Cognitive Authentication Mechanisms for User Verification in Autonomous Vehicles

By Dr. Mohamed Azzouzi

Associate Professor of Computer Science, Cadi Ayyad University, Morocco

1. Introduction

In the case of the smart attack, it is shown that for even highly secure DAF designs, drivers can be impersonated through emulation and cloning. Another research gap highlighted is the lack of standard methodologies for testing and evaluating behavior-based defense systems, especially in the context of vehicular architectures. Our paper demonstrates as a pilot work, that the proposed methodology can be synthesic, in the sense of proof-of-concept case studies and validate through static and dynamic security evaluations how the use adversarial simulations can systematically disclose the level of security in such locations. In the future, our research could be verified and prolonged by using this testing framework on the border environment with users having cognitive impairment or/and voice issues.

The report discusses the varied nature of threat models and proposes a formal model for executing attacks and a new approach for evaluating attacks against specific requirement sets. In the conducted studies, two adversarial attack scenarios are depicted: smart and stealth, where the attacker has a notable physical advantage in the smart attack, intelligent investigation of the defense system, and the capability to learn the patterns and secrets in a stealth attack. Created evaluations show that in both scenarios, all the attacks compromising the DAF do not require any prior knowledge of the patterns. In the stealth scenario, it is possible to learn driver patterns with almost no false positive or false negative error, "learning" and "testing," and saving a set of learning up for future attacks only needing few tricks.

1.1. Background and Motivation

In vehicle security it is common to resort to multi-modal systems to ensure that the implemented mechanisms are robust due to the volume of data that needs to be processed for

proper performance. Driver recognition mechanisms have been developed in an attempt to authenticate vehicle users. The main goal is to grant permission to access vehicle resources only to authorized users. The traditional authentication systems implemented in vehicles are scarce and in recent years the security of vehicle systems has been imperative [1]. This premise is based on the fact that the risk associated with vulnerabilities in these systems can represent as important consequences such as personal image rights, unauthorized data access, the ability to steal a car, among others.

As technology continues to evolve, the use of AI systems is becoming of greater social impact [2]. This is evident in the implementation of ADAS systems - Advanced Driver Assistance Systems - in which the vehicle is not only a means of transport, but also an active element in decision-making. Ensuring interface security on autonomous vehicles is critical, as these vehicles imply a higher degree of data exchange with passengers and associated systems than a vehicle with a driver [3]. If the autonomous transportation system presents security breaches, the passengers face greater risks than if they were driving the vehicle themselves.

1.2. Research Objectives and Scope

Moreover, unified modeling language structure diagrams are designed according to defined functional requirements for visual wearables that can be used to measure postural changes and facial recognition accurately. These wearable visual and voice system technologies can be used to measure the reliability and trust levels of the interaction between the driver and autonomous vehicle. A visual wearable paradigm is a model suggested in an investigation of newly developed Microsoft HoloLens virtual and mixed reality systems. In future studies, an embodiment that can mimic the principles made in social detection is expected to be developed. The mind perception model is based on two dimentional constructs of Agency and Experience. The most critical deficiency of this mind perception model is that the postures and facial mimics that matter most are not detailed concretely.

Initial studies have shown that to measure the cognitive capability of the person at different levels, different continuous authentication mechanisms must be applied in the autonomous vehicles [4]. These mechanisms aim to eliminate the disadvantage of authenticating principle of the knowledge base. In this context, the research objectives are defined as follows: To develop a framework for providing cognitive authentication in autonomous vehicles. To improve the authentication objectives with the feedback received from the human-machine

interaction. To develop a deep learning algorithm that measures the trust level of more innovative and imitative outputs. To provide the natural interaction between the autonomous vehicle and the driver by the eye movement recognition with the help of a developed eye-state detection application over virtual reality [5]. For the automatic e-identity recognition and trust measuring approach, an emotion recognition API technology can be applied to the crowd behavior by employing a Cognitive Authentication mechanism. Specified characteristics of best friends under given scenarios can be stored in the personal details section of the identity card. These characteristics stored with the given algorithm can be compared with the input characteristics and results will be given according to the source behavior of the person. In this respect, in gold standard-based Cognitive Authentication, fingerprint, face recognition solutions are examples to measure the information on knowledge base. By looking at both method and time, identification processes are a bit unnatural way to measure a person's trust level [6]. This research extends the findings of Peddisetty and Reddy (2024), applying their mixed-methods approach to examine AI-driven change management strategies in IS projects.

2. Fundamentals of Cognitive Authentication

By using Soar as the cognitive architecture, AIP is designed to check users who will use autonomous vehicle services and be in the system for the first time in terms of their emotional states as they are and their reactions to potential traffic accidents. When authentication is required in the system for the first time, the user is evaluated in terms of his reactions to the virtual accidents shown in the system and his affective state while driving [5]. This evaluation is made with the help of the knowledge and deep learning network developed based on the experience of millions of drivers. When the evaluation process is successful, the user will be able to use system services unless a new problem is encountered. The traditional password-based method is ineffective for autonomous vehicles because they must be based on honesty in the face of external hardware. If this hardware is subject to attack, the vehicle's control can be easily taken over. The detail of the proposed method has been explained in the proceeding section, named as The Proposed Cognitive Authentication Mechanisms.

