Usability Evaluation of Cybersecurity Training Programs for Autonomous Vehicle Operators

By Dr. Aliaksandr Siarkou

Associate Professor of Computer Science, Belarusian State University (BSU)

1. Introduction

Given the deficiencies in human-focused cybersecurity research, the authors set out to explore the usability of a subset of training requirements in the autonomous vehicle domain. This paper focuses on the question: Can trained operators perform their duties according to the security design standards when exposed to cybersecurity threats according to situational intelligence? The training assessment program that addresses this question is referred to as a usability evaluation, which measures the data's quality in an inspection process. The research examines physical security, cybersecurity, and other high-level applications in light of situational reinforcements for identifying suspicious behaviors. Furthermore, the full design specifications and training sequences are used to help participants perform their duties. The evaluation results determine the impact of training when participants perform a set task simulation. The paper thus answers the research question. Guidelines and recommendations that are suitable for the 19 tasks are then presented.

The emergence of autonomous vehicles (AV) has changed the land transport industry significantly, yet there are shortcomings regarding cybersecurity standards. As proposed by the National Institute of Standards and Technology (NIST) Special Publication 800-164, autonomous vehicle cybersecurity designers should discharge judgments which should include, but not be limited to the threats, the context of associated operations, and the potential risk scenarios. Further, advanced technology for autonomous driving has created demands for operators that are proficient before acknowledging safe deployment. Training such operators poses unique challenges which will require unique solutions.

2. Literature Review

Zhang et al. refer to the cybersecurity training programs for autonomous vehicle operators reviewed in this study as Autonomous Vehicle (AV) Operator Training Programs. Student assessment in cybersecurity training has emerged as one of the most challenging and time-consuming tasks in cybersecurity education. Since cybersecurity is one of the most widespread and serious challenges in cyberspace today, instructors need user-friendly technologies to automatically assess their student learning. In the "Digital Millennium Education" era, a few technical advances are following the same trend since the Covid-19 pandemic. For instance, in the college cybersecurity education area, two ongoing and internationally recognized trends are as follows. As the first trend at this level, many cloud-based training platforms are widely known, such as Cybervista and ONLC, for delivering instructor-based cybersecurity teaching significantly. When focusing on the second global trend, many colleges worldwide have shared numerous learning activities such as the Mastertrack program on cyber security courses on campus, the Udemy platform and Massive Open Online Courses, using either synchronous or asynchronous teaching approaches.

Since the advent of fully autonomous vehicles by companies such as Waymo and Uber, the cybersecurity of self-driving cars has gained increasing attention. More recently, with the opening of commercial robotaxi services, training programs for AV operators have also been developed. Although cybersecurity training programs for AV operators prepare them to handle a new and complex vehicle encounter, there have been few to no evaluations of their usability. As a result, the usability of cybersecurity training programs for AV operators currently remain unaddressed. This study sought to explore the usability of two cybersecurity training programs for AV operators by: identifying user challenges in those programs through a survey; and analyzing the effectiveness of two automated user-behaviour analysis systems for improving the security of autonomous vehicle operator education.[1]

[2] [3]

3. Theoretical Framework

Usability assessment provides metrics and heuristic evaluation models as well as system and user performance aspects on software design processes [4]. Usability studies have been widely applied to evaluate many types of e-learning environments and these studies have confirmed that e-learning benefits from usability analysis, design, and evaluation methodologies. Due to the absence of us- ability standards of the e-learning environment, many researchers have

utilized their own heuristics and developed usability evaluation tools parallel to traditional software products (Huang et al., 2005). Usability research on these systems was focused on the visual design and organization of the UI, response time, error messages, color, and the use of multimedia elements and has focused on the development of plug-ins and tools. There are many standardized usability surveys to measure traditional websites, in particular the Software Usability Measurement Inventory (Bangor et al., 2008). In recent years, several different authentication that measures the effectiveness and efficiency of adaptive cybersecurity system were designed and developed on the critical infrastructure and interdisciplinary nature of cybersecurity technology as they employed classical principles of user evaluation and their related tools for user interface design. The above examples target the conceptual design of software, but not the software that will be designated for cybersecurity training programs [5].

