Human-Centric Authentication Systems for Secure Access Control in Autonomous Vehicles

By Dr. Min Chen

Professor of Mechanical Engineering, Tsinghua University, China

1. Introduction

In the present work, the experts focus on requirements and challenges to be considered at: a) conceptual design phase, b) up to minor integration results, that have been possibly achieved, and c) potential issues faced with major integration [1]. In this context, the situation of achieving temporal approval for minor integrations, respectively the situation of potentially occurring liabilities on manufacturers' side, not only poses an enormous challenge, but also not only in the context of anti-tampering and manipulability security features. Moreover, during system integration and operation, the recognition unit has to be robust against hazardous system manipulation by attackers.

Crisis management experts at the Fraunhofer Institute for Integrated Circuits IIS in Erlangen have developed a model for secure access control systems in autonomous vehicles [2]. Secure access control systems in autonomous vehicles (AV) are crucial for preventing misuse by unauthorized persons [3]. The combination of technologies incorporated in these vehicles – including camera systems, Sonic, LiDAR and radar sensors as well as wireless communication systems – necessitates the introduction of a robust person recognition system that is capable of distinguishing legitimate drivers, passengers, and other road users, and to amalgamate the drivers' individual cognitive and physical abilities and limitations. Naturally, the recognition process of a secure access control system has to be implemented in a way, which makes it not just robust but especially secure to manipulation, and according to legislation and road safety norms and guidelines.

1.1. Background and Motivation

Despite the risks associated with autonomous vehicle (AV) security, developing secure, human-centric authentication systems featuring pluralistic secure access control systems is

extremely challenging especially when some of the security schemes are not build to adequately support the secure, interoperable and resilient service layers when exposed to adverserial actors. The main challenges can be summarised as follows: (a) the capability to handle partial controls in AVs through distributed shared autonomy as a result of a suspicious or compromised human-inteferface and/or controller human (H-operator), distributed level of responsibility in a platoons of AVs, audit trails, and end-to-end resilience to adversarial actors who exploit mobility vulnerabilities and security deficiencies.

[4]Autonomous Vehicles (AVs) are an emerging application of Internet of Things (IoT), revolutionizing the field of vehicular networking and communications, leading to entirely new challenges in terms of security and privacy. The vehicular network is an active area of research, involving Information and Communications Technologies, Electronics and Electrical Engineering, Automotive and Transportation Systems. The cooperation of vehicles, infrastructure, and other road users along with security and privacy are of paramount importance.[5]Most traditional authentication systems or cryptographic methods are built around the rapid establishment of security and privacy, which is vulnerable to timing attacks, key exposure, sensors and continuous communication necessary between the vehicle, environment, and the remote location in order to function securely and effectively. Authentication plays a significant role in interactive avionics systems such as vehicle to vehicle (V2V), vehicle to infrastructure (V2I), vehicle to device (V2D), vehicle to everything (V2X), and vehicle to network (V2N) interactions.

1.2. Research Objectives

[6] Securing the direct communication happens in the first stage. 'Vehicle-module' interaction is the smallest unit of supervised control that happens in every vehicle. When in the supervised "driving" mode, Continue Driving Authorisation should be used for its handover decision making, while in the supervised "idle" mode, Base Station Communication should ensure the least vehicle security needs including remote software update. The immediate line of privilege between the vehicle and its operator/designee should be with the User Coordinator, which can inform the system about the availability of a designated driver for the vehicle and the need to block remote software updates once both agree to it. Hence, the information line B Vehicle, Designee and System Operator needs to be secure and trustworthy while the "driving/renunciation decision" line C Vehicle, System Operator, User Coordinator

and Designee should be secure but not necessarily trustworthy. 'Vehicle – Designee' and 'Vehicle – User Coordinator' modules should provide local guarantee of being exclusive to DRS and assistant components of respective operators only, but vehicle-module adversarial inputs as well as adversarial output of DRS or the vehicle should be trackable down to the source of starting the leakage. Adversaries bearing adversarial output will most likely be external fall prisoner to ICV Physical Interference module. The relevant submodules of which are Leaking Barriers, Detecting Barriers and seizing Barriers. Not interested in any implementation details and only interested in making a passing mention of a very powerful system level SVM, the document presents a loss function for the detector module and proposes a safety dynamic Leaking Barrier as a case option to enforce the loss function necessitated by its residing Detecting Barrier effectively.[7] The last stage is securing the onboard computation module. Since the model based design comes with its own security precautions, the immediate opposite Land Vehicle internal logic should prevent vehicle malware from exploiting a combination of sensor physics and vehicle defence to derive welcome spilling behavioural knowledge. This maximally secure (software + physics + metering) information layer in the fault defensive system is presented in the last module, powered by the key composed from the Input Check and Vehicle Limit Check output values. In the global solution however, a threat model with three online attack scenarios has categorized sensor poisoning attacker into the ego-vehicle adversary, the remote-vehicle adversary and the blended adversary. While the Baseline system could only detect remote vehicle adversaries, it is seen that performance of the global system lies between the Baseline and the 20SP Hub Fail or distance attacker solutions in the ego vehicle context. It is found that even though DRS is ubiquitous, when combined with other DRS, solutions can suffer a security constraint. This reinforces the theoretical observation, that the diesel solution under attack performs better across all the models in global scenario.

1.3. Scope and Limitations

Humans have weaknesses owing to human qualities that make them a bad choice for a system to enter the credentials like knowledge. Yet, combining these inherent matching identities in our cars with the utilized human characteristics in the car communication with an instant collaboration unit will be extremely beneficial for an autonomous K3.0 ecosystem even though biometric systems are highly dependent on humans and biometric remains constant unlike knowledge. Each and every time when you turn on your autonomous vehicle, your dashboard

camera will be finished one security process. If they see that the last user is in danger of heart attack or is sleeping suddenly and yesterday, in spite of being completely healthy, she is doing unordinary behavior, it might decide that the system will take the full control and will find the healthiest path from AV supplier. The data itself, residing in different sensors positioned in the whole fabric of the modern vehicle, its control units, smart devices may be exploited at different degrees as an individual security device to train a new AV security paradigm where humans should not be responsible with explicitly creating secure environment in an IT-driven car ecosystem [8].

