Threat Intelligence Fusion Techniques for Enhanced Cybersecurity in Autonomous Vehicle Networks

By Dr. Heba Abd El-Aziz

Associate Professor of Computer Science, Cairo University, Egypt

1. Introduction

Furthermore, the sophisticated algorithms in the cybersecurity systems executed in the CAV should also be capable of detecting all the irregular events in real-time. Intrusions in the form of changes both in-packaged and out-of-band i.e., on cyber-interfaces of CAV must be thwarted by an advanced cybersecurity system. When these irregular events deviate from normal and go undetected due to lack of sophistication in real time, these can potentially foster a large-scale cyber-attack in the CAV. To ensure countermeasure against these, a study on the context of cyber-attacks in the CAN bus must be conducted to find the probabilities of cyber-attacks updating of CAN bus that will be used in this manuscript. By prioritizing safety over security, these studies can bridge the gap by designing in-tripcybersecurity systems for CAVs, which are capable of providing reliable security and still ensuring comfortable in-cabin experiences for both the drivers and passengers alike. This manuscript aims to contribute by facilitating research-based driver assistance [1].

The rapidly advancing connected and autonomous vehicle (CAV) technology ecosystem offers significant benefits allied with the promise of increased automation leading to improvements in safety, traffic congestion, and energy utilization. However, this wave of automation introduces new security threats and vulnerabilities to vehicle networked electronic systems, such as the Controller Area Network (CAN) buses and wireless communications. With the increasing complexity and the deficiencies in existing security mechanisms of the standard CAN protocol, the operational security of CAVs exhibits highly exposed vulnerabilities such as privilege escalations and man-in-the-middle attacks. Therefore, a pressing need arises for an advanced second line of cybersecurity in the form of an effective intrusion detection system comprising sophisticated detection algorithms specific for the CAN bus [2]. The advent of ISO/SAE 21434 as a cybersecurity standard for vehicles and their components necessitates a unified control mechanism addressing both physical information and cybersecurity simultaneously. However, increasing the real-time cognitive load of drivers through the poorly designed in-car cybersecurity interfaces neither aids in vehicle security nor the safety of vehicle occupants [3].

1.1. Background and Context

- A comprehensive classification of security threats in the connected and autonomous vehicular system domains. - A discussion on various security operations and functionalities. This discussion of potential security solutions included security operations, namely, authenticity and confidentiality, availability, privacy and identification. - A discussion of various security operations and offered a comprehensive taxonomy to computing security features. Shortcomings in the different existing solution design must be rectified to solve security issues in connected and autonomous vehicles. An association of possible data breaches was discovered, and a variety of precedent attacks were identified. The findings define the sources of vehicular security attacks presented within the literature [4].

The main contributions of this review to knowledge in the field were:

Road safety is a top priority in today's society, and the automotive industry is constantly exploring different technologies to make driving safer. With the introduction of electric vehicles, smart cars, and Advanced Driver Assistance Systems (ADAS), connectivity and automation have become the most influential technological trends in the automotive industry. Modern cars are equipped with state-of-the-art wireless communication technology and vehicle control systems. Connectivity in advanced car systems opens up a world of possible attacks and creates opportunities for the potential threat actors. We presented findings from the literature relating to many current challenges presented to connected and autonomous vehicular systems. This information was synthesized from various research papers, conference and journal articles, and reports sourced from various Web of Science databases, conference organisational and research sources [5]. In-vehicle, vehicle-to-X, and vehicle-to-vehicle protocols were discussed as extremely vulnerable, as many successful and extensive proof-of-concept attacks had been performed on these systems. These attacks could have potentially led to catastrophic effects.

1.2. Research Problem and Objectives

Connected vehicles face challenges from in-vehicle network security and related cyber threats. The trivial network protocols and architectures and the justifiable application of off-the-shelf solutions by the vehicle manufacturers have acknowledged these vulnerabilities. Moreover, the connected vehicles demand the refashioning of the communication architecture, i.e., introducing wide-ranging in-vehicle and in-roadside personal area networks (PANs) to accomplish the infotainment and comfort requirements for vehicle occupants. There is a wide research area related to the secure network development in terms of CAV security, which is a contributing factor in performing in silico simulations of analysis of network data and identifying attacks in network layers. The wireless network-based vehicle communication system has many potential security threats and vulnerabilities in the areas of physical layer/bit sequence. Therefore, this paper mainly focuses on diagnosis and optimizing secure transportation communication problems and provides possible solutions for security and privacy problems related to related art approaches and open problems to guide researchers about future directions [6].

The automotive industry is experiencing a digitalization process, with changes apparent in the areas of Mobility as a Service (MaaS) and connected vehicles. As a result, vehicles have been transformed into complex software-based IT systems, leading to increased cybersecurity challenges. This presents the automotive industry with two main challenges: (1) The convergence of the automotive and IT industries and (2) the transformation of physical vehicles to cyber-physical systems (CPS). To achieve strong overall vehicle security design, a number of technical mechanics have been developed, including isolated security control, transparent security solutions, intrusion detection and prevention, credential role-based security, and/or secure hardware implementations. The achievement of security requirements will contribute to the fundamental interaction between CPS entities, providing system security and long-term system reliability [7].

1.3. Significance of the Study

CAV riders are expected to spend more time on non-driving tasks while seated at the rear, thereby increasing the cognitive demand on in-vehicle interfaces to be well managed, so as to minimize their impact on perceived safety, trust, usability, and operational efficiency. Several cybersecurity user interface (UI) design mockups are expected to be tested and validated through an attempt to optimize the effect of UXNT on the overall cognitively-perceived cybersecurity performance and trust during vehicle driving. Enhanced situation awareness, increased cybersecurity performance, reduced cognitive workload, and deepened feeling of trust are the key UXNT requirements of the studied cybersecurity UI systems, to support the dynamically progressing human-vehicle-environment interaction.