Due to the human intuition when we cannot have the same knowledge as before, we use contextual knowledge [7]. For example, when we drive on a busy street, our contextual knowledge is different from driving on an open street. If we use the road mode of driving on

the busy street while we are driving on the open street, maybe it can cause an accident. In autonomous vehicles, there are artificial intelligence methods that can be used to make sense of the environment in an effective manner and making user authentications with the help of these features is an effective method [8]. Cognitive architectures can be defined as autonomous and interactive architectures with their environment, which reasons with real-time world changes and lets the behavior change based on the knowledge acquisition. In this study, one of these architectures, namely the Soar architecture, is chosen to be used in the designed AIP (Authentication in Autonomous Vehicle) technique. The Soar architecture developed by John Laird in 1987 is a cognitive architecture that can be used for multiple purposes.

2.1. Cognitive Biometrics

The scope of the Blocksec-ADA framework is to include trusted Smart Contract and Log Data structures to increase the transparency and effectiveness of Cross-chain participation with the ledger in the Blocksec-ADA framework. ESA holds trustworthy device fingerprint logs that meet the P2P, D2D, and assurance requirements and cannot be distorted by other intruders or devices. KISKE owns a unique key performance indicator (KPI) and manages ETF exchanges to prevent the attack of evil users. The authenticity and integrity of the transaction are between the devices in Blocksec-ADA with relaying the ESF Key to create a smart contract [9]. The block name is a Human Avatar Identity Passport (HAIP). The mapping of permissible permissions has the ESF key that has a semi-occupied fingerprint.

The illustration of the impacts and adaptability of theft prevention is identified with driver verification which can be potential if keyless worldwide systems are broken or vehicle or system gets penetrated with connected components [1]. In particular, the estimation of the differences observed in the driving patterns done directly in the car by the Master Module is not encrypted. In addition, the information will be accessible by the SCMs. two additional weaknesses are identified. First, the Master Module stores all the information and does not have any security provisions with regards to the heartbeats. In particular, the Master Module only communicates with the SCMs at request. Second, the key generator used is a relatively complex encryption algorithm. This leads to a complete method encryption and thus might not be suitable for certain Environments.

2.2. Cognitive Load Theory

It is important to understand and analyze the links of working memory capacity to CTTs to ensure the interaction between autonomous systems is efficient and effective. Cognitive function analysis has been utilized as a method to account for both human and machine memory and processing limitations in order to accurately assess interruptions and workload on a driver [10]. This cognitive model has been tested in a state-of-the-art vehicle flight simulator task for authorization task allocation as well as autonomous system response. It was demonstrated that human driver use of the eyes-off-the-road time (EORT) model was best for predicting system usage timing in a partially automated environment. The simulation concluded that for improving system usage timing to EORT model predictions rather than internal awareness the best target for simulation improvement was improving system awareness.

[11] Cognitive load theory (CLT) is used in the design of cognitive tasks (CTTs) to accommodate the current capacity of working memory and promote user efficiency. CTTs should be designed so that they do not exceed a user's cognitive capabilities while carrying out a task, as doing so can distort task results [12]. All interactive CTTs cannot be separated from working memory capacity. For example, the performance of a user can be affected when using an autonomous system due to the interaction with other system capabilities and the limitations of the human information processing capability to carry out a task.

3. Autonomous Vehicles and User Verification

Vehicles authenticate themselves for secure communication through embedded certificates, which try to ensure that only trusted users are able to manipulate the system. While these certificates allow system authentication, the driver can also log in to her vehicle, so that customization for different users and services can be integrated. However, the proposed methods often lack proper procedures for data integrity and authentications which may end up with malicious attacks. The purpose of maintaining security and integrity is likely to avoid repudiation and system fraudulence. It is not desirable to allow user manipulation and provisioning of false data. It also causes inaccurate data analysis. [13] proposes a few but elaborate scenarios, which are mainly suitable for large-scale operations. In the presented approach, for data authenticity, all the data frames are covered with HMAC hashing algorithms. Consequently, any malicious or corrupted data that arrives at the portal is

discarded and flagged as invalid. By this rigorous verification methodology, the collected data should be reliable and trustworthy for making business intelligence decisions.

User verification takes to the driving scene for Autonomous-Vehicle, is it possible to make sure that who leads the steering wheel? Conventional verification methods must be replaced with non-intrusive methods to avoid any physical based authentication method in order to increase the accessibility and minimize the driver distraction. A non-intrusive method has been presented in [3] to authenticate the driver in behavior-based manner in autonomous vehicle. The prototyped systems based on face authentication or voice authentication. Before starting the journey, the driver needs to communicate with our mobile application to register their face or voice samples. While driving, the face status and voice level need to be correctly captured to consider the presented face or feedback as valid signals. Insecurity is still noticed. In the presented approach, `playback attack` concept is also discussed, as an evil attacker might use a recorded voice for fraudulence. Some deep exploring model GAN-CAN may improve this discussed work for future work. Despite the presented convoluted approach, it has yet a lot of challenges and requires a lot of considerations.

3.1. Challenges in User Verification for Autonomous Vehicles

Movement and navigation in autonomous systems can be unreliable if the environment changes and the internal models are not updated. These systems pose challenges for formal and informal verification methods due to the integration of hardware and software components from various sub-domains [14]. Electrical, software, and robotics engineers build the vehicle based on dynamic and nonlinear systems theory and adaptation methods such as joint and fault-tolerant integrated, intelligent, proactive control, planning and scheduling of behaviors, behavior-based learning, learning by demonstration, skill learning theory, emotional learning, and reasoning by model-based policies and by using, open, and closed cyc petites, stochastic dynamic programs, and neural feedback link methods. In vehicle dynamics, using these techniques takes a great deal of importance in choosing the right range of driving behavior at the right time. This situation also creates problems related to the availability of verification and assurance control methods and techniques required for this control theory [15].

