Cyber Threat Intelligence Sharing Frameworks for Autonomous Vehicle Ecosystems

By Dr. Yan Song

Professor of Computer Science, Nanyang Technological University (NTU), Singapore

1. Introduction

Vehicular CPS has undergone a rapid growth and several leaps of technology including autonomous vehicles (AVs), intelligent transportation systems (ITSs), and connected vehicles [1]. This has led the transportation landscape to have a broader impact on society, playing critical roles in the economy, security and privacy. VCS focuses on EVs, as a particular category of connected vehicles, which are directly integrated into the V2X (Vehicle to Everything) communication alongside the rest of the networked sacred and end-user equipment (UE). In this direction, it is pivotal to highlight how fundamental it is to secure VCSs from their introduction phase. These threats must be timely and effectively addressed to foster adoption and diffusion of VCS; on the contrary this will not be accepted by potential consumers, which will deem such a solution an unsafe approach.

Attackers can use stolen user information to launch more effective socially engineered attacks in intelligent vehicle (IV) ecosystems [2]. These adversarial attacks, if successful, can lead to financial and personal information being deleted, exposed or stolen. Thankfully, it is possible to accurately identify and block rogue access and data in intelligent vehicle systems by applying context and computing the change in user behavior to discover unusual activities. However, tamper-proof AI algorithms are vulnerable to adversarial attacks, which can result in confusing AI algorithms and potentially cause failure across vehicle subsystems. Bypassing or deceiving the RF spectrum monitoring, the first stage in distrusting attacks can potentially trick an intelligent vehicle ecosystem (IVE) system and allow a hacking device to stay under the radar, without being detected [3].

1.1. Background and Rationale

Thus, the Type-Approval (TA) of the SAFETY-critical cyber-electronic (CE) system has to align with the functional development of the Cybersecurity Management System (CSMS). As a real-life motivating example, the Volkswagen Saga is an apparent one where the automotive company never approached the cyber-governance in a programmatically inclined fashion. The group came up with the blueprint which included 'a central and outer core security council and a ceiling of innovative and agile sub-committees, stretching till the lowest level of plant operability'. Now, with the consideration of both the automotive functional cybersecurity methodology E/E/Architecture design and the governance (Volkswagen) as reference case study and references from various international experiences, provided are the novel State-of-the-arts for the delayed cyber resilience as due to the flaws in automotive component pertaining to electronic and electric architecture. The electronic and electronic architecture (E/E/Arch) models prevail below the Automotive Systems Engineering (ASE) which the Intellectual Property (1P), Functional Safety (FS); Cybersecurity (CS) E/E/Wiring architecture paradigms. A set of Kinetically-Inspired (KI), Algorithm-Empowering Enterprise Management System (A2EMS), and Cloud-AI-CPS powered tools using Machine Learning (ML) algorithms are used to recover the delayed production-controlled industry 4.0 inspired cyber-resilience [4].

The transition from conventional vehicles to Autonomous Vehicle (AV) systems fundamentally changes the concept of mobility, driving experiences, and the landscape of business models. AVs come equipped with a various set of sensors, such as LIDAR, camera, radar, ultrasonic sensors, and provide navigation and collision avoidance solutions using the fusion of these sensor data with the help of intelligent computing platforms. As the onboard electronics and computational resources increase manifold, the hardware and software architecture of the vehicle systems have undergone continual changes to enable a fully connected ecosystem without any driver or user intervention [5]. However, modern software is rarely driven through devoted code development in the Connected and Autonomous Vehicles (CAVs) and moving towards "agile" based solutions overlapping the domains of Advanced Driver-Assisted Solutions (ADAS) and Connected and Autonomous Vehicles (CAVs). This feature-gap can be an open play field for hackers who can exploit the imperceptive software kernels to achieve real-time remote vehicle control, i.e., Sybil/ MiM attacks for enhancing the Extraction of Sensitive Information (EoSI) with general adversarial network based methodologies in support for the 'fake data overlay attacks' over the internal part of the automotive sensors [6].

1.2. Scope and Objectives

Nowadays, cyber security threats and cyber-attacks are increasingly more significant and attract progressively more attention, especially related to the issues of self-driving vehicles. Autonomous vehicle systems are so-called safety-critical cyber systems, that are vulnerable to cyber threats which can change the normal behaviors of its public facing interfaces, such as control systems, sensors, cloud systems, remote services, and internet connected devices. The detection of these threats is the starting point of proactive threat intelligence management in interconnected cyber systems. In the scientific and technical literature, there are different but similar management information systems, such as threat intelligence sharing mechanisms [article_id: 17cdbba4-58bd-4a78-a210-a6ab52e4f535] (TISM), cyber threat intelligence management systems, and cyber threat intelligence sharing frameworks (CTISF). The essence of the investigated research topic is as follows: Mining improvement opportunities in cyber threat intelligence data fusion for sharing, analysis, and decision making in the form of threat intelligence sharing and management systems, is a novel and growing branch in the field of cyber security research. This leads to several principal scientific and engineering problems.

The scope and objectives of our study are outlined with reference to [article_id: 80046a9d-e000-4c5e-a223-712cf6f394c7] and [article_id: 08b7caf0-fa36-45f4-8dd8-a59ce9ded440]. Our research deals with the study of different Cyber Threat Intelligence sharing frameworks for Autonomous Vehicle Ecosystems. This text will be focused on the following 3 main objectives. The first objective is to identify state-of-the-art C-TISF for AVE and highlight the capabilities and gaps of these frameworks at both the technical and business levels. The second objective is to identify and analyze strategically important information sources that contribute to enhancing the capability of a C-TISF for AVE. The third objective is to identify and analyze important future technological innovations which have the potential for empowering a C-TISF for AVE. This study will significantly contribute to the above identified research problems, for building a robust and efficient C-TISF-AVE.