In this book, we only aim to create a trustable autonomous vehicle in order to prohibit an unauthorized user to access the vehicle for its own interests. The most reliable way to handle access control for drivers is to use an authentication process distinguishing the authorized users from the unauthorized ones. Ideally, the authentication process and user's authorization status should not change due to time, location, and health conditions.The techniques used for accessing the autonomous cars should not contradict their basics : Knowledge, possession, and inherent characteristics. A successful access control system should have a right combination of the human-friendly drivers and the precise identification of their rich dynamics. This book aims to enhance the security in our car access control by blending the advantageous features of the conventional IT security with the cognitive and sensory human cyber security researches [9].

2. Fundamentals of Autonomous Vehicles

These advanced driver assistance systems can be considered as the basic building blocks of future L3 and L4 automated vehicles [10]. L3 designated vehicles have highly automated driving functions, which are able to perform all tasks like accelerating, braking, and steering in defined use case scenarios. However, these systems do need drivers to supervise the vehicle at any point of time and to take control within a short time window in case of error. The driver's responsibility is reduced to monitoring the model's environment knowledge as well as the systems' behavior. For that purpose, inside the vehicle, the driver is equipped with various sensors and built-in devices that help to deploy advanced in-cabin monitoring and assist the vehicle in driving autonomously. Boasting most well-established technology, L3 and L4 vehicles are expected to be launched faster compared to fully automated L5 vehicles.

As the primary purpose of all autonomous vehicle projects is the realization of a safer and more efficient automotive traffic, the development of autonomous vehicles is of high relevance [11]. Depending on the generation of such a vehicle, advanced systems have been developed and additional services implemented to protect drivers and passengers from accidents and harm. As a matter of fact, a level of automation is defined that is used to classify the state of autonomous functions of each vehicle. Classifications range from Level 0 to Level 5 [12]. While the driver has full control of the vehicle at Level 0, vehicles classified as Level 5 are fully capable of driving completely autonomously and without human intervention. Most commercially available vehicles do not yet reach the most advanced levels of automation. However, the majority of the models currently available are provided with different advanced driver assistance systems (ADAS) such as adaptive illumination, lane keeping assist, adaptive cruise control, traffic sign recognition, emergency breaking system, and other systems that assist the driver while he drives the car.

2.1. Definition and Types of Autonomous Vehicles

Road traffic is rapidly changing, especially with the developments of autonomous vehicles (AVs), and finding suitable, socially acceptable and safe management of the intermediate stages of HVI between entirely human-driven vehicles (HDVs) and fully autonomous vehicles (AVs) is critically important [13]. Recently, people who have preferred to use traditional HDVs have expressed concern about AVs, with different people frequently having specific reasons to be worried about them [14]. While some of the reasons derive from concerns associated with SVs generally, some of their concern might not be so much about AVs, per se, as about how AVs will respond to and deal with human-controlled vehicles (HVVs) providing mixed traffic that also has traditional human steering and control.

Recent advances in vehicle technology are enabling better, faster and wider range perception of the vehicle's surroundings, from both short- and long-range sensors, and, increasingly, `sensor fusion', leading to massively improved perception for collision detection and avoidance. Vehicle control is also becoming remarkably smooth and responsive, with important rapid and widespread vehicle control improvements across nearly all scenarios, including in bad weather, and, especially, at high speeds of up to 149 km/h. We can therefore look forward to an exciting future where autonomous vehicles transition to road traffic

networks that are able to integrate their traffic flows much more efficiently with the traffic flows of all other road users [11].

2.2. Key Components and Technologies

Since the IoT enabled devices will allow the transfer of data over a network without human intervention, the security of these devices need to be maintained with high degree of care in the context of smart vehicles. The use of IoT can be extended to passenger safety with recent advancement in technologies for enabling the passenger health in an autonomous vehicle that includes seatbelt status of driver and passengers, temperature and humidity of the vehicle, vital signs and alert notifications of passengers, passenger count in a vehicle, sleep status of the driver, and passenger seats with different colors in the design of autonomous vehicles. Smartphone(IoT-enabled) devices are in fact considered to be as attached-vehicle-devices. The use of structured authentication standard like ISO 83349 (which applies to C-ITS resource subscription and management) set the technical mechanism by which vehicles get federated within an entity such that the data sharing need to enable reliable and secure internet communication among vehicles, entities, and multicast services. [15]

Sensing devices are used for taking real-time measures of drivers' physiological characteristics in the biometric authentication process. [3] The VOCID sensors may be used to monitor breath samples and sense driver's emotional state. In addition to physiological attributes, the Dładacic Computing Accelerator Computing Device (DACCD) via sensors measures characteristics of voice features such as loudness, tempo, pitch, and dynamics to compute statistics like mean, median, mode, standard deviation, and attention ratio of the driver voice recorded. Intra-oral photoplethysmography sensor and high-quality photographs and/or video images may be used for checking biometric, behavioral or morphological factors such as color and pattern of tongue, lip profile, teeth gap, and etc.

Key components and technologies employed to achieve the required goal of this research are as follows: (i) measurement of physiological or behavioral characteristics, (ii) IoT-enabled devices, (iii) connected vehicle environments, and (iv) blockchain technology.

3. Authentication Systems in Autonomous Vehicles

Autonomous vehicles (AVs) forecast a significant shift in the transportation instincts over the past few decades, assuming the responsibility of an advisor in the navigation tasks.

Autonomous car systems rely on motes, onboard units (OBUs), telematics devices (TDs), and a vehicle-to-everything (V2X) communication to address diverse environmental constraints. Security protocols should assist these communication channels, in addition to preventing adversarial attacks. We investigate the access control security, which includes the mitigating of communication security, in the AVs and different dimensions that threaten this security. We need to verify the authenticity of the AV entities [8].

[16]A new regime in the field of automotive transportation, called autonomous vehicles (AVs), is likely to become a milestone in the not-too-distant future. Embedded technology in AVs, such as telematics devices (TDs), and onboard units (OBUs) implicitly offer new security challenges and features. Advisors willing to help boost human comfort and safety still have continuous interaction with each other; thus, they need confidence in transmitting and receiving messages through their security architecture. The communication channels must be resilient against the attacks and exploits of adversaries. Security mechanisms must contribute to verifying the authenticity of AV entities, i.e., access control [7]. However, along with the digital technology capable of mitigating data vulnerabilities, new cyber technologies also expand the range of possible exploits and vulnerabilities. The paper investigates technological requirements for the creation of new vehicular networking paradigms, called autonomous connected vehicles (ACVs), which are seen as 'one of the impending variations' in the transportation paradigm. Security challenges in the AV digital architecture are examined and technological directions for countering them outlined. We consider access control security.