Nowadays, as a cybersecurity expert, people are confronted with handling different layers of complexity and ensuring that their systems are protected from various threat agents. While autonomous vehicles have several well-identified safety issues and industry standards that set out the safety validation process of such vehicles, there is a need for the definition of a cybersecurity training program for the operators of autonomous vehicles which will form a critical part of the safety case. This paper provides a theoretical framework for the usability evaluation of cybersecurity training programs and sets the stage for providing practical guidelines on the design and implementation of test tools for the domain.

4. Methodology

The approach of the methodology ARME—the Agile-Risk-Management & Evaluation will be the following: Agile: The ARME process focuses on iteration and adaptation to improve risk management—key elements of agile development (if possible) and future research. Risk Management: By identifying and preventing potential risks in the design phase, mitigation of the criticality and likelihood is possible. Evaluation: The methodology will include a structured evaluation process with a focus on the AV Operator's ability to perform the required cybersecurity skills. This will be evaluated according to their completed practical tasks to ensure their maximum understanding when performing AV-related skills. Therefore, in the study proposed, the researchers validate potential scenarios with the designed expert

framework. They also validate hate level of observed (in real user training, in a focused group laboratary). [6]

The section introduces the methodology consisting of ARME—Agile Risk Management and Evaluation. Within ARME, the researchers developed a systematic process for analyzing risks, mitigating risks, evaluating risks, and therefore managing risks. To do so, the researchers introduced a performance-based usability approach that offers a consistent and systematic analysis of the usability impact to tasks, system, and the effect of scenarios on the system. Following the analysis part, feedback is provided as to what needs to be optimized regarding the scenario, system, and training methods. The ultimate goal of the described work is to develop expert-designed, scenario-based cybersecurity training for AV operators. The development process is defined by ARME, a three-step process of detecting flaws in her training concept, and defining methods for possible optimization. Very detailed scenarios ensure maximum contrast of training aspect for each skills. For strategies on mitigating IoT privacy and security threats, see Venkataramanan, Sadhu, and Shaik (2020).

4.1. Participant Recruitment

In order to validate user-centered design principles and raise awareness of vehicle cybersecurity attacks, the research included a follow-up evaluation. Future evaluations are necessary to assess the effectiveness of the vehicle cybersecurity training, as well as updated designs. Besides, in order to provide application-specific findings to vehicle OEMs and NGOs, the research will share its findings at disciplines forums such as the highly recognized annual conference in human-computer interaction. Pei suggests that the field acknowledges that proper training and vehicle design communication can play roles in vehicle cybersecurity attacks. Future considerations can assess the potential dangers of transfer learning on attacks on users, as well as the longterm implications of vehicle cybersecurity around the interaction-local vehicles aren't available for Malware protection.

[7] [8]A convenient sample with no specifics on participant availability can guarantee a convenience sample with extra weighting toward individuals with extra flexibility within their schedules. Qualtrics survey software was used for online survey distribution, piloting, and response collection [9]. There have been several discussions on what constitutes an

appropriate sample size in order to study how autonomous vehicles should communicate meaningfully with drivers. The sample size calculations for the ctl group and the treatment groups were as follows: according to the generally accepted ten to one ratio for independent variables to participants in regression analysis, the five demographic variables included in the model would allow for analysis with a sample size of 50 participants in each treatment group. Researchers have suggested that social science studies should include a minimum of 100 participants since advanced, user-focused, and flexible software was available to invite, yield, and manage participant data.

4.2. Data Collection Methods

Despite the fact that Virtual Reality-based training programs can be used for operators of autonomous vehicles, they do have a number of shortcomings, such as: causing motion sickness, leading to reduced concentration, are pseudo cybersickness, require a sufficiently large financial investment at the stage of the introduction of VR in the study of safety while driving indifferent conditions compared to classic driving simulators, difficult to use by people who do not have basic knowledge on general computer equipment, are not accessible to people with disabilities. It is possible to replace part of the existing training program with Virtual Reality-based education, which is both an asset and a necessity, given the potential of reality, in which we are driving our purposeful steps [10]. Moreover, the idea of allowing the autonomous vehicle operator to experience artificial people in a virtual social environment could be a useful addition to VR cyber-security training, and the idea of constructing a model of VR therapy for an Internet-dragging car driver, where the patient will use the VR program to simulate immersion in a virtual world and limit his/her exposure time.