2. Autonomous Vehicle Ecosystems: An Overview

This shift away from human drivers means that the on-road transportation system will now be heavily reliant on AI-based autonomous decision-making and the connectivity between all autonomous devices and their respective environments. Thus, actors aiming to harm the United States and its economy now have an opportunity to target these on-road vehicles in a manner qualitatively different from traditional cyber-attacks. This changed landscape has already been realized through various vulnerable autonomous vehicle components, which could prove tempting attack vectors to any group or nation [7]. Once a cyber-attack is executed against an on-road autonomous vehicle (AV)—in any form—put public safety in immediate jeopardy; effective mechanisms to detect potential cyber-attacks early are called for to be proactive and not reactive.

Recent advances in artificial intelligence (AI) and other cutting-edge technologies have resulted in a proliferation of autonomous systems within defense, industrial, and commercial applications [6]. In many instances, these systems are tasked with carrying out operations and missions in remote and unsafe environments, which would be dangerous, difficult, or inefficient for human operators to perform in more traditional manners. Social awareness and adoption have driven on-road vehicles to the forefront of this trend, where these vehicles promise to dramatically reduce the number of people who are killed and injured each year in traffic accidents [8].

anti_autonomy_threat_identification_sharing: 49fe447b-1838-495e-b4d7-6c86a7a2cbe2, 13670fb6-30b9-4c1d-8b7c-45b576afab92

2.1. Key Components and Stakeholders

In such systems, autonomous vehicles are often considered as a catalyst to deliver future automobile technology trends such as in-car entertainment, digital lifestyle and smart tech, digital lifestyle and smart features, communication, telematics, cloud services, data analytics, in-cabin comfort, cybersecurity, safety, and vehicle defenses such as over-the-air (OTA) technologies. Security threats include stealing vehicle user data, vehicle theft, positioning of a vehicle, remote hacking of EPS, TCU, ABS, NCU, VCU, power-take-off (PTO), OBD, ADAS, etc., and accessing application users data, among many other such attacks with large adverse economic impacts. To study a vast range of security challenges and proposed mitigations for such technologies, recent surveys are presented in [7].

The rapid evolution of transportation technologies in recent years has transformed the our lives. Short-range transportation service via aging technology has evolved to a comprehensive system with a number of functionalities that have significantly improved our quality of life [9]. In this context, the fourth industrial revolution and the cyber–physical systems (CPS) inspired many new technologies that have been virtually implemented for transportation, such as autonomous vehicles, Intelligent Transportation System (ITS), Advanced Driver Assistance System (ADAS) functionalities for commercial vehicles, transportation of goods, and unmanned aerial vehicles (UAVs), among others for long-range transportation. These technologies enable the massive technical features, improved predictive maintenance, sustainability, and complete smart features in the transportation of the future. Thus, this has created a new dimension for the future and welcome generations, especially by Generation Z. The emergence of numerous security threats of these systems continue to be the main bottleneck for enabling transportation technologies [4].

2.2. Cybersecurity Challenges

[10] Possibly the most threatening aspect of the cyber-physical attacks is the remote exploitation of vulnerabilities in the wireless communication protocols. These attacks could adversely affect most operations performed by the remote commands without physical access to the vehicles. It is highly dangerous as it can lower the overall trust in the AV which might lead to the slow rate of adoption and can thus adversely impact the environment. Especially, in the case of autonomous vehicles, V2X communication is critical, which should ensure the transmission of reliable information between vehicles and between vehicles and infrastructure and to guarantee the safe and effective operation of the AV.[11] In Security, attackers might compromise the entire network and launch an actual attack or use malware to capture the driver's or passenger's data with unauthorized access to those data. They might simply see them, share them or attack the driver or rider with others that is not the core part as the vehicle requires to fully share those data and information with them for better operation. But, depending on the data, the attacker could destroy the vehicle or theft vehicles and users' personal data which are the worst consequences automakers could face. Attackers who are capable of compromising the vehicle's GPS information causing a dangerous situation like navigating to the wrong route or even cause accidents. GPS information can completely be compromised with the help of the jamming or spoofing techniques. GPS

information is sometimes accompanied by false data which often contains legitimate avionics, consumer-grade GPS, and act as the Vikram Lander of Mars Orbiter Mission.

3. Cyber Threat Intelligence Sharing Concepts

Promising developments in Connected and Autonomous Vehicle cybersecurity—assets such as the CAN-FD and the IDPS, for example—can be combined with information sharing models from the literature to either proactively inform the community of potential threats, or in a reactive sense to inform the community how to better handle the information that is raised by concrete incidents [2]. Connecticut and Colorado in the USA have both passed legislation that sees CAVs as part of the future driver vehicle interaction. Until we reach this particular future the driver will remain as an interested cooperator, but a bad driver here is potentially a powerful adversary as the portlet approach shows, as we have seen elsewhere in the field adding a driver to the V2X communications means that the vehicle logic does not always have the final besides in the discussion about performing a particular action at a particular time.