3.1. Traditional Authentication Methods

Proof of physical possession is carried out through mainly two techniques– smart card technique and biometrics technique. Smart card technology uses a small portable card, which consists of a highly secured microprocessor where a user can store a set of credentials. User credentials mainly consist of the required user profile and sometimes biometric parameters such as fingerprint data, iris data, vascular pattern data, or image data. User biometric data is matched against the registered system-provided biometric data [17]. The final step is public key verification testing. This step is maintained in three phases and a ubiquitous biometric system integrated with the RSA algorithm should make the process meaningful, secure, and greatly designed that can be utilized for cryptological provide support for the public key and X.509 certificate standards. In this process, the user's fingerprint data is collected through a

biometric sensing device and then transformed into a feature set. With these secure features, the user biometric data is matched with registered system-supplied template data, and if the user template is not readily available in the acquired system v̇ threshold value, then the user's data will go ahead for further steps. These steps continue until the user data is finally verified. Confidential parameters, as well as security limits for secure data and private key procedures, need to be managed carefully by various such RSA signing and verification processes. The RSA offer zero-knowledge proof protocols that achieve user verification without the required transmission of any confidential user parameters. Algorithms like RSA can be utilized for some effective secure system authentication protocols [8]. These will allow a user-friendly, safe, dependable system of secure, and controlled vehicle protocols.

Traditional identity verification methods primarily rely on credentials and sometimes a password [18]. In the case of vehicles, these simple authentication methods are not enough and could result in misuse of the vehicle and data theft. With conventional one or two factor authentication the vulnerabilities are high and the probability of illegal access is thereby also increased. If someone is using a public Wi-Fi or is in a situation where a person can easily obtain password credentials by looking at the RSA token during an authentication process, mobile theft, etc., it's a very simple task to hack an autonomous vehicle. However, with increasing technology, there are certain security issues that need to be considered seriously. This method has its concerns as various vulnerabilities are associated.

3.2. Challenges in Current Authentication Systems

The European-Union-funded Infrastructure for Trusted Data Ecosystem for Autonomous Vehicles (IDSA) project proposes the secure creation of an information sharing system. The concept includes the car communicating with the internet and its cloud services as well as with its environment on the road using various communication technologies. We present a question and answer dialogue, amongst system designer, developers, legal experts and tax authorities, on how international transaction evaluations can be achieved. Based on this, we derive a list of attributes that must be subject to and object of a requisite and trustworthy process to solve information-asymmetry problems, which plague information sharing of all kinds. To solve the latter problem, we propose the concept of a Digital Corporate Identity, which represents the full extent of trusted information about a company or its products [2].

Automated vehicles today are equipped with remote sw updatable components eg, infotainment systems. Most of the important parts of the vehicle that contribute to safe transportation are connected over automotive networks and are deeply integrated in the vehicle itself. Therefore, special focus has to be put on these components. The ability to trust the correct operation of those components that are responsible for driving is of utmost importance. Breach of the security seal that ensures protection measures would be devastating, from data spy applications to malicious actions that result in fatal accident; creating a genuine trust chain for the correct and safe operation of an autonomous vehicle becomes a prerequisite for market potential [19].

4. Human-Centric Authentication

[20]Securing an autonomous vehicle system poses entirely new challenges that current hardware-centric and cloud-reliant security systems are not equipped to face [21]. In contrast to traditional vehicles, IoT vehicles are potentially able to execute code, which is a drastically increased source of attackable vulnerabilities. In this scenario, attackers becoming physically proximate to their possible targets, it will affect how authentication policies may be enforced. Consequently, it is important to design, build and implement vehicular-implemented authentication systems in a way that is cautious to but not fearful of this new body of security and privacy challenges that may befall it.[22]Automobiles have been indispensable to mankind for more than a century and have evolved into sophisticated machines that provide higher levels of comfort and safety. This vitality has also increased the theft and misuse of vehicles. According to a PTOLEMUS report, 1.1 million cars were reported as stolen in 2019, and only 50% of them were recovered in North America and 85% globally. The car thefts accounted for a loss of more than USD 7 billion to the insurance industry in 2019. In the current era of connected and autonomous vehicles where vehicular security goes beyond traditional physical aspects and into cyber and privacy contexts, the possibility for digital theft has only increased. In this paper, a behavioral-based vehicular authentication and anti-theft system for next-generation vehicles is proposed.

4.1. Definition and Principles

On this basis, we have formulated four principles with which the implementation of control within a human-centric authentication system for autonomous vehicles should be ensured. In the context of digital identity in connected mobility, smart devices such as smartphones come

into play, which are increasingly seen as the pivot of digital interaction between the user and external services. Although the smartphone is increasingly used in vehicle-related services, it is occasionally also used as a factor of authentication system to communicate with the vehicle. In the latter case, manual interaction for the purposes of authentication (e.g., entering a PIN) is often dispensed with in order to enable a "frictionless system" as part of a smooth integration. In the Smart Device as a Factor of Authentication principle, it is assumed that it is this smart device, i.e., the user's smartphone, that is used as the central component of a future human-centric authentication system in the sphere of autonomous vehicles [12].

The notion of human-centric authentication systems is based on the respect for human rights and dignity. This feature recurs in various philosophies, especially in the principle of autonomy in the legal philosophy of Immanuel Kant [23]. The idea behind personal control states: It is the individual who ultimately decides on the use of his data. This becomes particularly clear when digital identity is used actively, for example, as part of data exchange. When it comes, for example, to the exchange of vehicle data between the vehicle user and external partners, the focus is on determining whether the data of the vehicle user must be shared with others, and under what conditions this should be allowed. However, autonomy does not mean that the individual must be fully and continuously burdened with the assessment of data sharing and be faced with it unprepared because of insufficient data on the part of the user. Rather, the user should be able to delegate the examination of whether the data exchange is in his interest to technical systems, if the systems are capable of providing corresponding services autonomically and independently.