Users understand automated vehicles as self-driving cars, whose technology helps solve traffic accidents, congestion problems, and gas emissions. Large OEMs and key startups are

working intensively in developing these technologies, and the transportation and mobility industry can be expected to change radically in the next few decades. However, the process of autonomizing vehicles necessarily brings forth important issues. Firstly, it is clear that these vehicles still cannot substitute for human intelligence in some critical contexts. Hence, they require user verification mechanisms and prototyping. Research and development problems of vehicular cybersecurity began by imposing secure ontogenesis mechanisms on automobile systems to protect against cryptographic attacks. The creation of secure operation mechanisms that detect more primitive threat activities in real time becomes important under normal user verification mechanisms.

4. State-of-the-Art Authentication Mechanisms

The current mechanisms aim to allow access to the vehicle's intelligent system after authenticating the user based on different experience-related features. Such mechanisms exist for other context-aware systems, e.g., smartphones [1]. However, the vehicle as an IoT-based system has key features different from such systems, hence the dissimilarity in the properties of existing user authentication mechanisms. To our knowledge, no review exists for user authentication in vehicles. Apart from the comparison in Table 1, there exist some limitations of authentication algorithms strongly prove vehicle authentication research in recent times. These limitations are posed in the following questions. The survey conducted in this work actually has the solution to this question in the advanced technology area. That is, identifying which properties of vehicular networks— either presented in Table 1 or not—make them vulnerable to a successful attack is quite essential for developing more reliable and real-world technologies and eliminating existing features which compromise security [16]. Meanwhile, the rise of automotive technologies advances in wireless vehicular communication, Cloud computing service, Internet of things (IoT), Edge computing, etc, has profoundly redefined the activities of users on vehicles, as users' privacy content and data, including authentication features based on behavior biometrics, are at risk once the vehicular networks are intruded by adversaries [3].

4.1. Biometric Authentication Systems

This system has become a center of attention to implement different types of applications including verification of user existence in network, comments authorization, restricting anonymous usage in discussion boards, remote data access, theft detection in mobile devices,

social network privacy, content protection, and data sharing systems in clouds. Authors present the schemes that mainly focus on the storage privacy. In multi cloud data storage systems, the message authentication code (MAC) is utilized to obtain the data stored inside the cloud network. Restricting random data access to a dedicated subset that could be consumed using the second level of token requests was a primary concern. A unified agent-based architecture, User profiling, effective human interaction and attacker prevention were implementing fingerprint technology. This represents the biometric method in a big data mapping for vehicle theft. The goal of this research proposal is to encourage and emphasize safe vehicles to reduce the rate of insecurity on the paths. In this direction, a digital bribery system is proposed to verify documents and their understanding, where participant data can be signed with digital contracts and the driver could be profiled for detecting cloning vehicles.

[17] [18] Humans in many security systems prefer a method of biometric authentication. They utilize something that a person represents as his most secure approach. Physical identifiers (used in biometric authentication) include face, finger print, iris, signature and voice recognition in one's behavior. Majmaa, Bacivarov and Ahonen show that face recognition has various forms. Sameer and Sangeeta states that biometric have some limitations including computational complexity, variability, imposter, attack-free operations and non-acceptable error rates. Raspbian under proposed system is the authentication of the user based on biometrics. Therefore, biometric features of user face are captured and used for security proposes in under the proposed system. There in no any need form user to remember and carry card or key. The biometric authentication of a user based on their face presented by Ojala, Pietikäinen and Mäenpää. They analyze the unique features of human face and recommended a well-developed approach to analyse the significant of facial feature presented. The research compares human faces images primarily time into a set of main horizontal and vertical features. Famous methods of biometric authentication include Finger Print System, Eye Retina successful in identifying correct user. [1]

4.2. Behavioral Biometrics

In the face of these needs, our perspectives started, in the first place, to offer a compact presentation of some of the earliest authentication ecosystems for telemedicine scenarios. We synoptically mentioned some well-known algorithms including various hardening and protection protocols, emphasizing potential links between the acceptability and usability of

the verification modalities and the type of available security exploits. A review was also made from a sample of significant attempts to intervene, mitigate, and better safeguard the current ways off dealing with stochastic, electronic threats. The characteristic features and parameters that define currently trending security challenges and other learning-driven prediction efforts were aligned with compromised encrypted communication between various IoTdeviceattached health backgrounds, and password-stealing threats through the exploitation of biometric substrates for the identification functions.

The novelty proposed in this study consisted in defining scenarios and factors, as well as guidelines for secure biometrics-based healthcare applications with behavioural and authentication data such as hand movement data (http://www.20bn.com/), and 100 Hz ECG and EEG band data (https://www.biosemi.com/research.htm), for the password input are also shown. These studies do, however neglect to consider the adoptability of the proposed biometrics under workload. Clearly, designing the biometric modality with the workload faced by the HCPs in the health industry in mind is crucial to meet the challenges in verifying HCPs working with different levels of difficulty. Alternatively, not only Identifying a five-class workload level based on background color and implementing a GAN model for generating EEG-based workload in reference, the authors suggested facilitating hands-free bimodalparadigms in order to, for example, better include differentlyabled people, reduce pandemic-prompted SARS-CoV-2 transmissible risks and achieve other measures for infection prevention and control.