Connected and autonomous vehicle (CAV) cybersecurity is an essential part of broader connected car security strategies. CAVs must handle a breadth of data, from the state of the car to positional and navigational data [12]. This data represents a significant target for a potential attacker to manipulate CAV behavior and cause very real world threats, including physical injury. These systems may also do something similar in terms of what they communicate beyond the vehicle, including what we might call meta-information about a given trip such as the navigation destination, external sensor data, and safety messages (i.e., brake lights or alarms). Additionally, CAV systems may communicate digitally with outside systems as part of a V2X communication context, partly enabled through many established communication protocols including cellular, 802.11p, and more generally via cloud-based services [3]. Being connected to digital networks in this way, CAVs are vulnerable to attacks designed to manipulate the digital aspects of the systems they handle and with appropriately (mis)used specific information might be manipulated into delivering unpredictable behaviors.

3.1. Definition and Importance

However, there is still limited research in the definition and importance of vCTI as compared to overall CTI sharing. In much of the literature, vCTI appears only as a specific application of CTI sharing [13]. And similarly in the numerous recent reviews and action plans and pre-deployment standards, we can find significant differences among these regarding the most important sources of vehicle CTI – it could be some kind of threat attack (e.g., network, information shared across network), physical attacks (via modification of vehicle IT components), or product CTI (obtained during project interal verification activities).

Tao et al. [14] have defined CTI as threat intelligence developed and shared by a group of consortium members to help each other to use this information for protecting enterprise resources by minimizing damage to cyber assets and data. Similar to CTI, Vehicular Cyber Threat Intelligence (vCTI) can be defined as the detection, analysis, and sharing of threat intelligence information between Vehicular Cyber Ecosystem (vCE) members, as well as other organizations with an interest in protecting their resources, including OEMs, TSPs, developers, researchers, etc., to minimize the damage caused by cybersecurity threats within the vCE [12]. All the information could include typical Weaknesses/Threats, Attacks/Failures, and Vulnerabilities that could be detected at different levels of a vCE and their potential consequences. The CTI collected and analyzed at the ecosystem level could be utilized to take the appropriate mitigatory measures against these threats so as to reduce damages of the vCE and maintain its security.

3.2. Types of Threat Intelligence

Intra-vehicle cyber threats such as injection of malicious executable code or data into the vehicle's internal communication in the intra-vehicle network and indiscriminate flooding of broadcast messages. Environment-related cyber threats such as vehicles operating in an arbitrary way using responses and actions applied to adversarial, counterfeit data and attacks against the other vehicles drivers and passengers. Vehicle-to-Everything communication (V1V2X) related cyber threats and attacks like Massive Denial of Service (DoS) attacks on the roadside units and also the other vehicles. Vehicular routing protocol attacks where the attacker can launch many types of routing and data forward from attacks across vehicular networks, which will eventually disrupt the traffic flow. Man in the middle attacks that are quite common in any form of communication, and last but not the least. Sensor attacks pose the most dangerous risk as invalid sensory information could lead to potential changes in a vehicle's route or any kind of automobile control function.

VV (formerly SomeVehicle.com) This also includes a foretaste of things which are upcoming or going to come from those in the opposition. But, it's clear that sheer intelligence is necessary, rather than a warning. Regardless of the overlap (or the lack of it) at different level of external cyber threat intelligence, it is amply clear that the nature of threats themselves (examples relevant for the scope of the research) will vary between in-vehicle network (II), intra-vehicular network (V): vehicle-to-everything communication (V1V2X) and the direct interface with the human driver. Generally, we can divide vehicular cyber threats into six different cyber threat intelligence categories [15]:

Like in any other domain, threat intelligence can be divided into internal and external cyber threats [7]. Internally focused intelligence in the automotive sector refers to limiting the potential spread of a compromise within a given automaker domain. Each automaker will therefore likely focus on internal intelligence to the parameters and thresholds and threshold tend to vary by each organization. Beyond the narrow focus of internal security intelligence, the wider range of external cyber threat intelligence is shared between different organizations. V2 V (Vehicle (machine-to-machine) communication that is based on the standardized implementation has become an important component of modern vehicles. Identifying and characterizing the potential cyber threats in the ITS is therefore paramount in the cyber threat intelligence landscape. CAV's external cyber threat intelligence plays a role in supervising the current situation, like mundane malware, serious intrusion attempts by organizations having opposing aims, and a lot more.

4. Existing Cyber Threat Intelligence Sharing Frameworks

From several studies conducted on advanced driver assistance systems, autonomous vehicles, traffic light communication, website defacement, and numerous other cyber threats against automotive vehicles, this section acknowledges that no platform or system can be 100% secure. Also, the systems running in different domains can never be considered isolation-vulnerable to intradomain attacks, privacy violations, and authentication, as well as control problems. Furthermore, cloud services are no exception, while providing value-added services and loose-coupling IR and vehicle/to/vc IR through OTA signaling, position, navigation, and timing (PNT)slackening attacks will sabotage positioning data.

In this section, a comprehensive understanding of existing open-source threat intelligence sharing frameworks and their relevance to the autonomous vehicle ecosystem is established. The key components and capabilities of these frameworks, including their advantages and drawbacks, are reviewed. An analysis of the potential threat vectors, cross-vendor collaboration, and coordination framework capabilities were also evaluated in a broad sense

[10]. Threat intelligence is necessary not only for preventing incidents, but also to have detection controls and processes ready, which can be trusted in an ever-changing hostile environment [5].