The study aimed to assess and evaluate the usability of both existing and virtual world training programs delivered for operators of autonomous vehicles using methods based on the analysis of reliability and construct validity recognized by science representatives [11]. Also, we took the same research questions used in the direct research, but data collection was done in a different way – through virtual worlds, eg taking the associated Internet community information, inspecting and ordering it, and finally abstracting or summarizing it to collect it [1]. As a result of the conducted quantitative analysis, empirical generalizations that can be used to popularize virtual reality-based training programs among the parties involved in the development of autonomous vehicles were obtained. The conducted research led to the

conclusion that majority of the participants of the direct research saw the possibility of replacing some part of the existing training program with virtual reality. However, the evolved opinion resulted in the consideration and the idea of offering therapeutic possibilities of VR in cybersecurity.

4.3. Data Analysis

[12] The data was analyzed using a qualitative research approach in order to identify the usability problems in cybersecurity training programs for autonomous vehicle operators through interview responses and open-ended survey questions. Open coding method was used to identify usability issues related to goal effectiveness, training efficiency, and user satisfaction. As the result of the study, we identified five main sources of usability problems in the software and 1) in the middle of the session, the voiceover suddenly stopped; 2) the software was designed to work with mobile devices, but it was unstable and would sometimes not respond to mouse clicks or paint movements; 3) Qubes-Whonix was observed to be quite slow during the training, causing inconvenience for the users; 4) in Qubes-Whonix, 878MB update was needed after Tails was introduced, but an update was not performed before the training; 5) it was difficult to browse the Whonix gateway, unlike other tools.[13] We optimized tasks related to exploratory log file analysis in a visual interface by pivoting into a data-centric workflow. To destigmatize assessing students' socio-emotional states during training sessions, we created a telegram bot that can be used for real-time, subtle feedback collection in the users' natural language. Finally, we provide educators with an unsupervised machine-learning-based tool, the suggested case from the received feedback, which connects moments of confusion or satisfaction with relevant software, and spotlights the need to refine the tools and training environments [8]. We present the full design space of our three tools, provide the "essence" of the required adjustments suggested, justify the orphan defects of real-time user interaction in detections versus new capabilities. We offer practitioners a complete usability framework, methodologies and inbuilt analytical tools for continuous software improvement.

5. Results

The experiential evaluation results come from the cyber range exercises and are shown as representative screens (static and videos), quantitative data summaries, and analysis text from multiple perspectives, including multiple tools. The majority of cyber range exercises are

screenshot summaries of these virtual environments with trainee actions. In some cases, videos are included. These screenshots capture the actions the trainees are taking in pursuit of tasks throughout the simulations, in a coarsely chronological order. The quantitative data collected are summarized using a table. The summary includes the students in the group, the exercise conducted, the time step of the initial access and the victim operator, exploration and victim time, exploration type, victim-operator time, and the success type. The analysis is guided by three research questions. Although post-exercise feedback data are also collected after every exercise, the interview notes are important for supplementing the data and triangulating. Post-exercise feedback also provides some insights when available. The learning progressions tool's results are shown with representative output visualization from the trainees' digital footsteps and discussion from multiple perspectives. Individual trainees' visualizations are at the end of the discussion.

Results are segmented by evaluation approach first. Within the experiential evaluation, the results from the cyber range exercises are presented first with a representative exercise report and statistics from the quantitative data. Results from the learning progressions tool have a representative visualization. The results of the experiential evaluation inferential approaches are presented similarly by approach with details of task breakdowns and time estimations, suggestions for future training activities, and reports from the words reports' tool. The survey results include the demographic characteristics of the employees who completed the survey, a more detailed description of their experiences, and positive and negative feedback they provided. All results are synthesized as discussed based on the connections to the needs for new worker training cybersecurity frameworks and the barriers that suicide assistance chatbot design can overcome. In the following section, all findings and discussions use the functional security controls for the United States (US) National Highway Traffic Safety Administration (NHTSA) defined in the Mobility Safety Vision for 2020 and Beyond as the trainee-focused training touchpoints.