The evolution of connected and autonomous vehicle (CAV) control systems has created an increased need for cybersecurity risk-management technologies in conjunction with advanced threat intelligence fusion techniques [4]. Although cybersecurity requirements for proper management of authentication, availability, confidentiality, integrity, non-repudiation, and privacy have been identified, protecting CAVs from a multitude of stealthy cyber-attacks that exploit those vulnerabilities demands significantly improved cyber-resilience against multi-layered cyber-threats. Several conventional cybersecurity approaches can cause a higher cognitive workload when interfaced with the vehicle control systems [8].

2. Literature Review

Vehicular communication solutions enhance road safety and traffic flow, but in terms of cybersecurity the in-vehicle communication connects electric, electronic and software systems which are critical assets providing primary vehicle functions with a cyber world. A brief survey of various security solutions for vehicular cyber security has been attempted and this categorizes the security solutions into three classes namely Inside vehicle vehicle communication security, intervehicle communication security, and security of all systems and software required for automation and operation of the vehicle [5].

Intelligent Transportation Systems (ITS) is the global technological revolution offering innovative, dynamic and intelligent services that bring significant improvements to road safety and efficiency. Autonomous vehicles (AVs) are an important future component of ITS. Development of various technologies for AVs offers intelligent and automated solutions for road safety, connectivity and communication with other vehicles, infrastructure, and data processing. AVs rely on various types of sensors, intelligent algorithms, and machine learning techniques to handle environment perception, vehicle control and communicate with other vehicles, and roadside equipment to ensure smooth and safe driving and environment. The swarm intelligence of these entities makes AVs more vulnerable to cyber-physical attacks [9].

2.1. Autonomous Vehicle Networks and Cybersecurity

As the reliance of civilian and military networks on AV technologies increases, the need to protect these systems from cyber-physical attacks is expected to grow. Researchers at the U.S. Department of Commerce's National Institute of Standards and Technology developed the conceptual Autonomous Vehicle Security Framework to enhance security, safety, and privacy for AVs [8]. MASIA sought to identify the main methodological approaches used to evaluate the impact of the cognitive load of drivers on the interpretation and use of graphical elements that may be encountered in the user interfaces of the control systems of autonomous vehicles. This study is a double factorial design (2 x 3). The factors chosen were the visual complexity of the interface and the time to complete a decision-making task. We recreated an AV control panel by using a choice reaction time task to represent an AV cybersecurity alert. Subsequently, we studied two detection thresholds (45%). Finally, we estimated the average time necessary to detect a cybersecurity alert corresponding to the chosen threshold. The use of an increasing number of graphical elements can lead to an overload of cognitive resources and, as a result, to a decrease in the safety and security of the interface. This approach allows cybersecurity interfaces to be coheritentlyintegrated, designed effectively for future users, and tested virtually.

Autonomous vehicle networks and distributed systems are present in many military and civilian sectors. Notably, the automotive industry is heavily investing in autonomous vehicle (AV) technologies. The functionality of AV networks relies on cyber-physical systems (CPS), where sensors feed data through electronic control units (ECUs) which interface with actuators. As such, AV is rapidly evolving to support benefits like improved safety, energy efficiency, and reduced traffic congestion, and messaging has shown that public autonomous vehicle networks are expected to increase by an order of magnitude by 2025 [5]. [10].

2.2. Threat Intelligence Fusion Techniques

The need to focus upon the design of interfaces capable of fusing multiple data streams to minimize cognitive load in operation is highlighted [11]. In this way, the primary performance measure appropriate for future interfaces can only be "mind availability," this suggests all background and cognitive load sink operations are maximally decoupled from the driver. As this paper has already suggested, this will involve careful use of inputs from microphones and tangible interfaces around the cabin that do not consume the driver's visual or cognitive capacity. Pursuing this endpoint can further realize levels of operational utility within system 2 that were previously unimaginable in a static/low-pressure environment.

The vehicle design context, regulatory scenario, and emerging attacks require a paradigm shift when designing cybersecurity interfaces [12]. The future threat landscape for AVs now includes nationsate and cross-vehicle attacks which can result in the loss of life and limb. Also vehicle architecture has shifted from fragmented Vehicles control. Interfaces need to evaluate more data and path planning at once to tease out such attacks for drivers [10]. Hence, the corresponding interfaces are operating under a higher operational cognitive level than traditional vehicles. A potential mismatch between the forces for good and for evil provides the opportunities for implementing solutions that are only available within the emergent context. It involves tailoring the behavior of an interface to avoid any unnecessary increases in cognitive load.

2.3. Cognitive Load in Human-Computer Interaction

A main strategy for aiding human operators to manage and control their cognitive load is to modify how information is presented in the interaction interface [4]. For example, techniques that support the idea of providing users with filtered information and support in terms of the information presentation, modality, format, and placement are proven to be effective [5,6]. Furthermore, an increasingly preferred aspect of display support is the integration of multimodal techniques, which help in effectively distributing cognitive load via multiple modalities. An effort has been adopted by Microsoft Skype for Business, where information about the local audio status is provided to remote users by contextual, real-time graphical "hand-raising feedback" cues. The system utilizes a user's co-locating multimodal feedback by displaying the current speaking status and the status of remote co-attendees in the UI.