[19], [20] ByteKast [21] proposed an integration of both positional and behavioral biometrics to ensure enough complexity without causing extra fatigue or impairing user experience. These authors indicated the need for new verification paradigms in the automotive context as the proposed steering wheel-based biometrics did not achieve the established baseline in terms of user satisfaction, performance and security. Hence, RubikAuth was again proposed, this time using autonomous driving scene clues such as lane markers and reflectors on the road to drive the biometric input needed for the authentication procedure. To that end, associations applied physical indicators simulated through Oculus Rift glasses to alternate stimuli that should subsequently prompt different driving behaviors. Since glasses are detected through sensors with an observed jitter, that data was exploited to retrieve information about the angular deviation between the head motion and lane markers, the use of blinking as an indication for biometric input was proposed fulfilling the goal of integrating

it into an existing verification system, the wide adoption of which in healthcare scenarios by novices and experts has been shown.

5. Cognitive Authentication Approaches

Multiple semi-autonomous vehicles are operated using health status [10], cognitive workload or behavior signals are always important. And for behavior in FIFA operations, it requires human influence input for some signal verification system in real time. Fifteen different physiological signals such as ECG, PPG, EEG, etc. have been assessed to their response time in terms of real time. Signal processing of each signal is difficult, which is the main hurdle in using specific signals for real time user authentication process of supervision driver in semi-autonomous vehicle. Consequently, we can select eye gaze signal due to good signal response and less complexity of signal processing. Therefore, for real time user verification system, eye movement based signal is a better option.

Keystroke dynamics [22] and eye gaze patterns [23] are suitable options for user verification in an autonomous vehicle where the users cannot help themselves. A user of the system would need to enter their user id and password for the first time so the system can generate an interest profile which can be used to authenticate the user continuously. The keystrokes inserted can be static or dynamic and both can be used for the continuous authentication process. Static samples are the geometric properties of the appearance of the typed characters (absolute keying times, dwell times, digraphs frequency) whereas dynamic samples are those based on procedural timing like pressing and releasing of keystroke keys. A user authentication model is built through continuous authentication by keystrokes. Once the user continuously invalidated in the system, the authentication process is followed then a new user profile will be created.

5.1. Memory-Based Authentication

Our proposed solution uses a memory-based authentication principle for secure and efficient user verification in an autonomous vehicle environment. An adversarial experience may occur in cases involving secret-based user password techniques, which possess a high susceptibility for guessing and dictionary attacks. To eliminate or diminish the problems faced in the secret password, we investigated and proposed an anonymous mutual authentication scheme. This mechanism applies to both vehicles joining the system for the first time, and for

repeated authentication in the case of the vehicle leaving the system and then rejoining at a later stage. The scheme thus explores the privacy of the vehicles and supports mutual verification and duty verification. Furthermore, the designed scheme contains relevant cryptographic operations (KeyGen, KG, Exce, Dec, and Sign) in order to provide an effective privacy and trustiness environment for autonomous vehicles.

Further classification offers the features of the work performed in-terms of mutual authentication, conditional privacy, or privacy. Currently, there are no methods that implement mutual authentication, conditional privacy, batch group signature, and privacy protection. We find that the anonymous mutual authentication schemes are prevalent in a vehicular environment to explore anonymity and mutual authentication. The present technologically advanced era strongly necessitates the implementation of secure and efficient autonomous vehicles. An autonomous vehicle environment intrinsically and essentially requires secure and efficient vehicles because of their mass utilization in diverse safety-related, smart city environment applications; such applications are highly sensitive, technologically advanced, and strongly require high-level security and privacy measures [5].

Memory-based authentication mechanisms for autonomous vehicles can be classified into three major categories: identity-based cryptography, public key infrastructures (PKIs), and blockchain-based mechanisms [24]. Identity-based cryptographic methods generally employ a T(Trusted Authority), which generates and shares a secret key with the Vehicle Identity Unit (VIU). PKI-based approaches use CAs (Certification Authorities) to sign certificates when registering vehicles; the signatures are then used for vehicle comparing.

5.2. Attention-Based Authentication

Once the user reaches the car it is authenticated on the basis of secure handshake and other cryptographic techniques. User authentication techniques based on passwords, keyfob, face recognition, gesture, or biometric systems have been proposed in the literature. However, several studies demonstrate the limitations of such techniques and how they can be fooled by different studies influence on kinematic patterns likeness while imitating. This makes them vulnerable against impersonation attackers suggesting these techniques to be used with some back-up mechanisms. For example, the pattern lock for devices was recently shown to be vulnerable against the smears on the screen fingerprints attack. Also, the keystrokes of the password technique can be intercepted and replayed for the impersonation attack in another

study. The in-vehicle authentication techniques based on the brain signals and Cognitive Authentications based on virtual run and record tasks, EEG, and fNIR have physiological and psychological markers Therefore, their registration in human biometric traits faces challenges of the user's mental state such as critical attention, fatigue, stress, workload, and so forth. The requirement for the presence of cognitive and mental effort of the user for such biometric techniques became a research focus to determine the user's presence and absence scenarios. Also, a continuous authentication approach has been adopted to monitor user presence and absence by monitoring its physiological and behavioral patterns [25].

During normal driving conditions, the system continuously accesses low-level sensor information and high-level cognitive mechanisms. With the increasing of Automated Vehicles (AVs), malicious attacks such as mimics, such as dreaming, data poisoning and sensor attacks can cause disturbances in the system as pointed out in [7]. Therefore, it is essential to ensure that the current user is present and alert at all times in case of any attack or unauthorized access to the vehicle This will make sure that AVs are secure both from data tempering and from unauthorized access to the vehicle. Moreover, it will ensure that only authorized users use the invehicle system ensuring the safety of all other users/users on the road. Hence, there arises a need to continuously verify and authenticate the user inside the vehicle as suggested in [26]. To this end, this section presents an attention-based cognitive game which continuously monitors the user inside the AV. The game monitors the user's involvement in the task by sensing the user's attention on the game. The control of the game during this cognitive challenge is continuously sensed and processed to authenticate the user using different cognitive mechanisms. The result of the keypresses are utilized to answer random set of simple arithmetic questions. This makes the verification mechanism secure as well as very challenging for the imitators if the game is not known to the imitators.