5.1. Quantitative Findings

Participants scored equally high at pretest on their ability to identify and protect data from being fed back to a service provider, and at post-test demonstrated a significant increase related to the same section of the evaluation. The mean pretest scores for the ability to relate cyber issues with laws and restrictions in the driving area market for self-driving vehicles and

its operation, related to Faction C, were both high and mean scores dropped significantly from pre to post-test. Experiment results mean scores for the ability to define "tunnel effect" and identify possible solutions related to the same significant drop in scores between pre and post-test. Finally, the mean scores for the ability to define situational awareness and to understand its relevance in the context of self-driving vehicles showed a significant increase from pre-test to post-test.

The analysis of quantitative data was conducted using the responses of the participants who took part in the two-day in-person surveys (n = 7), as online completion could not be tracked to match pre and post data. The data was analyzed using paired samples t-test and the repeated measures ANOVA, as required. The majority of questions pertaining to the learning objectives used a 7-point Likert scale of which 7 indicates strongly agree and 1 indicates strongly disagree. Participants liked the in-person delivery of the program, as indicated by the positive responses for those questions: learning experience, learning instructors use of multimedia and imagery, and that the program was never boring or did not cover necessary material. The analysis indicated strong mean scores at pretest for questions related to the ability to identify and protect good data to feed automated driving systems, and plan a safe route by choosing locations involved in cyberthreats. This increased at post-test as participants demonstrated a deep learning of these three sections.

5.2. Qualitative Findings

Open-ended responses were also collected to inquire more specifically about the AR activity. Prior to engagement, responses indicated a clear preference for interactive activities: "I think the hands-on activities were really helpful, we had to apply our knowledge towards what we had just learned. We would talk about [the function] of the photos and videos and how they applied to the real world." The facilitator's emphasis on the connection between the AR tags used in the activity and the car made learning about encryption for the infotainment system "pretty concrete." Many participants recognized the activity's educational value: "The car activity was very helpful." This was not unexpected given the literature evidence supporting the use of AR in the classroom. Our subsequent interview reveals an additional reason for the positive sentiment expressed by participants; the focus on usability and relevance during the curriculum design phase: "You really focused on showing how each thing is relevant... 'Why is this useful? Why do I need to know this?' I thought that a lot of classes miss. They aren't

focused on telling you why they are teaching you something..., how it connects to the real world." The use of AR in this specific context appears to have had an additional benefit in that it met an underlying pedagogical need expressed by students. In other words, the completion of the activity mirrors recovery from the PIT maneuver. It was found to be useful due to educators' attention to relevance. These comments are significant because they relate to the introduction, at a foundational stage, of the types of creative thinking and the critical questioning expected by introducing creative thinking and invention tools in the June 2020 SAE J3016 document. These latter comments are significant not only because they define relevance as a practical application of the material, but they also address the present lack of such focus in higher educational institutions in the United States. Negative comments (deferred due to a need for confidentiality) were also constructive.

The open-ended responses from the pre- and post-test surveys and from the semi-structured interviews administered following the driving test enabled a qualitative assessment of learners' experiences. Post-test, responses were overwhelmingly positive, with learners particularly appreciating the hands-on and experiential nature of the content. The following statement exemplifies this experience: "Just the interaction, not necessarily watching the presentation, but actually seeing the examples." Visuals, via images and videos, provided a cognitive anchor for the material: "It's not just the visual, but when you put them all together and hear [the facilitator] speaking and showing the pictures with it, it really gives you a firm understanding of how to put the information into motion in your head." One person mentioned that the material was presented in a logical order which aided in their understanding. Most endorsements, such as "I thought it was really interesting," conveyed interest rather than usefulness, which was a common sentiment among automotive feasibility studies. However, the following participant also recognized the practicality of the material: "It's important to think about encryption and how you make control logic. You can understand the basic concept and consider it. It's important to know the possibility and the weakness."