Cyber threat intelligence (CTI) systems are an essential component for enabling the layered security monitoring of autonomous vehicle control networks [13]. However, the realization of their potential is contingent, as the human operator must be able to manage, act on, and respond to threat data and alerts to be extracted from CTI products, rather than being overwhelmed and succumb to cognitive overload, leading to erroneous or delayed responses. Also, improper adaptation of the CTI product to the interface design used [14]—particularly when the intuitive information usage strategies are not followed and more complex product interaction patterns are enforced—can similarly induce cognitive load, further exacerbating the problems of threat assessment and response facing the human operator of the CTI product. Consequently, a measure and its optimal advisory placement need to be developed for improved user-system interaction in cognitive interface design for CTI products to help manage cognitive load and improve human performance and enhance decision efficiency.

3. Methodology

Threat intelligence is a management and protection program, with the main objective being to beat cyber adversaries. The program approach is based on several hierarchical levels called Massachusetts Institute of Technology (MIT) levels. In this paper, a mathematical system encompassing an autonomous vehicle’s security baseline is presented. This is the first time to the best of authors’ knowledge that AI is used in a threat intelligence fusion concept, to optimize the quantitative assessment of MIT levels 1 and 2. The operator in the car receives the level of risk in real time by a system, formulated as a simple tool useful just to monitor the eventual changing of threat levels crossing the thresholds between baseline and increased security. The solution of the problem presented in this paper is practical in nature and easy to apply also to other tasks in the field of cybersecurity where an adaptive risk countermeasure is necessary. This kind of model is identical to the Te-TIOP control synthesis process (Te-TIOP) presented some years ago, whose features lay on the capability to guarantee the value independence from high variations of several parameters and the capability to include the operators inside the learning scheme, so that to elaborate security policies.

[12] [15] [16]One important aspect of autonomous vehicles is connected to the vehicle's expose to different kinds of attacks, especially in the future scenario where much of the communication travels via the vehicle-to-everything (V2X) channel. In this scenario, the autonomous vehicle is particularly critical, in terms of possible cyber-security threats. In one of our previous work, we discussed the opportunity to benefit from a security system providing a set of preventive and reactive measures, to help avoid possible risks due to cyber attacks and protect the vehicle, its data, and the passengers. This system is able to guarantee the control of the vehicle even in the worst conditions by the use of control recovery measures, as also shown via several experimental tests. This system also includes a monitor assessing the behavior of the vehicle and estimating the critical situation imposed by the cyber attack, taking a series of preventive measures. In particular, it also includes a decision-making process for evaluating the secure cyber strategies when choices among alternatives are

executed. In this work, we propose a new system for obtaining cyber data fusion techniques and we use this original strategy as a proof of concept of how to guarantee the cybersecurity of the future autonomous and connected vehicle by a threat intelligence fusion technology.

3.1. Research Design

The current research is triggered by the flourish of intelligent-threat agents into the connected vehicle networks (CVNs). Recent studies have revealed the prominent cyber vulnerabilities to the CAVs. In response, the recent research focus has been on establishing the detection and mitigation solutions to the cyber-threats in vehicular environments, which are mainly modelled upon a top-down perspective. The cyber threat mitigation loops essentially aim at fast prediction and detection of the network's vulnerabilities. Fast detection pre-assumes an already determined corpus known cyber-attacks. However, in real-world, the future cyber attacks have the potential of being quite diverse and different from their corresponding known counterparts, for which successful detection at its first instances of occurrence may be substantially, if not impossible. Here emerges the pivotal role that cognitive science has to play. Progressive integration of cognitive sciences in the recent years have opened new pathways in modelling and understanding human cyber decision making and cognition [2].

This research seeks to investigate the effects of cyberattack alerts on the cognitive workload of control decision-making under three visions: a textual interface, an augmented reality (AR)-based interface, and a mixed design of both interfaces. The main contributions of this research lie in establishing a basis for optimal design of driver-aware cybersecurity interfaces for autonomous vehicles using real-time cognitive load inferences [11].

[13] This study contributes to the enhancement of cybersecurity in autonomous vehicle networks powered by machine-generated intelligence using a collective intelligence approach. I believe that the main challenge lies in fusing individual threat data from individual algorithms to improve the cyberattack detection rate and gain foresight into unseen and future cyberattack technology. The current research aims to evaluate the cognitive demand for cybersecurity interfaces in the CAV control system.

3.2. Data Collection and Analysis Techniques

The authors of [17] analyze the feasibility of implementing a framework that facilitates multi-vehicle cooperation and collision avoidance in automated driving. The ultimate objective is to contribute technological solutions to enhance road safety. They propose the implementation of a framework that includes an AI-based novelty detector. The threat of anomalies on automobile interior and exterior signal buses is discussed since these anomalies can disrupt vehicle functionality. In this work, we explore different vehicle control strategies depending on the cooperation level. From a car control perspective, this work proposes a risk-based vehicle threat assessment scheme. The discussed mechanism could help to achieve acceptable and robust vehicle behavior and reduce road traffic incidents. A good approach to build a more effective assistance for drivers in automated vehicles (AV) might rely on combining knowledge from well-known studies on cognitive load and on the specific characteristics of the new technologies, but for wide adoption they must embed an optimal cognitive model.

Semi-autonomous vehicles are becoming increasingly common on roadways. The authors of [6] state that enhanced connectivity in modern automotive industries brings new challenges of security and privacy. These challenges must be addressed from the early stages of automotive design, as security issues in in-vehicle networks can jeopardize safety. Meanwhile, threat assessment (TA) is crucial for the safe operation of autonomous vehicles. When a TA occurs, a key goal is to identify the nature of the situation. The use of Artificial Intelligence (AI) and intelligent techniques is considered essential to effectively and efficiently resolve potential driving and navigation issues. In-vehicle protocol threats are a constant reality in the US automotive ecosystem, and it is vital that autonomous vehicles (AV) security analysts understand these threats.