6. Evaluation Metrics and Methodologies

Future potential evaluations should also consider user experience testing to understand if interactive cues, designed as perceived as natural and acceptable, are not intrusive and able to reduce driver's attention overload with respect to the status quo. In consideration of the limited third-party usability evaluations, a section of the anticipated evaluations also has to consider a comprehensive user experience (ref: 1a0b6f49-c0db-4e56-af0c-2cf9beef51e1). Such evaluations should be administered allowing for open-ended responses as well to pick up on

any emerging use cases or common in-home analytics. Long-term evaluations should be conducted to observe enduring effects on the PSAD. This will allow us to better generalize how these systems might help individuals who have repeated short-term issues with episodic memory and executive dysfunction feel less impeded or supported in their day-to-day life. Determining the best paths through the vast and varied space of usability principles and human capabilities in CogTruAV will allow us to better differentiate where safety can be more effectively managed in future TLAVs.

Regarding evaluating cognitive authentication mechanisms for user verification in autonomous vehicles, there are several potential methodologies to use for evaluation. As highlighted in the motivation for this research, the current standard for autonomous vehicle driver identity verification tends to be behavior-based and myopic at best. While historical and observational driving data may be useful in training AI to manage automated control state arrangements of the vehicle for drivers that are not typically seated in the "driver's seat" [3], this is not enough for fully autonomous vehicles, which require user interaction monitoring together with cognitive authentication metrics. User evaluation metrics can be derived from experimental validations that investigate the use of internal (coupling the driver to the machine) and external (coupling the driver to the environment) signals of human–machine interaction such as communication, trust and workload. A robotic system can be considered as a counterpart of autonomous driving: it is subject to specific constraints (i.e., working safely in partially constrained environments like car interiors) and has an impact on the person interacting with it. In car contexts, monitoring the driver's state using machine reasoning and decision-making to tailor the autonomous driving features to travel desires or remains always critical [27].

6. Evaluation Metrics and Methodologies

Cognitive Authentication Mechanisms for User Verification in Autonomous Vehicles

6.1. Usability Metrics

The usability and user perception of the proposed drive safe platform are addressed to evaluate the performance of the proposed Cognitive Behavioural Mining method [28]. The empirical evaluation of the proposed solution is carried out in three steps. First, we perform a usability test to investigate the interfaces of the drive safe platform based on raw scores.

Second, we statistically analyze the effectiveness of Cognitive Behavioural Mining based authenticator (pass/ fail decision for driver identification) on user perception using a tranquillity test. Third, we conduct a comprehensive confidence interval analysis of all the latent signals portrayed in Cognitive Behavioural Mining for testing user perception. First, usability test results gathered through statistical analysis indicates that the user interfaces of the drive safe platform are reliable, consistent and show high statistical significance (p-value = 0.0041).

This paper is centered on the survey conducted to gather the most significant and utilized metrics in each of the three authentication domains (biological, physical and cognitive) in the transportation industry, with specific emphasis on autonomous vehicles' security, privacy and usability requirements. Usability metrics used to evaluate cognitive authentication techniques have gained momentum in recent years. According to a survey of the cognitive domain, the performance factor is one of the top three metrics considered, highlighting the importance of evaluating the recognition of cognitively assessed data by the user, i.e. the training time and evaluation of accuracy and user error rate. In this paper [23], in providing the typical comparison of the usability metrics adopted in cognitive behavioral authentication techniques for overview above, it is significant that the operation time (latency) demonstrates high relevancy in all of the papers. It is important that the average false acceptance rate being another metric highly considered in the cognitive behavioral domain.

6.2. Security Metrics

Security event means an event in which a security goal is violated. The concretisation of security events then provides the basis for the definition of security matrix and then risk assessment. We consider three categories of fundamental security events or threats in this work: a) one threat related to personalized data and the violation of an avater's data privacy, b) three threats related to the security and integrity of data transmitted between the platooning communication partners, and c) an integrity attack on the real time GPS data relating to the localization of each subscriber [1]. For each of these fundamental security events in the level 2 and 3 of the hierarchy, going successively from project to item, and then to the security goal layer. Therefore, the following sections present the concretisation of the security goals in the project and item layers.

that are acquisition process security, communication security, layer-2 security, and second security [29]. Security can be focused on, on specific security features, which are V2X application identity verification, V2X application data integrity, and so forth. Finally, decision phase for all security components in ADAS and contextualizes in vehicular operating system are presented. All these security hyperparameters and security features are acceptable for autonomous vehicles overall cybersecurity.

Vehicle cybersecurity has become a major concern of the automotive industry in recent years. Security aims to preserve certain defined objectives and ensure that unauthorized operators are not able to access any system or services. In the context of performing risk assessment based on vehicle-to-everything (V2X) application security, it is important to consider a variety of security properties as well as reviewing a wide range of possible attack vectors [30]. For instance, it is essential to analyze strengths and weaknesses and determine the appropriate security measures and acceptability levels for different types of V2X data. There are four different security hyperparameters

7. Case Studies and Applications

In [31], it is known that capability limits the quality of a world model for autonomous driving. However, the most discussed issues are real-time computation, sensitivity to parameter changes, and interactions with the environment, with respect to model-training and learning processes. In this article, privacy protection and security concerns have briefly been discussed. Cuingnet et al. presented an approach of adversarial perturbation augmenting feature movement neural networks to improve the robustness of deep neural network-based models for autonomous driving; however, a potential attack was mentioned. Given this context, world models are evolving from knowledge about the physics of the vehicle to self-developing and maintaining intelligent decision-making and prediction modules.