4.2. Advantages and Applications

The authors meld a multi-stage authority judgment mechanism within VECDA, which is the module for processing key data in the vehicle network and hybrid encryption mechanism. Further diverse potential vehicle security processing paths are also available here. The complexity associated with the verification of these different paths can be processed through the executor and other existing hardware facilities on the vehicle network test bench. [7]

VDVP (Vehicle Data Verification Processor) is designed as a blockchain module where two-factor (face recognition and fingerprint technology) authentication processing can be realized. This test bench puts forward a solution for the cross-field joint verification of the autonomous driving vehicle data, and uses face recognition and fingerprint recognition as key research

objectives. For the experimental test, communication between the proposed vehicle network test bench, an audi RS-Q8 and the Roadnet test bench will be necessary. Simultaneously the system can also be expanded to include further vehicle platforms road and network test benches. The current system and corresponding method is employed to ensure the cross-field joint verification of vehicle data between an autonomous vehicle and diameter simulation.

Ni Mingxin et al. mentioned security vulnerabilities in the autonomous vehicle network as a threat to travel safety. To understand and address these concerns, Ni et al. (2021) present a low-cost two-factor authentication scheme, realized on the Vehicle Networks test bench for autonomous vehicles, based on blockchain and the Advanced Encryption Standard algorithm. The vehicular networks can be divided into three sections: vehicle-to-vehicle, vehicle-to-infrastructure and vehicle-to-public. Vehicle-to-vehicle and vehicle-to-infrastructure communication is implemented through the Proportion Integral Derivative controller, Integrated Chassis Controller and Linux-based computer. This work successfully implemented the proposed authentication scheme and U= user interface.

5. Biometric Authentication in Autonomous Vehicles

We have presented an effort to provide an in-depth analysis of potential attacks and vulnerabilities to autonomous vehicles from adversarial agents. In particular, we have focused on the strength of biometrics to defend effective and secure authentication schemes. We have analyzed the potential threats and proposed a model of a secure, biometrically-enabled identification of passengers in self-controlled cars that can guarantee an appropriate level of security concerning human-centric values. In this research, we have proposed and tested several human-centric authentication systems to ensure secure access control in autonomous vehicles [24]. Biometric security measures are better than commercially-obsolete password security measures. Hence, we hope that the drivers and passengers will enjoy secured rides in autonomous vehicles in the near future.

Biometric measures such as fingerprint or iris scanners are widely used to authenticate users or passengers in autonomous vehicles. Besides convenience; comfort for the users, vehicular biometric measures are faced with several privacy and security issues. Cyber-criminals have found ways of exploiting biometric features for illegitimate Access Control; and have caused severe threats to lay users and national interest. In this chapter; we have provided a comprehensive review of facial and lip biometric authentication measures to authenticate

passengers in an autonomous vehicle [25]. Human head movements and facial expressions are highly inconsistent for many reasons such as different lighting conditions, expressions, poses, and orientations. We have designed and tested lip dynamics-based biometric access control measures to open and close the vehicle door, and to start and close the car [26]. We have also tested aid-based authentication measures as trails cannot be replicated easily and repeatedly.

5.1. Types of Biometric Authentication

Since time immemorial, humans have realized the importance of having a guardian about themselves in the absence of themselves. Be it a safe house for valuables or be it a place, probably mentioned in most of the religions, where luminous light stays in absence of its owner. A similar technology is also required today as technologies for optimization have vastly exceeded physical dimensions. For any system, the efficient working of the system is as important as the management of the security and privacy of the information available. The same thought process can be utilized for automobiles where the access control secured those automobiles from unauthorized access while their owners are absent and unmindful. Recent interest in bicommunal technologies has resulted in the production of multiple successful systems evidencing their secure authentication mechanisms. Despite their managerial success there are very few systems accessible which have incorporated more than one type of biometric method for its authentication role. The potential of accessing too trustworthy services can be achieved by adding one of the other commercial and productive technology. A very recent technology as well as more near future technology is entering the digital world is the Internet of Things. This technology is producing a massive global attack on human life and is going to play the role of same status quo while managing automotive concerns to maximize their efficiency. One of the major concerns raised for the efficient working of the Internet of Things is about producing the ability to access authenticated sensors or devices. Therefore, existing systems present latest advances of multiple biometric systems present in the digital world, which can be harnessed with state of the art automobiles and provide a secure and authenticated residence to one's automobiles.

Biometric methods have the potential of offering the most secure authentication mechanism as it makes use of the unique attributes that a human possesses. This statement is true as long the system is not adulterated by compromising on the technological algorithms. Single

biometric methods have their limitations which can be exploited by the adversary. Hence, a multimodal biometric system forms the most secure and accurate authentication mechanism . However, multimodal biometric systems have the common infrastructure as its major drawback leading to the need for an upgrade in hardware. This is where the need for a completely software based biometric system arises. State of the art technology has changed to the extent that technology dependent on optical sensors like fingerprint, iris scan, facial recognition and retinal scan are no longer the only methods to rely on. In this context, a comprehensive comparison is done to select the better technology that can be integrated with others in order to form a multimodal biometric system which leads to an improved authentication mechanism. The decision and the methodology are based upon the efficiency of the technology in terms of security perception, scanning accuracy, time consumption and freedom of range utilization.

5.2. Benefits and Limitations

The use of multiple sensors with different measurement principles allows enhancing the security and robustness of the proposed solutions and, at the same time, preventing them from being circumvented by intruders. This represents a particularly critical point for rolling further the biometric authentication to the AV system and to the introduction of L3 automated driving, where the remote driving monitoring plays a central role with respect to driver-vehicle interaction. However, the exploitation of dynamic biometrics, using time-variant intrusiveness features, represents one of the future research lines to make the biometric authentication in the AV systems more dynamic and robust in terms of system security and intruders' detection [27].

The research efforts addressing human-centric authentication systems for secure access control in autonomous vehicles provide a promising roadmap for rationalizing the existing designs and authentication mechanisms [15] and suggest their potential integration in vehicle architectures together with other security and safety technologies. In particular, unlike the existing approaches, this study puts particular attention to perceptual biometric authentication, focusing not only on cryptographic aspects but also on the human factors involved in the authentication and access processes. This human-centric approach is making use of many innovative technologies and methods, including but not limited to head movements, touchless direct gaze, gesture, touch screen, vibromagnetic sources in the head

cushion, among others, for the design of different authentication mechanisms and access control management [3]. Moreover, industry standards and guidelines have been used for a proper understanding of the state-of-the-art solutions in the automotive and biometric fields and for the definition and the analyses of new research directions and development opportunities. Neural Network and deep learning sides have also been taken into consideration to understand their potential in terms of classification operations, and to define suitable and innovative methodologies and SW architectures, improving the ones currently available in the literature.