4. Threat Intelligence Fusion Techniques in Autonomous Vehicle Networks

Moreover, intelligence assessments performed using both high-level road traffic and low-level cybersecurity nodes can fill different use cases in the modern autonomous cybersecurity ecosystem. Consequently, when this low-level perspective could be influenced from modern in-vehicle frameworks, a high-level traffic security layer may be more concerned about compliance and regulation. A comprehensive wireless and wired vehicle network has been defined for high-level security layer independent of in-vehicle protocols. On the other hand, analyses about low-level in-vehicle frameworks have been conducted related to hardware-software incompatibility, proving low-latency requirements of the peculiar protocols. While identification, categorization, and prediction of known and unknown cyber attacks are typically important for the overall cybersecurity of modern autonomous vehicles, creating a hybrid approach with the ability to integrate a Cognitive Load-inspired security interface within the digital cockpit, this approach aims to secure that all involved human-in-the-loop decision making, including those related to incident response and recovery, are facilitated as effective and efficient as possible under the human cognitive constraints they have to operate in.

Modern vehicles, autonomous vehicles in particular, priorities safety-critical security use-cases such as cyber attack detection, intrusion response, and recovery from advanced persistent threats (APTs) and various attack vectors [6]. A carefully examined threat landscape informed by multiple practices, and decision-support can aid in the anticipation of potential incidents, providing insights in real risks and their impact on the vehicle systems [13]. In real-world implementations a need exists for instant detection, intervention, and analysis of all abnormal in-vehicle scenarios. However, the classical security concepts deployed in current vehicle architectures, or manin-the-middle have shown to be insufficient to properly protect these intelligent systems due to the rapidly increasing amount of potential attack vectors. In order to adapt to the higher dynamic load of potential in-vehicle known and unknown attack vectors, artificial intelligence (AI) and machine learning (ML) techniques are adopted to guard the security-related issues impacting in-vehicle networks by effectively being able to identify, categorize, and predict potentially known or unknown attacks.

4.1. Definition and Scope of Threat Intelligence Fusion

[18] The first step of the Method to Build and Automatize Intuitions inside the TaNaRiG is to define and delimit the scope of the problem at hand, which is presenting a new informative system in the autonomous vehicle control interface [34, 35]. The interface needs to deliver informations concerning the cybersecurity and is part of the human–machine interface (HMI) on the side of the Human–Vehicle Interface (HVI).[9] Our Techniques are particularly focused in the definition of a TaNaRiG of the matrixes, or of the layers of the All Data Classes at TwM R Critical, across the All Lz, and the output layer of decisions at C Differentiated in terms of the automata setting all over the TaNaRiG. An extra layer, much more complicated, containing all distinct modes of viewing the All Actions wanted that could be taken by the car, and of their successive consequences on the speed and acceleration of the car and thus on their next speed and positions could be added to the automatically build and automatized system in a subsie system over the action-choices tuple of the TaNaRiG.

4.2. Applications in Autonomous Vehicle Networks

To counter threats in the AVCS and protect users, countermeasures must be embedded in these systems to monitor and protect all broadcasting events. These interfaces can be LCS (Lane Change Signals), MDS (Manual Driving Signals) or other such minor events which trigger co-drivers' involvement. These interference methods can affect each task in a variety of ways, changing the response time, or the frequency of the cognitive switch between AVCS and the co-driving task. As various aspects of the visual and auditory intrusion occur on numerous entry levels, it is important to elaborate the effects of various interferences and pinpoint whether certain systems are more resistant to such frequent or abrupt interruption, to ensure potential improvements in interfaces for AVCS, particularly in situations where automation fails and the driver must be able to take back control [18].

Autonomous Vehicle Control Systems (AVCS) are a prime target for cybercriminals, seeking to exploit their vulnerabilities and cause accidents [19]. As the vehicular infrastructure becomes more interconnected and the surface area for potential attacks and infiltration swells, it is essential to monitor the various intercommunications of the AVCS and assess the implications. In modern Vehicles to Everything (V2X) networks, the diversity of sensors and data is captured thus, resulting in complex fusion requirements of the data from the various networks. Further, the expansion of the V2V communications allowing the direct exchange of Cognitive Load Dual Task - As a measure of the holistic mental effort, driving events, puts the vehicle at a risk of interference in the wireless interface and possibly incites dangerous situations. The modulation of the driving events can be achieved at various degrees of severity and control of AVCS, from tweaking the outcomes at an intersection to cause accidents to more subtle disruptions in the vehicle's trajectory to damage traffic flow and increase the stress on driver(s) [20].

5. Cognitive Load in Cybersecurity Interfaces

[7] [18]Prototypes of autonomous vehicles are a critical testing ground for the future of transportation. As autonomous vehicle prototypes become more widely road tested and human passengers become less and less needed as backup drivers, the time required to perform a handover for human drivers to resume vehicle control after an autonomous mode becomes less of a requirement. Despite a successful transition from autonomous to manual control in which there is still a human backup driver in the vehicle, the transition period for