6. Discussion

[ref: 2f91accc-fc26-4f0a-b6a5-015cdfe7b43a, ref: 3df868f0-dd38-4a2e-931b-142e1503c4b6]The findings from the present study suggest that while there remains much to learn about exactly how to best train for cybersecurity aspects of AV operation, some aspects of HMI design and decision support system (DSS) design can have an immediate impact on the perceived relative

threat and efficacy of various cybersecurity approaches. This study makes trade-offs in research design (e.g., study population and industry task priorities) with the objective of identifying immediate technical and operational concerns. Some interesting findings regarding the value of feedback loops, DSS and stimulus and how they trade-off in regards to enhancing security postures for VRUs, AV operators, and operational decision-making generally have emerged from this preliminary work to set the stage for future cybersecurity training sequence design optimization.[14] The uptake of security training for AV consumers, a.k.a. vehicle operators/driver, will be dependent on both formal training curricula and the wider familiarity with new cybersecurity threat scenarios in the population. The speed with which a wider segment of the population comes to be more aware of AV-specific cybersecurity-relevant knowledge, will in great part determine the sustained effectiveness of driver education. If you start from the "end" of security training and assume the driver/vehicle operator is both a human sensor, classifier/recognition system, inputting observation information into the AV domain, it is clear that enhancement in this observation and reporting relative to new cybersecurity-relevant events can be a critical the way to integrate insights driven from this research tightly into future road users cybersecurity training.

6.1. Comparison with Existing Literature

Therefore, leveraging human factors research to enhance security is critical. This article also discusses extensive, multi-dimensional, and systematic approaches that can be utilized to (1) investigate the human factors that make technologically advanced systems vulnerable to security failures and threats, and (2) secure systems by incorporating human factors theories, knowledge, and methodologies in systems development and design [15].

Moreover, in autonomous driving, there is an expectation gap that users do not understand their roles and responsibilities and do not master the operation of AVS, and it is suggested that it is necessary to establish a new security culture that includes the social effect created by users. By integrating human resource development, organizational culture and social systems as a result, to improve cybersecurity, a comprehensive approach encompassing the entire value chain from the development and design stage of technological resources to the socialization stage is needed. Measures against cybersecurity are likely to succeed if comprehensive measures involving every stakeholder including users are taken.

[16] Research on human factors in the cybersecurity of autonomous vehicles is increasing, and there are grounds for reducing attackers' motivation and enhancing the cybersecurity of autonomous vehicles by influencing human activities. However, the impact of users' characteristics and habits on the actual situation in cyberspace and the degree of vulnerability is not well understood. It is necessary to investigate the characteristics of people vulnerable to autonomous vehicle errors, educational methods to improve information and communication technology-related skills, measures to improve the working environment by proper information and communication technology education and training of those in charge of developing human resources and systems, and of or reducing motivation for the behaviors of attackers [17]. It is important to identify methods to realize appropriate human resource training and education, technology implementation, organizations, social systems, policies and international cooperation to reduce the attack motivation of autonomous vehicles.

6.2. Implications for Practice

More specifically, our heuristic evaluation was able to contribute refinements to the design of the NMT training tool. In conclusion, our study adds to our understanding of the degree to which established usability heuristics are able to capture both the usability and user-experience of training tools for AV operator Cybersecurity. We found that the general usability heuristics were able to index the impact of a lack of content description for a specific exemplar analytical mechanic of the NMT tool. Heuristic evaluations also took the top hits presented in our previously described usability and user-experience led evaluations. [18]

Recent advances in connected and automated vehicles are anticipated to offer considerable safety, social, economic, and environmental advantages, such as lowering accident rates, traffic congestion, and energy usage. However, these technological advancements create new security and privacy risks, including access from hackers to critical vehicle functions such as steering, acceleration, and braking and the theft of personal data. Effective resilience mechanisms and secure design strategies for connected vehicles are essential to minimize these cyber-physical adversities. [17]In this paper, we critically evaluated recently proposed Cybersecurity training programs for Autonomous Vehicle (AV) operators against a set of standard usability heuristics. We further evaluated the merit of existing usability heuristics in the context of AV operator Cybersecurity training programs. The heuristic-led assessment produced results that were in broad agreement with those described in our detailed usability

and user-experience led analyses. However, our heuristic-led assessments also provided useful information about the usability of both the training tools, and about how users engage with and are supported by the Neurophysiological Model of Trust (NMT) training tool. The cascade impact following our findings is that we are now in the position to iteratively refine our AV operator Cybersecurity training tools in order to better satisfy the needs of their prospective users.