6. Behavioral Biometrics for Access Control

There is a growing need for secure vehicle authentication systems integrated with biometrics to improve the security of automobile systems and advance connectivity and autonomous vehicle (AV) development. When providing biometric solutions for AV access control, observers predict that biometrics in AV context are likely to be used for different purposes like drowsiness detection, creation of vehicle user profiles, secure access control for shared vehicles and a lot more. While there was, and still is, extensive research in physical biometrics there is very little known about the behaviorally driven sensemaking and its intersection point in AV context. This means, that the behavioral aspects of interaction and the natural way they are habitually executed provide a measure of hidden and non-interrupting authentication method. However, despite the fact that gait is a simple movement that arises because of different neuromuscular diseases, gait abnormalities are treated by specialists especially in elderly and pregnant patients and can cause many difficulties in these different patient groups [28].

With the increasing complexity of human-vehicle interactions, the incorporation of biometric authentication technologies in vehicles is becoming critical. Although various biometric authentication modalities can be used to ensure secure access control in vehicles, behavioral biometrics is considered to be a particularly suitable alternative. Behavioral biometrics are intrinsic to the human body, non-invasive, and user friendly. Moreover, the biometric data used for recognizing individuals is less likely to l eaked or compromised compared to traditional biometrics such as fingerprints and iris scans. Among physical and behavioral biometrics, gait and eye movements directly correspond to the neuromuscular system and

have been investigated by numerous researchers as a means for identifying individuals with different applications [29].

6.1. Concepts and Methods

Authentication solutions based on digital signatures appear to be widely considered in the case of Smart Devices such as Autonomous Vehicles, but also in the case of Mobile Personal Devices of Users (Smartphones, Smartwatches—see later) or roadway-side infrastructures (e.g., RSUs). In places where third-party infrastructures are not accessible or are not reliable, one prevailing solution is to use vehicle-centric authentication schemes, i.e., schemes able to provide a secure form of authentication by leveraging information and resources stored in the DV or VV. In the vehicular field, vehicle-centric schemes can be virtually considered for both vehicular ad hoc networks (VANETs), using DSRC/WAVE protocols and services, and also for vehicle-to-everything (V2X) communication, in the context of the C-V2X paradigm. A TBVE is any single piece of information which makes two distinct entities hard to repeat, e.g., signs, natural or artificial physical appearances, or knowledge about past occurrences. Even if there are no formal proofs of TBVE schemes in terms of theoretical security, so far, there are known feasible implementations of secure primitives to obtain a well-scalable security, which is close to the best achievable security.

User authentication is a fundamental component for the security and privacy of Smart Devices, autonomous systems, and applications, where vehicles are included in the broad category of autonomous systems [30]. Although previous works have not presented a comprehensive view, many proposals and solutions can be identified and grouped in mainly three categories: vehicle-centric, device-centric, and user-centric [21]. Starting from these schemes, security and privacy goals and requirements that can be common to different application domains — in particular the require- ments arising by applying the devices or applications to intelligent transportation system (ITS) scenarios — are introduced and practically discussed. The aim is to identify the different classes of methodologies, protocols, and solutions, their main strengths and weaknesses, and their areas of application and to underline the open issues and possible future direc- tions for improvements, also being inspired by current novel research developments such as credentials-based authentication, identity federation, and zero-knowledge proof techniques [31].

6.2. Use Cases and Effectiveness

(2) The behavioral biometrics are less vulnerable against spoofing attacks with respect to a physiological biometric system. (3) The newer devices have mostly focused on behavioral or interaction-based biometric authentication systems that can be implemented in smart environments where the user will have to interact with different kinds of computing device systems for different kinds of services. A deep understanding of the human factors, including the security and usability advantages of the newly proposed human-centric authentication approaches, could provide opportunities to develop more effective authentication systems for smart car systems.[32] A smart and secure authentication mechanism for IAM, and perhaps more importantly, for a user's privacy, enjoys substantial significance if we want to design a secure and a smart car mobile IoT systems. Using human-centric multi-biometric user identities, we propose an innovative authentication system that uses the voice, keystroke, face, gesture, and walking patterns derived from sensors in an ubiquitous environment as behavioral biometric traits. In addition to more traditional biometrics, behavioral biometrics related to interaction patterns with smart objects are also used to form an 'object interaction-based identity.' These multifaceted user identities are then used as a smart car IoT device secure identity. For our evaluation, the standard dataset ULMFiT is used for training and evaluation, including a perturbed dataset. Later, the developed system will be tested on real-world devices such as smartwatches, smart glasses, smart cameras, and smartphones and will demonstrate a better secure, usable and functional system. From the evaluation, it is found that the proposed interaction-based biometric IoT authentication system is better than the conventional counterpart in terms of user usability, the security of the IoT devices, the smart car systems, and user privacy.

[2] A smart car ecosystem is a network of vehicles that communicate with each other and with other entities to improve passenger convenience, minimize traffic congestion, reduce driver fatigue, and enhance transportation safety and efficiency. The need for secure, safe, and usable authentication mechanisms in smart car systems has led to the development of different authentication systems. While various authentication systems can be proposed, human-centric biometric advances have provided safety and usability enhancements in IoT systems such as smart cars. We adopt a biometric-based authentication system for enhanced security in smart car access control. Through the evaluation, we show that human-centric biometrics are more secure against attacks and threats affecting smart cars and IoT devices since they mainly rely on an intrinsic unique characteristic of humans, but the non-human based IoT

devices do not have such a unique characteristic. Even though a biometric-based authentication system has less loss or vulnerability, a behavioral biometric-based system has the following superiority over a physiological biometric-based system: (1) one user can keep multiple devices and the behavioral biometrics will be different for different devices.

7. Multi-Factor Authentication in Autonomous Vehicles

A blockchain-based group signature scheme is the AuthChain [21] scheme, which leverages a multi-factor authentication approach through an improved Authentication Schema for groups of vehicles. The AuthChain security guarantees are maintaining of message confidentiality, anonymity, message integrity, untradable, fair traceability, and achieving an upper bound on both 1) the number of group security burdens in semi-adaptive adversaries and 2) the number of vehicles in RSUs. Its security proofs rely on an authentication second model in the ROM, while it has semiadaptive identity-based policy prevention in the RO ROM. The user's trust registrations for legal interactions within the AACS are interpreted as provenance registrations made in the AAPP, and the usage of the RO ROM leads to a less stringent security definition. The AuthChain scheme is compared to the AuthN [8] group signature scheme as well as push-pull methods and an extension of the Digital Signature Algorithm (DSA), extended as the ECDSA. Each method complicates in the authentication protocol's implementation in IoV, namely the timing, communication, and computational cost.