4.1. Overview and Analysis

From the title of the German Vehicle Ethics Law's perspective and importance-related second article regarding the AV security levels are to be analyzed. As we have seen, the issue of the automotive multi-transport network security has grown out long ago. The networkedness, automation, interoperability, personalization, digital data flow performance and content previously spelled out across The primary and secondary attacks in vehicles includes a surprising number of attacks in connected Vehicular Systems and Connected Autonomous Vehicular Systems (CAVs), however the vast majority of publicly known attacks in the vehicular IT system makes ineffective the full AV multi-material cooperative system (Complex Central247) software and hardware security solution and CAV from coherancy includes loss of safety, durability, quality and accessibility, suitability and robustness in the life cycle. In the future, the goal of information security should gain insight. Security systems are not effective in the crime detection and human-interest, Human-Accessible-Risk-Alert verification (HARAV) was introduced, which increases the foundation of the European Recommendation 30. Safety is determined for future scarcity in High-security levels.

[9] [13]The first article regards information security in the passenger-Autonomous Vehicle (AV) interaction. This made us realize that the threats and recent trends in connected and automated vehicular ecosystems are important for the AVs of the future cyber security. As AVs are emerging autonomous and connected IT systems with access to personal data mobility services and an extensive environment with various systems of systems, their increase in cyber risk categories are to be expected through more number of include. The AV information systems that operate on the characteristics and semi-connected networks, will become high-profile targets of cyberattacks in the future. The attackers will search for vulnerabilities in the metadata of AV-related hosted and networked distributed systems. For AV network attack tar-get data extraction methods, digital currency mining or rather making the AV sentient-botnets (also IT-based) are considered. The confidentiality, integrity and availability attributes in the Autonomous Vehicle IT system are very important parameters. This article describes just how big the connectivity, automation and personalization work in cyber vulnerabilities in the entire CAV of the value chain.

5. Designing a Framework for Autonomous Vehicle Ecosystems

Applications for protection of connected cars have been discussed in [9, 10]. The discussions are based mainly on threat analytics. For Anticar theft-attacks, Authors in [22–24] identify incidents and attacks from the CAN network and define detection mechanisms against these incidents. Similarly, frequent issues when switching off engine electronic, AV attacks against e-compasses and connected vehicles have been addressed. Authors in discuss how Blockchain can be used to easily detect attacks due to the decentralised external authentication that intelligently refers to data of other connected cars. They show the suitability of the procedure mainly in disclosing the ag-grid of disrupted vehicles. Finally, Intrusion Detection System (IDS) procedures are designed to strengthen the integrity between input and output messages via Blockchain-based approaches. This application requires sophisticated protection, also known as automotive firewalls, for realistic rules such as change of behavior, misinterpretations, protection against reflectivity and endurance. Additionally, adaptive mechanisms, such as IDSs, are required to comb areas and adjust threats in near real time.

[16] [1]The design of a well-functioning CTI security sharing framework for the automotive ecosystem, and particularly autonomous vehicles and parked units, needs to overcome several obstacles, such as competing business interests, national laws and data protection laws, and fears of los-ing competitive advantages. In addition, the particular context, i.e. inbound and outbound traffic and different kinds of communication partners, require a security sharing framework. For example, if vehicle manufacturer A shares Anomaly 1, then vehicle manufacturer B must be capable of understanding and working with the entry. On the other hand, vehicle manufacturer A often has an interest that di-verse car models are as well protectable as possible from a threat that is released by their car model (outbound traffic). Moreover, regulatory guidelines have to be adhered to for the sharing of CTI security in the automotive sector.

5.1. Considerations and Best Practices

The security of the artificial intelligence and systems by extension, requires an understanding of the potential security ramifications —"at the core of it, the issue is that both the systems must make decisions about trust with incomplete information" [17]. A significant activity of the proposed approach and other similar systems has therefore been to review the systemic capabilities of decision support made visible to the administrator, quickly detected and if necessary readdressed, according to changes in threat posture, while also being reparameterised efficiently iteratively to reduce system dependence over time. More generally, a paper published by the IT University in Denmark has researched the possibility of using blockchains to aid in trust representation, orchestration and general system administration, in the light of incoming threats, within mixed heterogeneous environments, but the feasibility and scalability of these systems remains uncertain.

The implications of the diverse and nuanced security compromises to automobiles have been rigorously investigated in literature [3]; In particular, the unique characteristics of these vehicles, such as their capability to update themselves, the growing complexity introduced by designer-invisible sensors and character-dependent communication, and the low-quality perception constraints these systems to face, are leveraged to design specific attackers who elude the standard security evaluations, compromising the hardware and/or the physics of the vehicle itself. In addition, open vehicular software ecosystems have been observed to foster the appearance and spreading of decoration ransomware [6]. The inevitable interdependence between security and safety requires safety procedures to be informed by security evaluations, especially at design time, such that all possible safety concerns are taken into account, including the peculiarity of a compromised environment.

6. Implementation and Operationalization

The effective sharing of cybersecurity information could allow potential vulnerabilities to be uncovered and fixed sooner. Consequently, stakeholders within the automotive industry and research community are working to define new architecture and methodologies to enhance the domain level of cybersecurity. However, due to the intrinsic characteristics of vehicular environments and their use, specific architectures are crucially required. Such architectures have to be scalable and performant, involving Cloud and Edge computing, and of the most important requirement is the security by design. Security in depth can be achieved only using a multi-layered approach and adopting hardware and software diagnostics, before authentication and authorization steps. The solution presented is member of a public ecosystem with free accessibility and it does not need any additional hardware or device be embedded in the vehicle or the infrastructure. So, it can be used on every vehicle and from every user. To make a concrete example of implementation, and evaluating the mean value of the model risks for over-the-air updates in autonomous vehicle, the barriers for their implementation on the transport network are also analyzed [2].