Blockchain might be one possibility of providing user authentication, trust monitoring, and data management on the IoT scale [32]. A Blockchain-based security solution is proposed for the IoV in. The authors incorporated the concept of User-Authentication and Data-Integrity (UADI) into the IoV system using the Ethereum blockchain. To achieve secure vehicle-to-vehicle communication, trust management and data management were also involved in establishing a generic Blockchain-based vehicle database (BVD) in this work. Another study [1] introduced a biometric-based system for vehicles where the long-term driving style is used

as authentication information for vehicles. Park et al. developed an in-vehicle biometric identification method: driving habit analysis based on five different driving patterns.

7.1. Real-World Implementations

In, authors argue the challenges of securing authentication. They centered on ease of use and deployment in this paper and proposed, implemented, and evaluated User-Centric Authentication (UCA) using real hardware and exhibitions of autonomous street driving on the basis of Camera-based Attention in PoliCAr (CAPC). They showed, CAPC can be used in SAE level 2+ roads by performing street piloting tests. Even for SAE level 2+ until full autonomous functions, Performing CAPC below SAE level 2+ would not be technically difficult. The main benefits are there will be no dangerous period in which the user needs to perform dangerous challenging control actions, and CAPC provides significant improvement in terms of safety. [6]

We briefly discussed some of the prominent means and methodologies for Cognitive Authentication mechanisms which are deployed in the realm of Autonomous Vehicles. Now, we will aim to encapsulate some of the actual real-world implementation of some of these methodologies. AutoAuth ensures secure and convenient user authentication with context and behavioral. Single-Node User Authentication leverages users' mobile devices and in-vehicle sensors for continuous authentication. We also briefly describe some of the real-world applications of the implemented model in section 2.8. [33]

8. Future Directions and Emerging Trends

Synthesis of the lessons learned from the above articles to infer the leap conceptual directions and expected knowledge gaps to be addressed in the upcoming years. The technological advancements in connection to the design of a secure V2X communication system in CAVs can be organized under rival deep learning architectures (i.e., CNN, RNN, R-CNN, GAN, LSTM, Transformer and language models such as BERT and GPT), individual attributes classification schemes and feature extraction methodologies, image/video enhancements to mitigate adversarial attacks, SLAM-like architectures for anomaly detection, and ongoing research works on secure V2X inspired multi-agent reinforcement learning models focusing on its specific applications to CAV domain. A detailed exploration of next-generation visual sensors, novel supervised/unsupervised/semi-supervised robust learning methodologies,

specific domain adversarial domain data augmentation techniques, and secured communication models shall be embraced for achieving superlative authentication performance and resilience against adversarial type input patterns to be witnessed with large-scale CAV deployment [6].

For the implementation of research needs requiring CAV's driving on public roads is anticipated. Formations of user authentication mechanisms in the foreseeable future require advances in the following critical areas: i) advanced V2V systems for the provision of real-time data distribution, ii) development of signature methodologies for CAV-specific sensory data along with efficient data-gathering strategies, iii) learning algorithms resilient to adversarial perturbations in sensor data, especially V2X waterhole attack, and iv) systematic investigations into the design and applicability of feature-extractor learning models for distinct classes of authentication tokens supporting multi-modal data streams [34].

8.1. Advancements in Cognitive Biometrics

The human verification paradigm, i.e., the necessity to arrive at a previously set threshold (confirmation) for being granted access to a system, can be bypassed, the so-called negative paradigm, or present in the form of an inequity, resulting in a confirmation (see "How positive and negative affect influence driving safety: A mediation analysis for self-determination-moderated model", Traf0c and all, 2021) or comparison (see "SirNotifications: Innovative cyber-physical anti social engineering protection", Traf0c and all, 2020) necessity. In psychology, this model has been trained with results showing a cognition-related load reduction, as the positive paradigm demands additional cognitive effort. The fact that cognitive overload generally leads to performance decline, together with involved findings like a 7-9% information transfer decline in concurrent learning tasks per cognitive load level, emphasize the negativity experienced by the increased cognitive load. Long Bit Coin puzzle-based cognitive task experiments gave additional evidence. Social psychological and biological studies showed in addition the impact of biometrics on people's psychology .

Biometrics can play a crucial role in verifying users' identities in autonomous vehicles. Biometric systems can assist in determining who has control over the vehicle and could potentially serve as a first step in a multi-step user verification mechanism. The emerging rise of so-called "cognitive" biometrics adds support to this claim. Though standard biometric systems mainly rely on physiological or behavioral attributes, cognitive biometrics employ

typical brain activities as biometrics. Because of their dynamic, hard to imitate, and continuous nature, cognitive biometrics in itself but also multimodal biometrics integrating cognitive- and non-cognitive biometrical measurements (e.g., vein structure and keystroke dynamics) are receiving academic and industrial attention. Some advantages are their characteristic liveness (with the exception of parts of today's commercially successful authentication modalities like fingerprint, face, or vein recognition), universal availability, and the failure-resistant non-intrusive and continuous nature, potentially suiting user verification in real-world environments like the automotive context. Other favorable characteristics include their non-exploitable and un-obtrusive nature, making them particularly suitable in security critical applications. Furthermore, they are potential candidates in user specific adaptation beyond personalization of driving settings from a seat occupant's identification.