Idemix [33] identity-based cryptography scheme can be realized using Group Blind Signature (GBS) to generate pseudonyms of a specific subject as a blinding factor without disclosing the real identity. The GBS scheme is crucial in delay-tolerant networks such as IoV, in which mobile vehicles and RSUs communicate for a temporary period and disappear. However, Group Signature (GS) certification resolution, a relatively outdated concept that assumes all communication is one-to-one, was used in the work. The Group Signature (GS) can also be adopted for Group blind Signature (GBS) with the credentials scheme. By the GS mechanism, the attribute revocation problem presents certain inconveniences, and the majority of the grouping strategies require entities' keys to continue the attribute-based anonymity procedure.

7.1. Components and Implementation

The essence of human-centric authentication should include secure and transparent access to web services, data retrieval from connected databases, secure transmission and communication, role- and contextbased authorization and activity tracking including change management. Continuous login or password authentication policies that do not consider environmental conditions are of significant use in complex environments. Hence, the user authentication process must be supported by various mechanisms and systems. To exemplify, the ongoing personalization process leads to customizing settings, including the ones related to password and policy management [22].

Managing the authentication process requires substantial system intelligence to keep users secure and allow them to operate various components seamlessly [34]. With the smart environments emerging, user's authentication should be passive and seamless, which means they have to be off-the-cuff and at the same time able to distinguish and act on user's activities. However, protecting users' identification information and privacy is very crucial. The lack of support for this individual has led to the unintended identity theft, privacy invasion, and severe consequences [8].

7.2. Security and Usability Considerations

The security and usability considerations are a fundamental consideration in the design of human-centric authentication systems assessment of biometric and location-based methods [34]. The adoption of a human-centric approach in HiBlockAuth allows an integration of location-based authentication techniques and the conventional biometric methods that are used through the infrastructure of the on-board units in autonomous vehicles. This integration allows us to smoothly move from a biometric authentication of the user to the use of a location-based approach without causing discomfort to the user during the driving of the autonomous car. This is possible at any time that the on-board units consider it necessary to re-authenticate the user to mitigate any malicious attacks like the rainbow attack demonstrated in Sect. 6. HiBlockAuth merges usability and security into an overall system combining strengths of multi-factor authentication and single-factor authentication systems, while aiming at minimizing their weaknesses.

We propose a secure access control system called HiBlockAuth (Section 2), which is a BIometric and LOCation-bAsed autHentication system that uses blockchain technology to securely process user requests. HiBlockAuth allows the vehicle to authenticate the user and

check for any malicious activities from data generated during authentication mechanisms. An important contribution of our work is the investigation of the system's usability using state-of-the-art security methods in homogeneous and heterogeneous methods [35]. The usability results were obtained using a driving simulator equipped with a quantitative analysis of subjective feedback assessing the usability perception of the two authentication modalities. The system offers the following advantages:

8. Case Studies and Industry Examples

Precisely because of his general use of the blockchain, it is possible to apply a biometric-based authentication algorithm between the user and the server, requiring the user to create a multimodal configuration using biometric information. As such a configuration can evolve over time due to interaction with an evolving system, skeletal movement and posture recognition become necessary [36]. To facilitate this recognition in a dynamic environment, the authors propose an innovative methodology to address the co-registration and visibility problem. The evaluation of the system in different environments shows a reduction in multicollinearity between biometric sensor modalities at higher levels of squat recreation, effectively limiting the visibility mask that interrupts access to the AV.

Block-chain technology can establish a creditworthy ecosystem for identification, authentication and access control in the AV [35]. In an American study introduced in [37], even 71% of participants expressed their willingness to authorize the AV. Pillette et al., propose a secure and lightweight biometric-based protocol, which incorporates an identity-based encryption (IBE) scheme for secure access control based on the distributed security using blockchain technology (BC). Unlike the IBE protocol, the blockchain is used to securely store the vehicle's public key and the user's biometric information stored as a private key, so no trusted authority is needed.

8.1. Implementation in Commercial Autonomous Vehicles

Interactions, behavioral patterns, habits, and features of the intelligent systems can be copied and faked by attackers to gain unauthorized access by employing Generative Adversarial Network (GAN)-enabled fake multimodal features. Authentication mechanisms based on only one sensor (i.e., a singular vision system, behavioral measurements) can be vulnerable to such adversarial attacks [38]. They propose an extended user-centric architecture and an

exploration (Simulated and Virtual Kernel Diagram lattice: electrical and electronic pulse models with the kernel graph lattice–association, as a background brand) of MHC to protect such privacy and ownership issues and thus deliver privacy-preserving and ownership-preserving modern vehicle automation that the users can trust.

Self-driving vehicles form a global market with different leading companies now integrating various vehicle autonomy features. The global market is diverse and encompasses many different automobile companies, regions, and stakeholders. Some leading vehicle manufacturers and technology companies have begun delivering up to Level-2 and some Level-3 autonomous driving functions in their cars. However, the widespread use of autonomous vehicles is still limited by many concerns. The rising concern presented is in protecting autonomous vehicles from cyber-attacks. Hence, new and sophisticated cyber security attacks have been introduced in connected smart cars that illustrate the vehicle autonomy features' vulnerabilities and attack scenarios from the CAN bus to cloud-based services [2]. Most autonomous cars are using LiDAR as a principal sensor that measures environmental characteristics systematically and extensively, making hackers understand autonomous cars and manipulate them.

8.2. Success Stories and Lessons Learned

Currently defined standards and new sensor technology for drowsiness detection show promising results and have been found to address a key problem of driver drowsiness effectively by using heart rate variability measured silently. A face recognition smartphone app using triangulatory photogrammetry is also found to have tremendous potential applications, not only in autonomous vehicles, but also in VR, health, and education [36]. This work combines the benefits of forensic intelligence with multimodal user recognition inherently designed for an intelligent car. The design and implementation may be operated autonomously in an L4 scenario. It achieves lifelong learning performance with only 0.18% reduction in efficiency, ensuring security, continuity, and anticipative vehicle maneuverability behavior improvements. This work offers immersion character within the intelligent vehicle, etc. Application of the innovative system grants the driver the flexibility to respond to the car production during the access control context, featuring efficient continuous authentication, until the car models its AI-enacted anticipation-based context assessment likely [39].