Developing functionalities for a cybersecurity ontology promoting and the operationalization of cyber threat intelligence in the exchange and share of threat data, potentially useful to detect and block possible security attacks. The responsible and safe operationalization of a such tool require that all critical operations should be approved and validated by authorized users to avoid any erroneous or wrongful act. In this scope, it is important to distinguish the legitimate countermeasures from the possible actions which can have collateral effects and put the operational safety at risk, that require an additional "monitoring step" to be approved. Testing is crucial. nn by engeneers, why. In this paper, we experimented in CWS four different machine learning techniques available from Weka including Random Forest, J48, SMO, and Recurring Cxreps for cross-validation [18].

Protection measures aim to avoid or minimize the exploitation of automotive security vulnerabilities. Unfortunately, these measures are not foolproof and it is therefore important to continuously monitor the autonomous vehicle for potential security threats. Test benches, as a complementary power-aware solution, are a promising solution that simplify and foster security vulnerabilities testing and their corrigibility. In the context of autonomous driving domain, we present in this section a non-exhaustive list of operational functional and security for threat intelligence sharing framework [10].

6.1. Technical Aspects

[5] [19]One key objective in enabling the sharing of Cyber Threat Intelligence (CTI) in the context of an autonomous vehicle ecosystem is to secure this sharing process from adversaries. This security requirement applies to almost all area of the data flow mechanism in the intelligence sharing lifecycle. More specifically, this sharing of CTI across multiple stakeholders, which includes both vehicle manufacturers and drivers, potentially open gates in the network for an adversary, and this would put the vehicles, and in turn, drivers, in risk of threats. Therefore, the framework must ensure that unwanted actors are filtered out and only legitimate and authenticated data is disseminated in a network.[14]Protection of vehicle architecture requires a special non-intrusive evaluation, that is able to monitor the whole network traffic allowing to isolate and investigate the specific security issues. Besides, testing during normal working conditions, it is not possible to predict the presence of all possible attacks because of the continuously evolving threat scenarios. Thus, for a correct and exhaustive assessment of the In-Vehicle Cyber-Security, advanced and flexible test platforms able to replicate and evaluate a huge number of possible attack scenarios are preferable.

6.2. Organizational Aspects

In order to answer RQ3 and conclude the discussion, we can say that the kind of control that emerged in Italy, called traffic modulation, is probably the best option for all cases. This approach suggests that the operator will manage information flows originating from ITAs, TAs, web services, or SATVs effectively and efficiently in all the considered scenarios. This sort of orchestration model affords the region of safeguarding secure and trusted networks. As a consequence of this approach and action, the trafficking system of A-ATVs will become increasingly flexible, quick, and capable of responding to new cyberattacks. By leveraging an artificial immune system, the Cybersecurity coordinated system will be capable of anticipating critical phenomena for a wide and variable range of threshold values, like the spread of malware or positioning against cyberattacks. Modification management establishes and prevents security attacks against the system and countermeasures the actions launched by the attackers [1].

Based on the analysis provided, RQ1 is answered (inviting participation in ATV development while securing network connectivity is a crucial matter for industry organizations). Indeed, when the responsibility of the respect of certain regulations is fragmented to the maximum degree, the security of the whole system of systems and of all – at all levels, from the state to the stakeholder to the infrastructure and the passenger/users – is at risk. As such, we argue that the effort to secure the confidentiality, availability, and integrity of a complex system such as the one overseen in the case of ATVE should be coherent and harmonized at the level of all organizations participating in the development, deployment, and maintenance of this technology. With the purpose of minimizing possible threats and the risk of information loss, before a C-ATV will be launched in the market or will drive on a public road, it will be cross-checked carefully by the stakeholders and pass a validation protocol. Each team of developers will stress cybersecurity checks to guarantee that every single system has been efficiently secured before system deployment. In this way, a fully secure and trusted orchestration system model will be able to support both logical and physical security of the TraffioNetwork for RQT4.

Regulations are known as a significant aspect of technology development (Warrell et al., 2013a). That said, it is also important to remember that excessive regulation can create difficulties that hamper the efficiency of the whole process of system development (Taddeo, 2020a). Owing to these aspects, it is therefore important to stress that government participation in system development is crucial, but it is also equally essential to determine the best strategies for this [20].

While developing and deploying ATVs, the following is proposed as an appropriate strategy for enhancing cyber terrorism management and therefore securing each stakeholder's interest in the ATV.E (Autonomous Vehicle ecosystem) [6].

7. Case Studies and Use Cases

Incomplete list of the elements which need to be accomplished are: secure digital identities for vehicles, pedestrians, cyclists, and any special user (blind, deaf, etc.), based on decentralized identity management, as proposed [3, 49]; secure road maps, giving graphical representation of applications, user types, privacy preservation mechanisms, traffic rules, driver assistance policies, etc.; secure personal identity representation, accessible in a defined format and protocol (to receive any kind of external support with customizable sharing conditions); defensive connotations, inspired by defense in depth paradigm, between critical V2X data suppliers (as, for example smart cars) and even immediate beneficiaries equipped with classic V2X communication devices [5, 14, 51]; open incident presentation mechanism [3, 49] to maximize the effects of good practice sharing, connect the previous and actual documents, and generate the attack response solutions for the general case or for the specific targets recursively deduced; cyber-attack event-driven management system strong protected for analyzing non-standard cyber-physical system types of linked diversity of data from the original sources; 24/7 astutely decision-making infrastructure, founded on partial autonomy car operation capabilities and the optimized user policy management; the advanced anomaly detection system at V2X communication device or IT support; trust as service provider, implemented mainly for the effective periodic security and resilience evaluation, based on info serials, derived from regular attacker's interaction simulation; IoT ecosystems founded on neutral systems able to control mission security over multiple areas, while operating in a competition framework; centralized incident evaluation and communication enhancement with the proposed oasis (resilience policy formally defined across different authorities) initializer; and, management system of operating urban traffic in optimal trust provider conditions and, if necessary, across virtual cities [3, 76, 77].

