's status and/or behavior, so they can give useful information to the cybersecurity process. Another system is added to the framework as a support for the implementation of all sorts of predictions, Node-RED. A connection between the LINC layer of the security framework, and a Node-RED instance, is carried out through the aforementioned PubSub system. Furthermore, the security framework is also interfaced with application software that provides a web GUI for End-Users [2].

5.2. Performance Metrics and Evaluation

To satisfy the security requirements of devices, the IoTCyberVANet framework goal for vehicle communications is to ensure incurring zero losses to the vehicle users, and therefore, zero network packet delivery losses, zero vehicle-unavailability duration, and zero fault tolerance ratio are desired to measure the KPIs [20]. The performance indicators must be designed in such a way that soon after the occurrence of an anomaly, the vehicle switches to another security level, either a reboot of the affected application or a whole-vehicle reboot, as described in the architecture [21]. A Markov process best serves in this case, and DMZ can act as a trigger factor to effect the change in the security level of the vehicle.

A performance evaluation of the IoTCyberVANet framework is presented in this section [22]. Since the focus of our IoTCyberVANet framework is security, we define the performance of the IoTCyberVANet framework using two types of key performance indicators (KPIs): reliability/availability KPIs and security KPIs. The reliability/availability KPIs of the IoTCyberVANet framework should be evaluated according to the requirements of the expected traffic performance regarding end-to-end communication links. In the proposed framework, a co-design algorithm for robust and secure route management needs to be evaluated in terms of these KPIs.

6. Case Studies and Use Cases

All of assaults are fore-warned by the training dataset, i.e. they are zero-day attacks which possess a dangerous novelty type but driving these attacker autonomously for every dataset data with a mean cost without a loss. All malware types, at least five offers including Ransomware, Scareware, Trojans, Worm, RootKit, Cryptocoin Miner, and others like Honeynet and Diamond (Peacock), that impact devices' operations. Additionally, this section all metrics were calculated to improve the learning procedure and analyzed by the results section. Hence, we profile guardian actions of the network using zero-day labeling and are performed an OMI stress test [19].

Reference and present studies for vulnerabilities that are found in systems of autonomous connected vehicles and show that it is crucial for users to prioritize security in the design and development of autonomous vehicles. However confining the need for security in connected vehicles to these studies is not comprehensive because the demonstration of attacks and litigation towards autonomous connected vehicles are almost non-existent. This paper attempts to fill this gap. It will contribute to a better perception of autonomous vehicles by identifying, through looking at many articles, the most current available knowledge summarized in terms of attacks and their types, triggers, solutions and compromises through revealing possible attacks in autonomous vehicles, exploits, and vulnerabilities in the broad spectrum [23]. Simple attacks that can be done by IoT devices via interconnected services are encroachment, snatching, and halting other devices, creating a black hole between the device and the other device, mutating and interrupting the existing communication, and applying IP geolocalization. Due to the sensitiveness of autonomous vehicles there is dozens of intrusions and not limited for the fore-named. Customer diagnosis and upgrading. Another OT1 action that could ruin the company activities belongs to abnormality detection and diagnose, updating, deactivation or activation thereof. Out-of-scope attacks are targeted scenarios that direction the autonomous vehicle, e.g. in extrinsic path attacks. Beside to the normal traffic to some services of the client, multimodal attacks directed to an autonomous vehicle such as impersonation, service blasting causing timeout in availability, thanks to an overloading of the onboard resources (e.g. overuse of the CPU), are made.raficiary spends about 9 times more money when securing corporations.

Autonomous vehicles have the potential to transform transportation into a service with direct impacts on the local environment and infrastructure, and other health and life domains. As