Behavioral biometrics, such as gait and vehicle control, can enable continuous user identification in vehicles and provide continuous low-intrusive authentication without interrupting the driver. However, user behavior changes, reducing accuracy. In order to address this challenge, the study leverages a population-based approach to diagnosis user behavior shifts using a generative modeling method and trains user-independent generative models. Other user-behavior-based authentication schemes have often been attacked and proved to have low robustness. Defense techniques, such as feature extraction and classification, have also been proposed to mount attacks and make user-behavior-based authentication schemes more secure [38].

9. Challenges and Future Directions

Future research directions include developing human-in-the-loop validation to address potential biases and inaccuracies and forging a true trust in the face of adversarial inputs, exploring security analysis beyond adversarial machine learning for autonomous vehicles by addressing digital and system-level attacks and developing comprehensive metrics for autonomous vehicle AI models impacted by adversarial machine learning, conducting real-world testing to evaluate robustness of security systems in practice under the interactive influence of adversarial attacks and safeguards with human machine interfaces (HMI) through vehicle testbeds and augmented reality systems, and integrating explainable AIs (XAI) techniques to make AV decisions more transparent and understandable. In addition, future work is necessary to examine how customized experimental settings affect drivers from different cultures and explore novel human-centric authentication mechanisms for drivers and passengers with disabilities. It is also critical to consider human factors involvement in the AML adversarial attacks detectability User needs to be considered in terms of testing conditions and application scenarios in recent cyber-physical systems. [1] [40]

In this article, we presented a comprehensive review of the human-centric authentications systems and categorically explained the concept, human-in-the-loop, and attacks and their defenses to improve security solutions in autonomous vehicles. Despite the comprehensive analysis and solutions, human-centric authentication systems need to address several existing and future research challenges and direction to improve the actual driving scenarios security and safety. Age-related changes in vision, hearing, motor, and abilities are challenging in developing practical approaches of human-centric authentication techniques for the older

adults in HADs. To solve this issue, we need to require to establish a baseline for physiological measurements for the elder group along with the middle-aged and younger people to extract the features of each individual and apply machine learning and deep learning models to provide consistent and continuous authentication in autonomous vehicles.

9.1. Current Limitations and Issues

- By the design, the proposed human-centric mutual authentication protocol for autonomous vehicle systems provides evolving adversarial threats at both client and edge network levels. For a case, at the edge network level, if the ABS is malicious, then she can use the personal data of the client to clone a token making the real client unable to access an autonomous vehicle as per her requirement. Further, by using public-shared immutable data in the edge network, the adversary can compromise the client's privacy. Though the protocol is designed to function in a resilience of adversarial model when the adversaries act as per her selfish interest, but it cannot withstand such adversary, who try to inspect or learns new insights of the system by borrowing some help. Moreover, an adversary can compromise the system by using an autonomous vehicle's system. As the client's human-centric data becomes public-shareable, any adversary can reuse the system and violates the anonymity: this issue severely restricts the attractiveness of applying the protocol in the real-life scenarios for the autonomous vehicle, especially for the concerning personnel. Moreover, the need for extended computational cost constraints of the system due to the use of various cryptographic primitives is observed. As the ABS is already a resource-constrained entity, the extended computational cost limits the use of the protocol in real-world autonomous vehicle systems.

As elaborated in the analysis and discussion of the current limitations of the Human-centric Authentication Systems for Secure Access Control protocol for autonomous vehicles, a number of limitations can be observed and the resulting issues can be discussed as follows: [36]- The client's personal data remains exposed to an adversary in the public-shared immutable blockchain. Therefore, an adversary with less computational resources can obtain the identity of the client from the data stored in the blockchain. The exposure of the personal data restricts the use of the protocol in real-world scenarios. For instance, an adversary can easily retrieve the biometric data of the authorized personnel from the blockchain of the edge network. As one of the limitations of the protocol, the use of third party data owner (TDO) has been noticed. This will increase the cost of the system, due to the presence of an additional

trusted domain holder. In the case, when the client directly registers or digitally certifies with the ABS, then the use of TDO can be nullified, and the discussions associated with TDO can be avoided.

9.2. Research Opportunities and Emerging Trends

It is important to thoroughly validate the developed hybrid AI–HCA systems strategies with global— and potentially "invisible"—adversarial planning, design, requirements, and test data [41]. It is vital to explore and to expand the broader security analysis prior to deployment AI safety, identifying HCA vulnerabilities or system usage errors that can be exploited, or utilized to launch attacks against the proposed AIs. These important identifiers need to be explored in future work. The complexity of future AI–HCA ecosystems in AVs is envisioned to require their own conscious strategies to de-layer, interconnect, and secure in terms of hybrid AI–HCA systems strategies. Lastly, ethical multi-stakeholder engagement and AI/AV safety data assets to validate AI–HCA system performance, verification and validation can be ethical and legal conformity enhancers for HCA within the adaptive AI solutions.

It is imperative for future AVs to be equipped with multimodal HCA for drivers, passengers, and road authorities to experience a secure and trusted environment as a consequence of using these adaptive traits. The application includes monitoring humans in the loop and AI modelers to enhance robustness and resist post deployment issues [42]. HCA applications are in development to maintain ethical and legally acceptable human–machine mating, to ensure safety and privacy with ethical AI. Thus, the proposed developments are fundamental to enhancing safety and experience in autonomous driving environments and prolonging good relations and trust in future vehicle designs. The expanded roles and responsibilities of AVs require continuous exchanges, data collection, and interactions from and to different AI and HCA systems. Therefore, future work expanding explainability, cognition, and preserving privacy are timely research topics.

10. Conclusion

Finally, the article introduces a Quality of Service System for a Voice over Internet (VoIP) consisting of three actors: primary (VOIP Servers), secondary (VOIP device), and user triage. Consequently, the National Institute of Standards and Technology (NIST) has presented physical liveness attacks unby a responsible People's Birla's Strength According to the Spin

Paradigm. This work weaves together secure, impurity-based spin qubit hardware devices with quantum protocols, including quantum Key Distribution (QKD), spatial cryptographic quantum communication approaches, and Downlink Layer (DL) Privacy Support [37].