the human back-up driver was recorded as high cognitive load in experiments. High cognitive load leading to increased driving errors could potentially overlap with high cognitive load from a cybersecurity system that provides warnings and monitoring, particularly if it is not well calibrated to the driver's expectations and preferences. As in many human–machine interaction scenarios, system use is more likely to lead to acceptance and use over time if it operates at a low to moderate cost to the user. Our objective was to explore user needs for the design of warning systems for autonomous vehicles. There are many mitigating strategies for reducing cognitive load impact. From visual static (e.g., color coding) to aural static (e.g., alarms or canned warning scripts) all the way to dynamic, context-aware static and dynamic displays (e.g., vibrotactile, HUD displays) are all potential solutions that can be effective. Within all of these solutions, less complexity tends to be better, with less text and fewer colors and shapes making perception and decision-making likely to operate at more optimal levels. The use of AI and intrusion detection systems to protect and shield an autonomous vehicle from both attempted physical cyber threats via their sensor-based hardware as well as remote threats sent on the vehicle bus or over communication links can be crucial for preventing harm and damage to vehicles and passengers. However, cybersecurity interfaces that function as surrogate trip drivers in place of a human trip driver or co-driver must be programmed to be well calibrated to the human user. When an environment or interface is not having to be held as constantly monitored or when the active use of cognitive resources are required for another task, then a cognitive trip driver or warning system can be more aggressive in its warnings and reactions. So the optimal warning system needs to be aware of concurrent cognitive loads, be context aware, and provide warnings.

5.1. Definition and Measurement of Cognitive Load

In order to measure the cognitive load while driving, different approaches have been proposed in literature. One possibility is to measure task-related brain activity. In a study on the working memory load involved during driving, Kuzyniak, Zilic and Ramadani [7] concentrated on detecting the driver's safety during the interaction with traffic signs. They measured Electric Encephalogram (EEG) as a response to the tasks. In the context of network security, the study of Lewandowski, Woods, Eastwood, Ocana and Rallis [21] demonstrated the EEG changes employed in identifying TCP/IP stack vulnerabilities. In this study, they used the classification framework, guided by the Inter Process Communication (IPC) headers for seven different operating systems.

As can be seen from the fusion architecture and the defined vocabulary, multiple layers are involved in the fusion of threat intelligence (TI) data for autonomous vehicle (AV) cybersecurity from the seemingly purely technical level through to a psychological and cognitive level [ref: 0bf7a2da-4a2c-4567-8e76-2877c38d8728, ref: 3ffe003f-a33a-44cc-98af-7304ee4228d9, ref: 714029f8-3aa6-4814-bcf8-184b63fa856d]. The aim of the present section is to provide insights into the cognitive load experienced during autonomous driving tasks in order to develop optimal cybersecurity interfaces. The generation of cognitive load necessitates cognitive resources, which are however limited, so that reducing unnecessary cognitive load is an important objective in design. In human–automation interaction research, it is well-established that a mismatch of workload between operator and system can have numerous detrimental effects on human performance and wellbeing— both operative and cognitive, ref: 714029f8-3aa6-4814-bcf8-184b63fa856d].

5.2. Factors Influencing Cognitive Load in Cybersecurity Interfaces

Several studies have shown that working memory is of key importance for performing security tasks related to the recognition of fraudulent websites [4]. Flynn and colleagues (2019) found that participants who had been highly loaded on a nearby working memory task were less able to spot fraudulent stories as fake. Participants who viewed misinformation stories were twice as likely to label them as fake news as were those who viewed the control headlines. On the other hand, Fly and colleagues (2019) also found no effect of working memory load on visual misinformation detection. These findings highlight that variables such as the stimuli used and participants' prior experiences and knowledge about the subject matter may account for differing effects of working memory on social engineering attacks.

Two models have been developed to explore the influence of individual differences and prior experience with technology on the cognitive load related to cyber security tasks [22]. Two factors were found to be of significant influence on the cognitive load of cyber security tasks. Specifically, the frequency artifact contains all items that are related to daily activities both around the home and at work. Four factors were created to represent the four groups of significantly loaded variables within the Rortal. The leadership fac amongst all nine of those items, the classification of the Cognitive Load index into these different subcategories highlights the various ways in which the to-be-remembered items may interfere with choice of text and colour in

6. Designing Cybersecurity Interfaces for Autonomous Vehicle Control Systems

Vehicles are rapidly transforming from purely mechanical to comprehensive cyber-physical networks. Autonomous Drive (AD) vehicles and Cooperative AD (CAD) have exponentially increased the attack surface [18]. The in-vehicle network comprises ECUs, sensors, actuators and other telematic components. There have been extensive breaches all around the globe, affecting millions of cars. In order to molt a safer automotive ecosystem, a bunch of secure principles and Guidelines have been proposed in the last few years. Existing cybersecurity architectures of AD systems focus on the orthogonality of security and safety concerns. We posit the necessity to offer a systemic approach towards both safety and cybersecurity for AD systems . The architecture design of automotive cybersecurity mechanisms can be designed to evolve into a more precise and resilient hybrid approach that zeros in on cognitive load mitigation (design orientations against adversarial attempts of attack underpinned by psychological principles of attention, perception and schemata). Cognitive Load considerations can then arise at three different levels, and AD system design needs to consider their feasibility and generalisability: - System Architecture: aiding design with the capabilities of automation in AD systems, and research in connectionist parallel processing and rule based cognition in cardriving behavior as introduced at Level I; - Signal Mechanisms for Agency: regulations and paradigms for a natural interaction between the human and the autonomous co-driver-car are topics that will be discussed as AD systems are continuously evolving at Level II; - Experiential Prototyping: blending interaction and User Experience (UX) Design of the HMI with cybersecurity, as considered in Level III. We present a preliminary review that will aid architects and design personnel of AD systems in their efforts to augment existing systems with security disregarding or health realted aids, and to prevent their AD systems from being derailed due to the limitations in HMI presenting indiscriminate boundaries to in-vehicle network functions [7]. At this architecture level we point to advances and gaps in approach to enhance AD systems from orthodox cybersecurity into a systemic approach on neurological underpinnings. This is inferred via a structured summarization of the road following standards and proposals. Ultimately, we must prevent the AD systems from being derailed since there are no HMI boundaries in in-vehicle network protocols that present discriminatory levels of control, and AD systems are intrinsically designed to perceive and manipulate in-vehicle network activity arrays back without a regulated understanding of attention, perception and memory [15].