[21] The V2X communications present the foundation of a future transportation ecosystem, offering challenges and opportunities. In a positive direction of the situation, we have to

accomplish the sharing of knowledge and experience, as well as the building of secure and efficient communication frameworks, valuable for the final users: vehicle occupants and their safety systems, pedestrians, road users, and governmental interests. This case is even more important because the development pace of the automotive advantages is absolutely independent from the research and development advances of communication technologies. This compass can be followed in decision-making process by the stakeholders (OEMs, local authorities, V2X communication suppliers, service providers, insurance companies, top management authorities, and any other eventual involved entity. Additionally, on such a level of trust and efficiency, shared standards and strategies can be perceived as competitively common objectives for vendors and integrators, while competition will be concentrated mainly on service specialization area. Reference presented a comprehensive data model to represent the intrinsic characteristics of modern driving context, based on a wide systemic vision, introducing a living approval system from the data sensor and communication technologies and interchangeable service proposed by the low-cost vendors in terms of software defined networks [3, 67, 76].

7.1. Real-world Examples

The presented examples serve as a good starting point to better understand what kind of CTI-based interventions would be important in different phases of the life cycle of autonomous vehicles, to show similarities and difference between current approaches and their potential ethical, legal and impact-related implications. Additionally, this section illustrates the complexity of the vehicle ecosystem and the necessity of a shared CTIAV framework. With respect to the security of autonomous vehicles, either a substantial malfunction of the entire control system must be avoided or the generation of false control commands by unauthorized parties must be prevented. Furthermore, malware is to be precluded from gaining control over the AVM by attacking E/E-systems in external vehicle devices (e.g., via Bluetooth) or by using the control system over the air.

[13] [16]To illustrate Section Section 7: Practical and Ethical Implications on Understanding a continuous Shared CTI Framework, 7.1 draws real-world examples: connected and autonomous vehicles (C/AV) with a focus on autonomous vehicles. At present, with different levels of automation in vehicles, connected and autonomous vehicles are capable of connecting to various sources and destinations, including other vehicles, local infrastructure, and the cloud. Depending on connected (C) and automated (A) capabilities level, SAE (Society

of Automobile Engineers) differentiates between vehicles. A classification based on shared control between the human driver and autonomous vehicle system, in its turn, comprises six different levels ranging from 0 up to 5, with the latter designating a fully-automated vehicle.

8. Evaluation Metrics and Performance Measurement

As the evaluation of the proposed threat intelligence sharing frameworks is crucial, concrete metrics, and performance measurements are to be established [22]. 1. Internal Evaluation Metrics: • Reduced Detection Time: By leveraging TISCC and EDPR frameworks, the security-related threats that are detected against the self-driving vehicles can be promptly resolved, which means the timespan between the occurrence of a threat and the detection of the threat can be minimized. • Protection from Legitimate Payloads: As we identified in the TISCC article [23], there is a possibility of detecting cyber-attacks (e.g., denial of service, disabling the AI autopilot) as normal/legitimate traffic. Therefore, we need to ensure the systems should not raise any automatic alarms on the legitimate payload, and we need to ensure averaging the normal traffic is understood by the system and doesn't raise any false positives. 2. External Evaluation Metrics: • System Robustness: Autonomous vehicle technologies should possess robustness, i.e., when a system is exposed to ambiguous/misleading information, the vehicular system is still able to function smoothly and maintain safety and security. • Secure Establishments of Walking Relationships: Introducing secure Self-Driving Car-to-Car Communication (SDC-C2C) and secure EV-to-Cloud-Communication (EV-C2C), the proposed countermeasures in this research assure Walking relationships/peer-to-peer relationships are established always in a secure manner.

9. Legal and Ethical Implications

The results suggest that legal, organizational, and economic challenges make broader adoption of open sharing models less likely in the future. Instead, it is more likely that "gatekeeper" ISACs and select trusted third parties will continue to hold, aggregate, and disseminate threat intelligence gathered from the original data sources. This keeps valuable intelligence within an ecosystem that may not be conducive to data sharing, or have incentives to be "first" to signal significant incidents. The study urges for international support to ensure law and regulations are updated to enable the sharing of cyber threat indicators and maintaining of a competitive environment for new start-ups [24].

Autonomous vehicle ecosystems comprise a complex network of stakeholders spanning technological development, corporate affairs, governance, and normative and ethical discussions that will continue to evolve over time [13]. Cyber threat intelligence sharing is paramount in understanding cyber threats and vulnerabilities against these infrastructures. Evidence shows that companies do share meaningful cyber threat intelligence with appropriate stakeholders in these ecosystems. However, our analysis also highlights a range of key issues which hinder more comprehensive sharing: prevailing legal and regulatory ambiguities that no longer match the speed of technical advancements, the economic necessity of proprietary technology and the bureaucracy of larger corporations, a lack of trust in new start-ups, and limitations to the ability of digital forensic and emergency response capabilities within information sharing and analysis center (ISAC) operations to adequately address malicious activity.