6.3. Limitations and Future Research

The redundant sensing-and-actuation equipment on an AV counteracts the failure on one part of the sensor, model, and actuator . However, the use of the HIPPA framework to show that a risk associated with AVs and AV-society interaction is related to the capability for making intelligent abducted assessments. This is not the appropriate type of approach in our case because the above approach is based on the social risk assessment related to AVs driving in the streets of L,A., and equipped with societal cognition systems . In contrast, suitable driving behaviors for AVs can be detected in the daily driving of the environment in which our studies are performed. These behaviors can be accepted and rejected by human cognitive behavior. Both of these approaches are suggested. It is a reverse three-phase decide, act, and categorize where another agent makes the categories associated with safety risks application domain.

Using both a controlled simulator, which can be used for controlled studies similar to this study, and a real environment like Virginia Tech's Perception and Action Laboratory, which is more realistic but can be extended only to training, breed both advantages side by side. The main limitation of the present study is intent, the mimicking of pedestrian natural walking speed, and a single phase investigation . Even if robots perform perfectly at a prescribed region, how often the robot needs to be conservative in interacting with real pedestrians at that region is not addressed. Additionally, the second level subfactorial design will help in experimentation of environment types - (real, virtual simulations). This study will also help to replicate the above findings and interpretations, and the protocol could be investigated in other interactions of AV and Pedestrian, like Tour Guides, and delivery robots, in real and controlled conditions.

The usability study employed a between-subjects design, where the study considered humans, the weakest link in defense . Although we cannot account for human intention, controlled environment studies can provide us with insights about how users choose to

respect or take advantage of vehicle maneuvers, which according to Lewis et al. [15], can provide valuable insights in designing operating mode indicator design or biasing algorithms towards socially optimal autonomous vehicle (AV) operation. To prevent a hit-attributable pedestrian fault, vehicles should be equipped with complex, redundant perception and action systems based on redundant sensors and models, and equipped with design choices that prevent exploiting predictable pedestrian decisions . Recent trends have also suggested robot design to be more alert at intersections, where much dangerous pedestrian behavior is seen in urban settings.

Apr-2023

7. Conclusion

The human-in-the-loop concept extends to robust and trustworthy autonomous vehicle systems. However, necessary to maintain privacy of data, users must be able to put trust on the system operators who have access to their personal data and are able to use that data to capture intelligence that aims to make decisions about people or their rights, freedom, and interests. The example used of machine learning is well known in the literature of adverriesary examples. It is important that operators can trust the systems being used by authonomous vehicles, and believe that the operators get to decide how the outcomes will be used or operationalised or modified based on their given outcomes. In this sense, it is vital that they trust the intended adversarial ML algorithms and the intended and unintended risk engineered into machine learning privacy component needs to be developed of autonomous vehicle systems so that it fully appreciates the consequences of taking certain actions on people, privacy, and fairness [19].

From the broader perspective of autonomous vehicle technology, it is clear that there is a need for a standardized process where usability is evaluated and appropriately addressed in cybersecurity research, design, and development processes. User trust, stress, and effectiveness should be assessed at all stages, starting from creating and evaluating the quality of the data set, development and deployment of security algorithms, and training and management of autonomous vehicle operators that serves as a human back up [8]. Testing should be dynamic, adapt as per user learning, and be performed in a virtual world under the principle of continuous assessment. In case where organisations cannot provide secure

security controls or training/retention to secure operators, measures should be in place to help protect vulnerable users, and ensure data privacy [14].