6.1. User-Centered Design Principles

In order to counteract the influence of a cyberattack optimally, the technologies of cybersecurity have to be designed “from the ground up” with respect to their effects on the cognitive and motoric faculties of the users. “Anomaly detection”: For the early detection of cyberattacks, the human assistand should support the driver and offer the possibility to manage the situation with priority assistance and early detection of cyberattacks. This could help to reduce any increased degree of strain on the driver. Here, machine learning can be used for a sophisticated design of the human–machine interface in security areas. Semi-autonomous driving functions also alleviate the load on human drivers in classic driving scenarios, while only certain, low-risk driving operations are transferred to the pedestrian’s ability. As opposed as human drivers, vehicle’s relative to its environment is determined the same way with autonomous vehicles by sensors and driving functions. To prepare for the possibility of a full takeover by the human driver and in this way to better anticipate the form of action, it is therefore recommended to take visual, acoustic, and kinesthetic human–machine interfaces into account in the design of autonomous cybersecurity interfaces [10].

To effectively counteract the impact of a cyberattack, the design of an AV must encompass both human-centered usability issues and user-centered decision-making abilities. A user-centered design process is recommended to address human-centered usability issues in AV cybersecurity [23]. A test and advice process may not be beneficial in an aversive safety-relevant AV scenario. Human-centered design techniques such as “Discoverability” and “Feedback and Dialog” have the potential to enable any kind of user to interact adequately with a system. However, despite this, the terms “usability,” “user experience,” and the particular requirements of drivers are often not adequately taken into account in the literature on AV security.

6.2. Integration of Threat Intelligence Fusion Techniques

A novel Reactive Autonomous Intrusion Response System (REACT) that allows a vehicle to respond to incidents instantly and without relying on a V-SOC (Vehicle Security Operation Centre) that is embedded in the vehicle interface is being proposed in [16]. Unlike traditional IDS/IPS systems, the suggested response mechanism allows the vehicle’s intrusions to be blocked by having them evaluated against potential responses and then using the highest-evaluated response. The evaluation system uses Fuzzy Logic Controller (FLC) to determine which response to implement based on the highest input. The evaluation system can work in parallel with the maintenance system. The Thomas Steiner model is created to predict the total number of systems in the future using a Predictive Maintenance (PdM) algorithm. This assists in monitoring the status of the system. An evaluation mechanism is then executed to assess the risk effect of each feasible response. This aids in deciding the most appropriate non-modal response.

To realize a safer and more secure operational environment, in addition to the aforementioned mechanisms, a learning model-based threat intelligence fusion strategy that combined both static (knowledge-based) threat intelligence and dynamic (behavior-based) threat intelligence is proposed [2]. Although static threat intelligence is able to enhance the accuracy of analysis for security risks, it requires prior knowledge, and can generate a large number of false negatives due to the possibility of discovering known threats in an unknown manner. Therefore, learning models are used in the proposed method to adapt static threat intelligence from static intelligence data to the dynamic characteristics of the data. Specifically, the two respective feature extraction processes for static intelligence features and advanced intelligence features from raw data are used. This divide-and-fuse method avoids the problem of information loss. The threat intelligence data A that contain only expert knowledge are divided into two sets of features sets according to the same structure of the data. The proposed method can therefore adapt any static intelligence dataset A to the dynamic characteristics of B by training machine learning models on B.

7. Case Studies and Practical Applications

The introduction of autonomous driving systems requires a more critical awareness and control of the cyber-physical properties of the new driving technologies that are going to integrate soon or are transitioning them to the automotive markets today. Automotive companies are expected to adopt mediation-by-design methodologies to develop and maintain connected vehicles with autonomous driving capabilities to overcome these challenges. Producers are also expected to detect, evaluate, and resolve known and unknown cybersecurity threats to treat this problem. The growing public awareness in recent years of the potential negative impact of the automotive industry is quite clear for these goals. Hence, to respond efficiently in a structured way to these challenging cyber physical trends, defining connected vehicles as a component of cyber-physical systems may integrate the engineering and managerial task of securing vehicle fleets through being FLRLD systems over and above protecting single vehicles. Cybersecurity of cyber-physical systems needs to address these newer needs forecasting roadmap of keeping systems secure-by-design. Therefore, we automotive expertise of secured-related and analytics goods try to advocate the concept of FLRLD as being the salient and central cyber-physical management element to support the predicted security-by-design concept of cyber-physical vehicle systems.

[24] Automotive developers are facing ever-growing software-based complexity for vehicles, leading to elevated cybersecurity risks. This rise of complexity was fueled by state-of-the-art concepts such as Mobility as a Service (MaaS) where end-users can lease cars rather than owning them. This challenges the traditional car concepts of engineering, marketing, and sales, depending on the products and knowledge area. They exacerbate the digital transformation of car manufacturers from technical, process, organizational, and officer-related perspectives. Integration of the aforementioned factors also enforce new challenges. The most challenging gets integration of moving transportation in and between complex connected ways, which should include varying infrastructures, sensors, actuators, vehicles, vehicle sharing devices, other mobile subjects, which might include other sensors, sensors and actuators provisioned in cloud services, and even not connected, but cloud-provisioned reliable vehicle-to-anything (V2X) connectivity and services. Moving and stationary vehicles will be dynamic components of Internet Solutions of Things (IoT).