10. Future Trends and Emerging Technologies

Article [5] has identified potential future attacks on the infrastructure of vehicles, and the solutions that have been developed, namely the vehicle, traffic and intelligent transportation system security measures. However, the study has also concluded that there is a dire need for centralized authorities to regulate the current, unregulated, and untrustworthy vehicular traffic frameworks. Steganography can also be used to send messages secretly, and warning messages broadcasted to the vehicles can also be encoded with malicious payloads. The effectiveness of the communication channel, which is the main source of V2X data flow, could be hampered through a jamming attack. Managing, monitoring, and controlling the communications and data flow requires appropriate security recommendations, and the establishment of standards will be the key factor determining the success of future implementations of measures.

The primary contribution of article [10] is to present a working definition of vehicle-to-everything (V2X) communication, catalog the possible V2X attacks, and list out the vulnerabilities and exploits that can be leveraged during the VI and VA phases of vehicle exploitation. A survey on the dependency of vehicles on wireless communication and the inclusion of an external backend where OTA updates and new features can be facilitated is also introduced in this article. It is determined that the V2X communication is vulnerable with a myriad of possibilities and has diversified attacks, exploits, and vulnerabilities that IoT technologies have managed to create, where predicting behavior before establishing the existence of an attack is possible. A resilience in cyber defenses for vehicle systems must be developed to eliminate the current status quo of relying on the helper and the mere connecter along with the driver, and effort must be invested in enabling the AVs with more autonomy to handle wider cyber threats.

Article [8] aims to identify the key enabling technologies, introduce the operational system architecture of NEVs, and highlight the important aspects of IoAV security and privacy by elaborating on the advance attack and defense techniques. A framework composed of five differentiated layers, namely, the connection and sensing layer, edge computing, storage and analysis layer, communication and networking layer, operation and business management layer, and the evolution and trend of key technologies and operational protocols have emerged as the critical features of a successful IoT–5G integrated system, which are integrated with advanced technologies and operational functionalities. Block-based computing has become a fortune-changing technology for AVs since it provides intrinsic features of tamper-evidence and enhanced data integrity, data availability, and confidentiality. By incorporating IoAV, IoV, connected device, and edge intelligence capabilities, complementary functionalities and features of each entity can be furnished to build the intelligent base to enable the proper transport management system.

11. Conclusion and Recommendations

The data crawlers have direct access and assisted with the pull–push mechanism to make less intrusive honeypots produce prescriptive datasets. It concerns protocol and mechanism adoption for Allowlisting, IOC (Indicator of Compromise), and anonymous threat-derived data sharing. AI-enhancements are done to nurture effective CTI sharing. All advanced GMOASO online calculations, further host/device models, and RobJIST–EV systems have also been integrated. All these mechanisms make CTI plainly distributive (Federated) so that Devices compartmentalized into Threat Intelligence Layers (TILs) under TI amusement, and commensurate Models are updated by the TRCA-MODEC simulation. The contact graph management protocol is a major contribution to the DCN. Finally, we recommend that, when deployed, this system has the inherent capability to not only deter and withstand but also respond proportionately for Fact Refutation, and DIH enhancement using the Non-Marginal Search (NMS) algorithm.[7] As billions of Internet of things (IoT) devices become popular due to various application and advances in technology, a large volume is bound to be connected in order to acquire data and accomplish complex and independent tasks, like a community of autonomous solutions robots in the smart city equipped with seems to be the normal conditions now. It guides to the creation of the super network surround linking machines in various ecosystems from aviation and automotive to environmental products having the commonalities of instability due to hyper-connectivity and rather disparate trust bindings due to far-reaching connections. The harbor-environment of such sensitive super systems poses an attractive and an ingenious World 3.0 called HBOI, with multiple attack masking prospects of anonymity, vagueness requisites, and kill-cloud troop dynamics in targeted networks. Aware and Cognizant like Humans for managing HBOIoTs have to devise Intelligent Counter Cyber Measures (ICCMs) so that security is a feature by design. [14] A modern HBOIth educational system presented in the manuscript was formulated using an Artificial Missing Value Imputation Enactment driven by NFT and layer-specific Gaussian Radial Basis Function Networks (LRBFN) so that Agents and Consumers are fully trained to underpin the BCEADR and EAvSITTCV dynamics. However, due to the presence of pervasive nearest-neighbor harnessed noise, modern technologies of genetic algorithms and knowledge base supported Journals of NSGCITAR and JFI became the primary motives to design Robotic processes. For the design of the WGOICOCTTS, the researcher introduces a model structure with direct and indirect connection weighted elements between all present and absent Observers of event states and Action Servers of Team Communication Variables (AFCV). This is the first ever advanced game-theoretic guidance to resolve SeCoV embedded StructChNMs. Although fraud-resistant SCGAs demonstrated higher topology optimization propensity, mixture hybrid tie-breaker genetic ant algorithms and optimal control were deemed influential for solving future HSAACoO problems.

[25] Cyber Threat Intelligence (CTI) sharing frameworks do not have specific technical and non-technical support and are currently not commonly designed to protect global autonomous vehicle (AV) ecosystems from internal and external threats. This research therefore undertook HBOIoT design for CTI sharing in AV ecosystems, with comprehensive repositories (data crawlers, honeypots, black boxes, etc.), protocols, and mechanisms relevant to the design of the framework, involving transport, communication, platform, and human factors. The framework's core is a full-fledged concept of Threat Intelligence Enclave (TIE),

which exposes a hierarchical four-layer model responsible for both low-level and higher-level operations.