8. References

1. [1] V. Švábenský, J. Vykopal, P. Čeleda, K. Tkáčik et al., "Student assessment in cybersecurity training automated by pattern mining and clustering," 2022. ncbi.nlm.nih.gov
2. [2] I. Pekaric, C. Sauerwein, and M. Felderer, "Applying Security Testing Techniques to Automotive Engineering," 2023. [PDF]
3. [3] Q. Song, E. Engström, and P. Runeson, "Concepts in Testing of Autonomous Systems: Academic Literature and Industry Practice," 2021. [PDF]
4. [4] H. W. Alomari, V. Ramasamy, J. D. Kiper, and G. Potvin, "A User Interface (UI) and User eXperience (UX) evaluation framework for cyberlearning environments in computer science and software engineering education," 2020. ncbi.nlm.nih.gov
5. [5] R. Ošlejšek, V. Rusňák, K. Burská, V. Švábenský et al., "Conceptual Model of Visual Analytics for Hands-on Cybersecurity Training," 2020. [PDF]
6. [6] W. Morales Alvarez, N. Smirnov, E. Matthes, and C. Olaverri-Monreal, "Vehicle Automation Field Test: Impact on Driver Behavior and Trust," 2020. [PDF]
7. [7] S. Lee, Y. Cho, and B. C. Min, "Attack-Aware Multi-Sensor Integration Algorithm for Autonomous Vehicle Navigation Systems," 2017. [PDF]
8. [8] P. Xiong, S. Buffett, S. Iqbal, P. Lamontagne et al., "Towards a Robust and Trustworthy Machine Learning System Development: An Engineering Perspective," 2021. [PDF]
9. Tatineni, Sumanth. "Beyond Accuracy: Understanding Model Performance on SQuAD 2.0 Challenges." *International Journal of Advanced Research in Engineering and Technology (IJARET)* 10.1 (2019): 566-581.
10. Venkataramanan, Srinivasan, Ashok Kumar Reddy Sadhu, and Mahammad Shaik. "Fortifying The Edge: A Multi-Pronged Strategy To Thwart Privacy And Security Threats In Network Access Management For Resource-Constrained And Disparate Internet Of Things (IOT) Devices." *Asian Journal of Multidisciplinary Research & Review* 1.1 (2020): 97-125.
11. Vemoori, Vamsi. "Comparative Assessment of Technological Advancements in Autonomous Vehicles, Electric Vehicles, and Hybrid Vehicles vis-à-vis Manual

Vehicles: A Multi-Criteria Analysis Considering Environmental Sustainability, Economic Feasibility, and Regulatory Frameworks." *Journal of Artificial Intelligence Research* 1.1 (2021): 66-98.

12. [12] P. Theodorou, K. Tsiligkos, A. Meliones, and C. Filios, "A Training Smartphone Application for the Simulation of Outdoor Blind Pedestrian Navigation: Usability, UX Evaluation, Sentiment Analysis," 2022. ncbi.nlm.nih.gov
13. [13] K. Dočkalová Burská, V. Rusňák, and R. Ošlejšek, "Data-driven insight into the puzzle-based cybersecurity training," 2021. [PDF]
14. [14] A. Shah, "Adversary ML Resilience in Autonomous Driving Through Human Centered Perception Mechanisms," 2023. [PDF]
15. [15] G. Pappas, J. E. Siegel, J. Rutkowski, and A. Schaaf, "Game and Simulation Design for Studying Pedestrian-Automated Vehicle Interactions," 2021. [PDF]
16. [16] V. Linkov, P. Zámečník, D. Havlíčková, and C. W. Pai, "Human Factors in the Cybersecurity of Autonomous Vehicles: Trends in Current Research," 2019. ncbi.nlm.nih.gov
17. [17] P. McDaniel and F. Koushanfar, "Secure and Trustworthy Computing 2.0 Vision Statement," 2023. [PDF]
18. [18] M. Ebnali, R. Lamb, and R. Fathi, "Familiarization tours for first-time users of highly automated cars: Comparing the effects of virtual environments with different levels of interaction fidelity," 2020. [PDF]
19. [19] S. Nordhoff, "A conceptual framework for automation disengagements," 2024. ncbi.nlm.nih.gov