7.1. Real-World Implementations of Enhanced Cybersecurity in Autonomous Vehicles

Known are various families of security control systems cyber security researchers have made and are still developing for land surface transportation infrastructures. Such systems physically and logically separate exposed safety-critical signal processing functionality by requiring that encrypted messages be physically separated in two networks originating at the same point in the exposed software stack control center of some subsystem of the exposed software stack and shared among any newly arriving control center, newest control center, and its adjustable weighted mix of some fixed set of other software components. They also separate out manually or algorithmically chosen logic encryptions from lossless encryptions which slow down processing speed. Typically the protocols providing humans with either apparently important only feedback from the realm of vision or the realm of sound only based on their preference are intentionally made audio-visual noise-indistinguishable in which even the messages from mutilated and still partially exposed software calculated using those poorly exposed software are made audibly noisy and visually noisy at perfect or near-perfect intensity [25].

Cybersecurity engineers are still trying to establish the safety of autonomous vehicles in the midst of recent public trials of self-driving vehicles from startups, automotive manufacturers, and technology firms around the world. The collective experiences and the findings from the recent cyber threats have made clear the gravity and the immediacy of the need for a secure perimeter to safeguard the privacy and the long-term physical safety of autonomous vehicle occupants [7]. This security needs the ability to be updated reasonably often in real time, but since autonomous vehicles will enter densely packed environments with future "SAE Level 5" autonomous vehicles likely to share the roads with conventional fixed-route mass transportation vehicles, we are now asking for secure automotive communication systems with the ability to securely delegate security-critical functionality with ease to recent subscribers perhaps untrusted by the previous systems with the same work assignments for the exposed control systems [11].

8. Discussion and Analysis

The neural networks diagnose technical problems within AV networks by processing data and then decide how to act or automate the driving in different circumstances, like through a range of the collision risk [25]. Procedure cyberattack could extract essential information regarding the AV speed, the position, and as the distance to circumnavigation. The SaVID application, which assists the driver when the vehicle is in stormy or foggy mode, had to be warned as to the products of the multiple accidents involving the NaPrS episode. This paper illustrated only penetration testing and showed some security issues with the Autonomous Vehicle network. For the protection of Autonomous Vehicle networks from Cyber-attacks, the Cyber Intrusion Detection System (CIDS), is necessary to improve the security of the Autonomous Vehicle care networks.

Some challenges that Autonomous Vehicle (AV) networks face are: public skepticism, legislation and policy, cybersecurity breaches, system noise, infrastructural communication errors, unanticipated failure and integration errors, latency and energy consumption, ethical concerns, enforceability and liabilities, and emergency protocols and fallback identifiers [13]. The security, privacy, and establish data access rights and protection centres constitutive concerns for Autonomous Vehicle (AV) networks. Cybersecurity threats in Autonomous Vehicle (AV) networks are a serious cause of concern. This paper has showcased the vulnerability of AV network security and privacy through initial penetration testing, and several crucial issues related the Semi-Autonomous Vehicle Incident Detection (SaVID) app and the ADAS driving assistant.

8.1. Interpretation of Findings

The findings from this study demonstrated a strong association between acceptance determinants for cyber security management systems and cognitive load imposed on drivers. Thus, the study concluded that the reliability, which is referenced as performance expectancy, user friendliness, ease of learning and clear task visibility, which reference effort expectancy, and threat interaction, which references situational awareness, all contribute significantly to the total cognitive load imposed on drivers during the management of cyber security alerts assessmen [17]. Although this study validated three key theories—Standard Protocol, HateCrimeAvoidance and False Acceptance, as being primary cybervisual diligence components, these findings have implications for potential human cognitive challenges that can be eliminated through automation and algorithmically enforced trust in the management of cyber security Risks.

The study investigated the cognitive load when drivers participated in three cyber security related activities; a cyber security assessment activity, a cyber security alerts assessment and acceptance activity, and hypothetical driving scenarios (see the method given in Section 4). The usability assessment of the in-vehicle design was based on the two individual assessment measures being the NASA Task Load Index and the Subjective Mental Workload Scale. Both activities utilised the STAMP model [3]. The NASA Task Load Index was adopted to measure the drivers' task load in three sub-dimensions: mental demand, temporal demand, and effort, whereas the Subjective National Workload Scale was used to gauge on three sub-dimensions, effort, frustration, and performance. Dual-task driving performance was measured using a test of cognitive test involving a simple reaction time task.

8.2. Implications for Practice and Research

Research into increasing the cognitive load of user interfaces and investigations of procedure and policy violations must be conducted as the interfaces of this paper indicate that participants are easily manipulated. Reducing the potential for cyber threats and the reaction time of the user, who often only realizes an error when something fails, will be the primary direction of the future research and design effort. We have detailed the principle of fusemon, a unified and coherent interface and have demonstrated through it that increasing interaction between the interfaces and a user leads to better ERP results. The effectiveness of coherent presentation on interface future studies will indicate the the improve of reducing cognitive load and reaction time for the user. [18] [6]

To address the implications and impact of military-specific challenges, several close-to-military case studies have been examined here which contain step-by-step actionable lessons for technologists and UX researchers. However, this review is not intended to present the solution to cyber defence training problems; many solutions to these problems must be tailored to the individual situations. It is, once again, important to have user experience design and interface design specialists who understand these needs, but who are also willing to get their hands dirty. The HCI processes employed did not do that, with the interface designers doing all the forms and analyses and the usability engineers discussing with the Subject Matter Experts only at the end of the process. The amendment of this process is a possible improvement and will be critical to the effective design and evaluation of such systems into the future. The military restricts oversight of software construction to partner nations; this is risk-averse, but it does do extra to assist the progress of their issues.