such, an entire new industry was created to make the product offering in terms of transportation services and one of the main challenges faced by all the stakeholders is the cybersecurity. The goal of this paper is to propose a data-driven cybersecurity approach, applicable in the context of autonomous vehicle networks, and involves the development of various machine learning models and techniques for real-time dynamic security monitoring and adaptive decision-making based on Input/Output (I/O) abnormal patterns in the context of the vehicle network. One of the Kubernetes examples is the AICamp project, which is an open source effort from a number of companies like Linaro, Facebook, and Arm to automate the process of installing, managing, and maintaining AI and machine learning applications in edge devices, thereby enabling network edge AI technologies and making it easier to deploy ML applications in any type of infrastructure. The concept of a data lake, a shared data environment with comprehensive security and governance management, which simplifies data management, is part of the Industry 4.0 drive and has been the focus of recent research. A data lake is a repository that allows for storage and analysis of large volumes and variety of data coming from various sources. It creates common business goals and regulatory data sets by unifying different types of data [16,17] Throughout the life-cycle of connected vehicles, the fleet data has a unique potential to transform the ways they provide transport services, and it will become important to manage this data efficiently by considering infrastructure, capabilities, trustworthiness, and regulations. [12] The intention of this paper is to provide real world business uses of adaptive cyber security powered by data lake with big data analysis against auto sharping cyber attacks to answer below questions: 1) how to profile cyber-attacks and threat actors; 2) how to develop adaptive data-driven network cyber security infrastructure?; and 3) what are the data lake policy levels that are critical to save the fleet data For this situation, we suggest a model that is set empowered by a data lake for threat detection to unveiling cyber-attacks that have some similar sequences, or to novel attacks that cannot be found in the annotated data. Minimization at System Integration Process (SIP) in Advanced Driver Assistance System (ADAS) development is a crucial process that reduces unforeseen risks compared to traditional prototypes for testing. Thirdly, we suggest to minimize fuel usage, recover energy, and balance power growth in ECO strategy in order to avoid desynchronization related to the use of energy (Eng) and the recovered energy (Rec). According to the first question: how to profile cyber-attacks and threat actors? Our results suggest that three archetypes of APT21 actors are e-Shop Prince, Trader Tito, and Tech Titan. We unveil a variety of manually written LeafPad, Star Office and PocoMail artifacts. The OOD

image sets contain the cyber-attacks generated by malicious users who are not in the training set when they are tested with continuous deployment.

6.1. Real-world Applications

Connected and autonomous vehicle technologies are an attractive solution to social, environmental, and mobility problems. Nevertheless, in recent years, connected car technologies have been increasingly targeted by various cyber-attacks that are becoming more sophisticated over time. These threats often exploit the use of wireless communication, and encompass a wide range of problems that need to be resolved. The CAN bus protocol is a particularly enticing target, because it has been adopted as standard by the majority of car manufacturers as an easy and fast way to communicate data inside the car. Meanwhile, the security settings required to handle it properly are left to the discretion of car manufacturers, who often overlook this crucial aspect. This creates an obvious weakness in the communication protocol itself [24].

Connected and autonomous vehicles face a high risk of cyber-attacks. Traditional vehicles transfer data wirelessly, through which cyber-attacks can penetrate to exploit the vehicle's internal network by using the CAN bus. Security risks to vehicles are also introduced due to changes in communication between vehicles ('V2V'), between vehicles and Roadside Units or Edge Gateways ('V2I'), and to internet services ('V2X'). When these credentials are vulnerable, the managed ln-Vehicle Cyber-Physical Internet of Vehicles protocol suite (iVero) can detect and prevent unauthorised traffic piggies leading to stream reflection attacks. iVero can also manage credential management including attribute establishment and distribution [6].

6.2. Success Stories and Lessons Learned

In this section, we present the implementation and deployment of two systems and two cybersecurity testbeds. A testbed for automotive systems that ensures Time Sensitive Networking and Time Sensitive Audio Video Bridging, and a Low Power Wide Area Network infrastructure that can be used as a reference model for smart city systems are deployed [19]. For this, a threat analysis of LED-based LiFi data communication technology is performed to expand existing research in the context of LED based LiFi data communication standards. Furthermore, the vulnerability analyses of WiFi, Bluetooth and LTE data interfaces were performed in the green IT lab. Further, two cybersecurity testbeds are implemented and available for research. The first testbed is used for security analyses of vehicular

communication networks and uses multiple LEDs for LiFi connections. The second testbed is used for cyber threat analyses of wearable IoT device.

The success of an autonomous vehicle system of the Internet of Things (IoT) ecosystem depends on successful deployment and performance of their IoT devices communication networks. While there are numerous success stories for IoT system deployments [25], autonomous systems present specific challenges to be addressed such as malfunctioning sub-systems like sensors, and power supply. If these challenges are not overcome, an autonomous vehicle will not be deployable, reliable, and safe. For this purpose, new Security Management (SM) challenges in all the layers of the OSI model have to be addressed, which are specifically presented in Section 3.3. A model that describes how these challenges can be met is the Resilient Model for the Internet of Things of Cyber Physical Systems [26]. It describes the resilience concept at the application, architecture and network levels, and presents the state of the art of anomaly detection and power-efficient solutions in the research literature that can be used to address the described interruptions in Non-Resilient Architectures (NRAs).