9. Conclusion and Recommendations

This survey also highlights the need for significant research at the intersection of automotive security and human factors to design more trustworthy on-vehicle confirmation techniques. Authors outline various factors, benefits, and challenges of a possible blockchain-based architecture for different aspects of a connected vehicle scenario. AV applications present a unique context with concerns that are often different or can be greatly increased when compared with the already studied V2X cases. Overall, this survey provides novel motivations, discussion points, and challenges for user and driver authentication in autonomous vehicles. Finally, the article discusses possible connections to the vehicular mobility and the in-vehicle behavioral models used within AVs [24].

With the ever-increasing number of autonomous vehicles (AVs) expected on roadways in the near future, on-vehicle security and user authentication have become highly important areas of research. Most work in this area is focused on the behavior-based driver identification and validation of the driver's identity . Apart from these two areas, there are no comprehensive security and user verification protocols to validate the users' accurate identity and protect the AVs from unauthorized access. Authors have studied the vulnerabilities of the existing behavior-based driver identification models and the possibility of overpowering them using few-shot attacks such as GAN-CAN or a student-teacher attack. Although this is a step in the

right direction, it's still another behavior-based model, that can still suffer from the same drawbacks {ref: 4047aec6-30cd-423c-8716-554a975e4d53] [4].

9.1. Summary of Key Findings

Uninvited incursions within an autonomous mobility ecosystem can have multifold repercussions, including sabotage, human injury, property loss, etc. Open forums, including scientific platforms and industry consortiums, are relentlessly investigating the robustness and resilience of autonomous surfaces, with two distinct lineaments; 1) testing and validating DS/ML models, vehicle systems, IoTs analytics, variate non-adversarial and adversarial conditions and scenario designs tested and evaluated with the targeted autonomous fleets and systems, 2) providing an effective countermeasure to adversarial machine learning by proposing novel DS/ML-backed resilience and robustness building strategies and mainstreaming the efforts. To the best of the authors' knowledge, with SG-tracking and SG-LSTA alignment paradigms, no such data set currently exists. The rationale behind forming a comprehensive adversarial and resilient AV benchmark security data modelings are proposed with six tactical attack vectors within AV datasets, covering basic to advanced attacks, with black-hat adversarial objectives and resultant impairments across multiple operational contexts. [35]

Several datasets have experienced certain degrees of cyberincursions, illegal and malicious activities across multiple operational and security domains, with explicit AGI and DS/ML alignments and endowments. The apparent efficacy of The dataset first large-scale adversarial machine learning, security, and privacy-oriented benchmark classification within autonomous vehicles (AVs). Driven by distinct attack vectors and 1, Nãoégauss statistical expression targeted security, robotics, and control sub-disciplines, the proposed dataset aimed to provide comprehensive, systematic, holistic, and contemporary benchmarks that bridge conventional security frameworks into the recently evolving adversarial machine-learning and data science-based resilient and robust autonomous missions and deployments. In principle, the proposed dataset is designed to feature comprehensive collection of deliberate AGI- and DS/ML compromises, desecrations, distortions, intrusions, and manipulation, within the AV operational context, targeted towards black-hat harm and white-hat resilience and robust-challenge benchmarks, through variant adversarial domain-aware and targeted spaces (different operational domains, sensor types, and staggering operational

and scenario-based complexities) defined through a set of security objectives emanating from fundamental to advanced attacks. [36]

The automotive industry and automobile systems are transforming into digitized and interconnected digital networks – i.e., Internet of Vehicles (IoV). IoT technologies have been proposed to provide efficient and reconfigurable operational designs in this domain. Conspicuous efforts are being enabled to contend towards achieving operational autonomy, through establishing autonomous operations that can ensure operational convenience towards maintaining a multi-dimensional automated driving environment paradigm. Over the years, various research endeavours have explored dedicated autonomous vehicles' (AVs) design, deployment, and development mission domains to enhance the overall system response performance, safety, security, reliability, and usability. In the past decade, technocrats worldwide have been inching forward towards achieving automated and intelligent vehicle operations roadmaps, by providing architectural primitives, enabling autonomous vehicles' operational convenience, and stability – i.e., towards designing, modelling, and validating vehicle networking and computational architectures. [37]

9.2. Recommendations for Future Research

The implementation of predictive cognitive hedging efficacy of human–machine interactions can even transpire with the possible alternative self-administrative baffling consequences. Autonomous vehicles are considered to be the most operatively contemporary infrastructure-oriented application among others[}, yet still, they constitute ambiguity regarding inclusive detection of all potential active adversaries. Therefore, still there exists a need for further progressing research while incorporating broad study thematic in driving based social intelligence using active and novel testbeds, human-in-the-loop validation to cover potential implicit bias issues, comprehensive formulating of the security validation analysis including digital and system-level attacks, and their real-world testing on algorithms, and also their associate explainable artificial intelligence techniques, which can reveal legitimate introspections of decision-making scenario in an unbiased, fair, reasonable manner in order to integrate in real time the extra perception to cater to diverse and critical scenarios [37].

Vehicular networks are complex systems iteratively involving the connection of vehicles, sensors, infrastructure, and service providers between them. Secure, reliable, and authenticated communication systems are largely essential to cater to infrastructures like

vehicular ad-hoc networks, intelligent transportation systems, and the emerging domain of intelligent and autonomous vehicles. The realization of vehicle authentication faces individual and exclusive industry-specific adversaries, which broadly contribute to the insufficient implementation considering residual shortcomings like safety, security, and privacy. These sectors embed user authentication with different naturally occurring applications for reliable and efficient user identification and management. Various established and potential reinforcement mechanisms will be compared like, PKI (public key infrastructure), digital signature, MEC (multi-access edge computing), ETSI MEC architecture, and on notification-based edge computing [5].