9. Conclusion and Future Directions

An intelligent vehicle–driver interface that serves to protect the operation within the integrated cockpit using learning-based decision-making for autonomous vehicle cybersecurity as part of an integrated cybersecurity management structure to be built, in which real-time safety and cybersecurity analysis can operate together. The minimum cognitive load needed to make reproducible driving decisions at various levels of security awareness and trust within this system architecture should be further explored, and humans should only be included within the driving decision-making process once. The findings can be used as a foundation for the design of a highly reliable cascade of defense mechanisms. Until then, the vehicle–driver interface must be guaranteed to provide minimal navigation for a human in distress. Therefore, research and development remain needed in this area of study to ensure a safe autonomous future. [3]

The increased demand for convenience and quality of life has fueled the swift advancement of driver assistance systems. Recent improvements in the artificial intelligence field, particularly within the training of deep convolutional neural network models, have led to advancements in autonomous vehicle functions. However, encryption for in-vehicle communications is usually purposefully omitted to assure minimal end-to-end latency between processors and controls within the vehicle. [4] With this system architecture, connecting to AI cybersecurity systems can offer enhanced protection. Approaches to secure real-time operations within the integrated cockpit must accept that these operations are restricted and the cover network is only capable of carrying low data rates.

9.1. Summary of Key Findings

In contrast to classical distributed automotive system architecture, in which the majority of functional electronic control unit (ECU) have been domain-localized, software and compute infrastructure will be widely distributed across different in-vehicle compute nodes in future automotive system architectures. Such code steering is called software-defined vehicles (SDVs) vision. Software distribution in automotive domain brings many benefits but also aggravates cyber security problems. Specially, performing security checks on the vast software data and enhancing the measures of security enforcement demand high cost and complex management. Also, the distributed software system and the enhanced capability of in-vehicle communication may lead to many complicated and cascaded security threats. It is necessary to address security issues from a hierarchical and interconnected perspective [26].

Future mobility services require a security-first architecture based on an end-to-end approach for cybersecurity which covers the vehicle, data processing centers, after-market devices and the connection to the Internet. A successful attack to one of these system components could have dramatic effects on the physical and cyber security of the entire system. The Software Era in vehicles, with advanced and interconnected software, needs to cope with cyber and physical automotive security challenges. A clear understanding of their interdependency is essential in realizing secure, future-proof vehicle architectures [24].

With the increase in connectivity and the rise of intelligent vehicles, autonomous vehicles are becoming a reality. This increasing digitalization of the automotive industry paves the way for new services and business models. Following these developments, the prevention of potential cyber threats is a key requirement for automotive systems and mobility services in the automotive and mobility sector. A successful attack could monetarily harm the affected vehicle owner, have significant negative impacts on the trust-worthy reputation of the targeted brand, and permanently violate customer trust in intelligent vehicles in general [6].

9.2. Recommendations for Future Research

From the given results of different car user groups in study 2 it seems that a reduction of the intrusive, warning-based information design of cyber security interfaces is mandatory. Although such implementations could be helpful for re-informing and attracting the focus of authenticated users after an attack warning had occurred, the overall demand for performance measures through usability, propensity to error, and user efficiency, prepared for attackers attacking the user, should receive consideration. Such design solutions following the concept of artificial intelligence really aimed at consultation with the driver could help to counteract the described attacker strategies here in the context of an overwhelmed situation. It is important to hereby make such support quickly available after a cyber-attack has been identified. We strive for correlating results in conduit with a consideration of cyber strategies that are more unique with the shock of a recent cyber-attack. This is the only way really to oppose the attackers' strategy of overwhelming a driver by preventative impairment.

For the valid implementation of cyber security measures in the automotive domain, new software technologies and the recognition of specific side-effects such as the investigation of the user-burden when implementing new safety measures should be addressed. Our core concept lying with the CP approach has demonstrated high threats of intrusion attacks; not only in order to turn of engines, albeit to lock vehicle functionality altogether for a specific period of time until the systems are power cycled. Cyberattacks and malicious data manipulations can concern every subsystem of networks, like the infotainment head unit by faking traffic anouncements on car radio. We advise an increased focus on better understanding and optimizing user cognitive load of human-machine interface and the human side, including attacker typologies affine to CP approaches in simulated human practice research contexts. More risk analysis and planning should be accomplished within modifiable and assessable simulation environments. Furthermore, a focus on the evolving and dynamic threat analysis of attacking strategies following attending the security strategies could be explored. A combination of these factors and the recognition of the threat by the driver offers additional potential; not just to react to cyber attacks but to actively set security strategies in future automotive interfaces. The findings on the influence of cognitive load on the use of complex, embedded, safety-relevant cybersecurity systems.

Although the concept of iteration in cybersecurity seems to be trivial, inferring results and implementing practical prototypes do not necessarily transfer the theoretical designs routinely as new design paradigms are being launched. The suggested studies should be further substantiated by new systematized architectures so as to support an intelligent fusion comprehensively going beyond centralization or isolation. In order to facilitate the understanding and generalization of our results, our approaches should also be validated and implemented on other security design approaches of mostly similarly exposed areas.

Article [24] has formulated the design approaches and recommendations for the development and enforcement of automotive cybersecurity in the technological domain. This paper, however, focuses primarily on human- factors and the researching of cognitive load (CL) in cyber-physical systems such as autonomous vehicles. Nonetheless, the security measures and the design of the vehicle networks fundamentally determine the overall available level of security within the overall environment of autonomous systems.

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.