7. Future Directions and Research Opportunities

Cybersecurity is widely regarded as one of the most important issues for IoV [23]. As a result, there is a need for additional research aimed at making IoV more secure, trustworthy, and reliable by designing a solution that is capable of detecting malicious security threats toward IoV and neutralizing them through effective, efficient, and timely response mechanisms. Similarly, researchers should improve autonomous vehicle security by developing novel security mechanisms such as adaptive and intelligent trust management mechanisms that address the massive data sharing and processing, connectivity issues, and machine-to-machine interaction needs of autonomous vehicles. This is particularly true for networks with very large numbers of vehicles that must ensure data confidentiality, integrity, and authenticity as well as availability, accessibility, and accountability at all times.

The existing research within this domain is mainly focused on intelligent decision making at an individual state level within any such system. Intel requires optimum collaboration among different devices throughout an IoT environment in order to generate a fuller picture of the environment. For example, a threat identified by a Lights Out Management (LOM) server system may seem to be a remedial rather than a critical threat; but when collectively addressed by the IoT environment, that may prove to be an absolute threat. This example is useful as an

evaluation of the need for SOC as a basic postulate within a secured IoT environment represents an encouraging domain for research [27].

Cybersecurity is an appropriate area for future research given that it is evolving dynamically [28]. A bulk of existing research focuses on developing new detection mechanisms for security breaches and cyber attacks. Researchers are currently seeking to transform design-time and run-time mechanisms to embedded systems that observe not only environmental reality but also the intentions of adversaries. As a consequence, concepts such as co-evolution are surfacing, with an increasing awareness of the need to provide natural extensions to current technologies. These extensions are required to not only evoke adversarial intent, but to disrupt or deceive them. The cradle of research for IoT security remains in traditional Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) that are widely used across different domains from cloud networks to mobile devices.

7.1. Emerging Technologies

Cyber-physical systems emerge as an area of interest due to their interdisciplinary nature and widespread adoption in various application domains, such as smart grid management, smart cities, industrial production, road traffic safety and management and many others. There is an increasing interest in securing cyber-physical systems from various kinds of threats and malicious activities. The existing techniques for securing cyber-physical systems are mainly design and engineering oriented. The focus is on providing solutions that capture the areas or the layers in the system where attacks could manifest. The system is viewed as a set of interconnected nodes and the focus is on studying the network structure to capture vulnerabilities of the network. The design and engineering aspects are insufficient from theoretical and practical standpoints. Our study and analysis did not bring up the effective defense strategies that can be employed in practice to address the attacks that are mediated through the physical layer. Physical layer attacks are in effect passive, and hence not carried out on the information communicated over the network to disturb the normal workflow of the system; they violate fundamental assumptions of operational adaptability and thus necessitating an adaptation method that is secure against the physical layer attacks [29].

Emerging technology in IoV platform integrates blockchain, machine learning, artificial intelligence, blockchain to eliminate the challenges of security and able to provide a secure platform for IoV. Blockchain technologies will be the best solution to maintain the security,

privacy, and data integrity of IoV platform. With the growing popularity of IoV applications like the Internet of Vehicles, automated vehicles, and other vehicular applications, we anticipate that the platform will be one of the key components and as challenging issues will continue to grow in terms of scalability, security, and privacy, there is still significant ongoing research trying to provide solutions. Apart from it, vehicles are required to communicate securely, and compliance with blockchain technologies carries out the secure communications amongst vehicles, nodes, and the transportation host, therefore ensuring secure vehicular networking communication [30].

7.2. Policy and Regulatory Implications

The roadmap for Cybersecurity in Autonomous Vehicles [3] identified the major distinctions between Autonomous innovation, Intelligent technology, software development, cybersecurity, and power industry – with the use of autonomous technologies the increasing security and safety concerns could also be likened with the reforms or certain points of reformation in the existing systems. The enhancing and grooming up of new ATS invariably impose supplemental security and policy measures. These steps are both on-the-road and on Cyber front. Again this is the fact that the various industries are carrying out the activities involving automotive ATS. This research introduces a framework for a Cybersecurity model for Intelligent Adaptive Systems, which provides a research direction and which can assist the experts to come out with some feasible measures in the context of designing Cybersecurity laws and policies for ITSs.

Securing Autonomous Vehicle Networks is a fundamental requirement for their safety and commercialization. With the increasing dependence on intelligent and autonomous features on vehicles, it has become essential to register the major distinguishing aspects and features that call for policies and regulation formulations. This encourages Cybersecurity experts to come up with the policies and regulations for such ITSs, keeping in view the Cognitive factors, so that the ITSs may be adopted with full heart, and necessitate the ways of educating the users regarding these different features [11]. What need to be done in the area is identifying the potential risks posed and adapting the existing legal and regulatory frameworks to protect these emerging autonomous vehicle technologies from cybersecurity threats.