References:

1. Vemoori, Vamsi. "Envisioning a Seamless Multi-Modal Transportation Network: A Framework for Connected Intelligence, Real-Time Data Exchange, and Adaptive Cybersecurity in Autonomous Vehicle Ecosystems." *Australian Journal of Machine Learning Research & Applications* 4.1 (2024): 98-131.
2. Prabhod, Kummaragunta Joel. "AI-Driven Insights from Large Language Models: Implementing Retrieval-Augmented Generation for Enhanced Data Analytics and Decision Support in Business Intelligence Systems." *Journal of Artificial Intelligence Research* 3.2 (2023): 1-58.
3. Sadhu, Ashok Kumar Reddy, et al. "Enhancing Customer Service Automation and User Satisfaction: An Exploration of AI-powered Chatbot Implementation within Customer Relationship Management Systems." *Journal of Computational Intelligence and Robotics* 4.1 (2024): 103-123.
4. Tatineni, Sumanth. "Applying DevOps Practices for Quality and Reliability Improvement in Cloud-Based Systems." *Technix international journal for engineering research (TIJER)*10.11 (2023): 374-380.
5. Perumalsamy, Jegatheeswari, Bhavani Krothapalli, and Chandrashekar Althati. "Machine Learning Algorithms for Customer Segmentation and Personalized Marketing in Life Insurance: A Comprehensive Analysis." *Journal of Artificial Intelligence Research* 2.2 (2022): 83-123.

6. Venkatasubbu, Selvakumar, Subhan Baba Mohammed, and Monish Katari. "AI-Driven Storage Optimization in Embedded Systems: Techniques, Models, and Real-World Applications." *Journal of Science & Technology* 4.2 (2023): 25-64.
7. Devan, Munivel, Bhavani Krothapalli, and Lavanya Shanmugam. "Advanced Machine Learning Algorithms for Real-Time Fraud Detection in Investment Banking: A Comprehensive Framework." *Cybersecurity and Network Defense Research* 3.1 (2023): 57-94.
8. Althati, Chandrashekar, Bhavani Krothapalli, and Bhargav Kumar Konidena. "Machine Learning Solutions for Data Migration to Cloud: Addressing Complexity, Security, and Performance." *Australian Journal of Machine Learning Research & Applications* 1.2 (2021): 38-79.
9. Selvaraj, Amsa, Bhavani Krothapalli, and Lavanya Shanmugam. "AI and Machine Learning Techniques for Automated Test Data Generation in FinTech: Enhancing Accuracy and Efficiency." *Journal of Artificial Intelligence Research and Applications* 4.1 (2024): 329-363.
10. Konidena, Bhargav Kumar, Jesu Narkarunai Arasu Malaiyappan, and Anish Tadimarri. "Ethical Considerations in the Development and Deployment of AI Systems." *European Journal of Technology* 8.2 (2024): 41-53.
11. Devan, Munivel, et al. "AI-driven Solutions for Cloud Compliance Challenges." *AIJMR-Advanced International Journal of Multidisciplinary Research* 2.2 (2024).
12. Katari, Monish, Gowrisankar Krishnamoorthy, and Jawaharbabu Jeyaraman. "Novel Materials and Processes for Miniaturization in Semiconductor Packaging." *Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023* 2.1 (2024): 251-271.
13. Tatineni, Sumanth, and Naga Vikas Chakilam. "Integrating Artificial Intelligence with DevOps for Intelligent Infrastructure Management: Optimizing Resource Allocation and Performance in Cloud-Native Applications." *Journal of Bioinformatics and Artificial Intelligence* 4.1 (2024): 109-142.
14. Katari, Monish, Lavanya Shanmugam, and Jesu Narkarunai Arasu Malaiyappan. "Integration of AI and Machine Learning in Semiconductor Manufacturing for Defect Detection and Yield Improvement." *Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023* 3.1 (2024): 418-431.

15. Prakash, Sanjeev, et al. "Achieving regulatory compliance in cloud computing through ML." *AIJMR-Advanced International Journal of Multidisciplinary Research* 2.2 (2024).
16. Peddisetty, Namratha, and Amith Kumar Reddy. "Leveraging Artificial Intelligence for Predictive Change Management in Information Systems Projects." *Distributed Learning and Broad Applications in Scientific Research* 10 (2024): 88-94.
17. Venkataramanan, Srinivasan, et al. "Leveraging Artificial Intelligence for Enhanced Sales Forecasting Accuracy: A Review of AI-Driven Techniques and Practical Applications in Customer Relationship Management Systems." *Australian Journal of Machine Learning Research & Applications* 4.1 (2024): 267-287.
18. Althati, Chandrashekar, Jesu Narkarunai Arasu Malaiyappan, and Lavanya Shanmugam. "AI-Driven Analytics: Transforming Data Platforms for Real-Time Decision Making." *Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023* 3.1 (2024): 392-402.
19. Makka, A. K. A. "Administering SAP S/4 HANA in Advanced Cloud Services: Ensuring High Performance and Data Security". Cybersecurity and Network Defense Research, vol. 2, no. 1, May 2022, pp. 23-56, https://thesciencebrigade.com/cndr/article/view/285.
20. Venkatasubbu, Selvakumar, and Gowrisankar Krishnamoorthy. "Ethical Considerations in AI Addressing Bias and Fairness in Machine Learning Models." *Journal of Knowledge Learning and Science Technology ISSN: 2959-6386 (online)* 1.1 (2022): 130-138.