12. References

1. [1] M. Gupta, J. Benson, F. Patwa, and R. Sandhu, "Secure Cloud Assisted Smart Cars Using Dynamic Groups and Attribute Based Access Control," 2019. [PDF]
2. [2] V. Kumar Kukkala, S. Vignesh Thiruloga, and S. Pasricha, "Roadmap for Cybersecurity in Autonomous Vehicles," 2022. [PDF]
3. [3] F. Berman, E. Cabrera, A. Jebari, and W. Marrakchi, "The impact universe—a framework for prioritizing the public interest in the Internet of Things," 2022. ncbi.nlm.nih.gov
4. Tatineni, Sumanth. "Beyond Accuracy: Understanding Model Performance on SQuAD 2.0 Challenges." *International Journal of Advanced Research in Engineering and Technology (IJARET)* 10.1 (2019): 566-581.
5. Vemoori, V. "Towards Secure and Trustworthy Autonomous Vehicles: Leveraging Distributed Ledger Technology for Secure Communication and Exploring Explainable Artificial Intelligence for Robust Decision-Making and Comprehensive Testing". *Journal of Science & Technology*, vol. 1, no. 1, Nov. 2020, pp. 130-7, https://thesciencebrigade.com/jst/article/view/224.
6. Mahammad Shaik. "Reimagining Digital Identity: A Comparative Analysis of Advanced Identity Access Management (IAM) Frameworks Leveraging Blockchain Technology for Enhanced Security, Decentralized Authentication, and Trust-Centric Ecosystems". Distributed Learning and Broad Applications in Scientific Research, vol. 4, June 2018, pp. 1-22, https://dlabi.org/index.php/journal/article/view/2.
7. Vemori, Vamsi. "Towards Safe and Equitable Autonomous Mobility: A Multi-Layered Framework Integrating Advanced Safety Protocols, Data-Informed Road Infrastructure, and Explainable AI for Transparent Decision-Making in Self-Driving Vehicles." *Human-Computer Interaction Perspectives* 2.2 (2022): 10-41.
8. [8] A. Biswas and H. C. Wang, "Autonomous Vehicles Enabled by the Integration of IoT, Edge Intelligence, 5G, and Blockchain," 2023. ncbi.nlm.nih.gov
9. [9] M. Bakhtina and R. Matulevičius, "Information Security Analysis in the Passenger-Autonomous Vehicle Interaction," 2021. [PDF]

10. [10] A. Dinesh Kumar, K. Naga Renu Chebrolu, V. R, and S. KP, "A Brief Survey on Autonomous Vehicle Possible Attacks, Exploits and Vulnerabilities," 2018. [PDF]
11. [11] M. Scalas and G. Giacinto, "Automotive Cybersecurity: Foundations for Next-Generation Vehicles," 2019. [PDF]
12. [12] S. Lee, Y. Cho, and B. C. Min, "Attack-Aware Multi-Sensor Integration Algorithm for Autonomous Vehicle Navigation Systems," 2017. [PDF]
13. [13] A. Kriebitz, R. Max, and C. Lütge, "The German Act on Autonomous Driving: Why Ethics Still Matters," 2022. ncbi.nlm.nih.gov
14. [14] R. Singh Rathore, C. Hewage, O. Kaiwartya, and J. Lloret, "In-Vehicle Communication Cyber Security: Challenges and Solutions," 2022. ncbi.nlm.nih.gov
15. [15] A. Jafar Md Muzahid, S. Fauzi Kamarulzaman, M. Arafatur Rahman, S. Akbar Murad et al., "Multiple vehicle cooperation and collision avoidance in automated vehicles: survey and an AI-enabled conceptual framework," 2023. ncbi.nlm.nih.gov
16. [16] T. Andreica, A. Musuroi, A. Anistoroaei, C. Jichici et al., "Blockchain integration for in-vehicle CAN bus intrusion detection systems with ISO/SAE 21434 compliant reporting," 2024. ncbi.nlm.nih.gov
17. [17] X. Masip-Bruin, E. Marín-Tordera, J. Ruiz, A. Jukan et al., "Cybersecurity in ICT Supply Chains: Key Challenges and a Relevant Architecture," 2021. ncbi.nlm.nih.gov
18. [18] I. Mavromatis, T. Spyridopoulos, P. Carnelli, W. Hau Chin et al., "Cybersecurity in Motion: A Survey of Challenges and Requirements for Future Test Facilities of CAVs," 2023. [PDF]
19. [19] A. Manimuthu, V. Dharshini, I. Zografopoulos, M. K. Priyan et al., "Contactless Technologies for Smart Cities: Big Data, IoT, and Cloud Infrastructures," 2021. ncbi.nlm.nih.gov
20. [20] Y. Mei, "First-order coherent quantum Zeno dynamics and its appearance in tight-binding chains," 2023. [PDF]
21. [21] S. N. Saadatmand, "Finding the ground states of symmetric infinite-dimensional Hamiltonians: explicit constrained optimizations of tensor networks," 2019. [PDF]
22. [22] N. Chinpattanakarn and C. Amornbunchornvej, "Framework for Variable-lag Motif Following Relation Inference In Time Series using Matrix Profile analysis," 2024. [PDF]
23. [23] J. R. V. Solaas, N. Tuptuk, and E. Mariconti, "Systematic Review: Anomaly Detection in Connected and Autonomous Vehicles," 2024. [PDF]

24. [24] A. Taeihagh and H. Si Min Lim, "Governing autonomous vehicles: emerging responses for safety, liability, privacy, cybersecurity, and industry risks," 2018. [PDF]
25. [25] H. Rivera-Rodriguez and R. Jauregui, "On the electrostatic interactions involving long-range Rydberg molecules," 2021. [PDF]