8. Conclusion and Final Remarks

[9] The Internet of Things (IoT) has brought about significant advancements in the field of autonomous vehicles. It has also led to the digital transformation of automotive systems by facilitating the seamless data exchange and real-time decision-making capabilities. While these developments are invasive and appealing from the user perspective, they have also introduced cyber-physical system security issues. Ensuring the security of autonomous vehicle networks involves securing the information moving through different layers of communication in-vehicle networks. This paper proposes an exclusive Intrusion Detection System (IDS)-based In-Vehicle Network Security framework for autonomous vehicles known as IoTACyS, which portrays enhanced security measures at the data and application layers. The IoTACyS framework is developed using the Simulink environment, and the performance of the proposed system is evaluated using some highly sophisticated cyber-attacks such as denial of service, remote to return controls, man-in-the-middle and external attacks.[2] This paper proposes a new security framework known as IoTACyS (IoT-enabled Adaptive Cybersecurity Framework for Autonomous Vehicle Networks). The proposed IoTACyS framework is devised using the powerful and versatile as well as widely used mathematical tool known as machine learning. This machine learning algorithm, namely; Hidden Markov Model, effectively scrutinizes the inputs from the controllers placed in the execution environment, in order to identify the behavioral discrepancy in their activities. Furthermore, the paper defines and prove the QoS (Quality of Service) of the proposed model routes. Each of them validates its effectiveness as well as its adaptability to significantly minimize the occurrence of the breakdown. Additionally, the paper contains the implementation of the Hidden Markov Model on the execution controller of the system. In the IoTACyS framework, the car along with each engine processes the real-time data of the incoming controller requests and other potential suspicious activities.

Reference:

1. Perumalsamy, Jegatheeswari, Bhargav Kumar Konidena, and Bhavani Krothapalli. "AI-Driven Risk Modeling in Life Insurance: Advanced Techniques for Mortality and Longevity Prediction." *Journal of Artificial Intelligence Research and Applications* 3.2 (2023): 392-422.

2. Karamthulla, Musarath Jahan, et al. "From Theory to Practice: Implementing AI Technologies in Project Management." *International Journal for Multidisciplinary Research* 6.2 (2024): 1-11.

3. Jeyaraman, J., Krishnamoorthy, G., Konidena, B. K., & Sistla, S. M. K. (2024). Machine Learning for Demand Forecasting in Manufacturing. *International Journal for Multidisciplinary Research*, *6*(1), 1-115.

4. Karamthulla, Musarath Jahan, et al. "Navigating the Future: AI-Driven Project Management in the Digital Era." *International Journal for Multidisciplinary Research* 6.2 (2024): 1-11.

5. Karamthulla, M. J., Prakash, S., Tadimarri, A., & Tomar, M. (2024). Efficiency Unleashed: Harnessing AI for Agile Project Management. *International Journal For Multidisciplinary Research*, *6*(2), 1-13.

6. Jeyaraman, Jawaharbabu, Jesu Narkarunai Arasu Malaiyappan, and Sai Mani Krishna Sistla. "Advancements in Reinforcement Learning Algorithms for Autonomous Systems." *International Journal of Innovative Science and Research Technology (IJISRT)* 9.3 (2024): 1941-1946.

7. Jangoan, Suhas, Gowrisankar Krishnamoorthy, and Jesu Narkarunai Arasu Malaiyappan. "Predictive Maintenance using Machine Learning in Industrial IoT." *International Journal of Innovative Science and Research Technology (IJISRT)* 9.3 (2024): 1909-1915.

8. Jangoan, Suhas, et al. "Demystifying Explainable AI: Understanding, Transparency, and Trust." *International Journal For Multidisciplinary Research* 6.2 (2024): 1-13.

9. Krishnamoorthy, Gowrisankar, et al. "Enhancing Worker Safety in Manufacturing with IoT and ML." *International Journal For Multidisciplinary Research* 6.1 (2024): 1-11.

10. Perumalsamy, Jegatheeswari, Muthukrishnan Muthusubramanian, and Lavanya Shanmugam. "Machine Learning Applications in Actuarial Product Development: Enhancing Pricing and Risk Assessment." *Journal of Science & Technology* 4.4 (2023): 34-65.