This is an important domain for autonomous vehicles, and this article has explained a novel authentication model to identify six tactical activities for safety, comfort, and entertainment. It automatically explores six bioacoustic-based activities by extracting ten prominent acoustic features to describe inter-class variance. The authors have confirmed the presence of noise resistance features using the ANOVA test and have also underlined the accuracy increase using the backward selection technique. Consequently, the low-cost lighter touch bioacousticactive model implements the piezoelectric fibre sensor for active listening. It promises to develop IoT bioacoustic products to satisfy the safety, health care, industry (IIoT), human–robot interaction, and security services by robust behavior of the accuracy, security of RBFNN, and synchronized health features. Consequently, the user suggestions are to imminently support the movable electronic devices by bioacoustic-based Android and IOS-2022 systems. Ahjapal has realized verification tasks using a voice killer or burner (VK) device, enabling a novel approach for identifying voice recognition problems. Nevertheless, the voice contains a user digital serial number, making a real-time secondary path for imposters to access the voice servers. This short communication suggests a brand-new hybrid model that utilizes acoustic antivirus (AV), biometric behaviour (BB), hybrid speech signature enumeration environment (HSSEE), and privacy protection for the voice biometrics, ensuring five categories of safety regulatory networks.

The existing authentication systems for verifying the identity of the drivers and their passengers typically function as radio transmitters, or standardized visual or vocal messages that confirm the identity of the AI system–user based on pre-defined policies. Of these features, physical characteristics including fingerprints, facial features, and iris colors are especially well-documented [15]. Even though these are accurate, straightforward methods, their security is low as the systems can be hacked through various means. The newfangled VoiceSSH model that authenticates the voice and user identity simultaneously introduces managers for every phone and its features including mouse, keyboard, and other program system [38]. The smart manager assigns to each phone operation a value which restricts the access of the mobile devices. The author presents three methods to enhance the effectiveness of the proposed model, such that the efficiency of voice recognition and verification increases

effectively with these models. It is important to underline that there have been enumerable research works on bioacoustics-based authentication models, however, to our knowledge, this paper proposes the first biodetection technique, using a low-cost embedded microphone that supports voice verification strategy in car environment, offering high security as well as accuracy.

10.1. Summary of Key Findings

[43] [44]As we look to the future, transportation is predicted to use more and more automated solutions, from cars and buses to trains and ships. This will reduce congestion, lower emissions, and make journeys more comfortable, and will also profoundly affect jobs, behavior and daily life [2,3]. However, humans are not used to staying passive once they have learnt the logic of driving and have legal responsibility, and are unlikely to be willing to trust the life-and-death decision-making process of AI due to situations they might not be able to handle. Therefore, it is difficult for people to obtain appropriate trust in, and remain in control over, automated vehicles (AVs). Interesting and challenging work has been reported in, the main contributions of the paper are briefly discussed as follows: (1) Previous studies have revealed that people do not have an appropriate understanding of AVs or high enough cognitive abilities to be able to understand AVs' behaviors and make judgments about how safe and smooth AVs' operations are [2,5]. Evidence has shown that people sometimes want to abandon the control to AVs in order to obtain a positive feeling in times of weakness, yet they cannot trust AVs completely.[45]It is possible for computer hackers to harm future transportation by remote users, irrespective of how safe and comfortable it may be. More seriously, some researchers reported that the camera, LIDAR, and ultrasonic radar of an AV could be hacked by using jamming, replay, and spoofing attacks on the controller area network (CAN). As the mainstream technology, nearly all electric and electronic components in modern vehicles are based on the controller area network (CAN). These communication protocols are based on arbitration which can cause denial of service by the manipulation of CAN communication messages such as the lethal bit stuffing, the notorious long stuffing bit or the faulty frame format. These issues impose new challenges for privacy providers and especially for automobile industries. Therefore, it is critical that all cyberspace communications are secured. As a result, many research studies on the authentication and key management for in-vehicle networks have been introduced over the recent years. Generally, authentication protocols for the CAN can be classified as key or keyless ones.

However, the authors focused on the key-oriented protocols studying on their security properties, strengths, and weaknesses in this paper. In, a methodological model is developed in order to compare, analyze, and discuss security properties of the selected representative protocols by considering 11 features. This research contributes to the design of future automotive E/E architectures in which both external and internal threats are addressed in an integrated way.

10.2. Significance and Implications

[35] As an innovation in connected vehicular technology, Connected Autonomous Vehicles (CAV) technology and its network have brought several technological, operational, and social advantages. From a technological perspective, CAV technology would represent a breakthrough in a few areas, such as energy consumption efficiency, traffic capacity and travel time efficiency, and consequent pollution reduction. On the social front, this mobility innovation could help maintain community structure and improve individuals' Quality of Life (QOL). The security challenges in CAV technology thus present a significant barrier but also signal for the scope of research and development that can help to remove these barriers. [38] The credibility of human–machine interfaces is crucial in ensuring safe and trustworthy user interactions. Autonomy, usability, and interactivity are closely linked, as safety-critical decisions made in autonomous vehicles should be determined by responsibly attended users. Functional arrangement of critical vehicle controls, functionalities, user access management, and situational awareness in autonomy should retain vital human involvement. Identity management and access control are salient concerns within the growing community of connected autonomous vehicles (cAVs). In this context, human-centric authN technology is just at the modern mobile device era. Extending these concepts to cAV users raises a number of new challenges. This work identified security concerns in Driver Centric Authentication (DCA) and Passenger Centric Authentication (PCA) within cAV in terms of, authenticity, user impersonation and property jeopardy. Moreover, dynamic authentication of passengers is a nontrivial issue for enabling seamless experience in the cAV ecosystem.

Reference:

1. Tatineni, S., and A. Katari. "Advanced AI-Driven Techniques for Integrating DevOps and MLOps: Enhancing Continuous Integration, Deployment, and Monitoring in Machine Learning Projects". *Journal of Science & Technology*, vol. 2, no. 2, July 2021, pp. 68-98, https://thesciencebrigade.com/jst/article/view/243.
2. Prabhod, Kummaragunta Joel. "Advanced Techniques in Reinforcement Learning and Deep Learning for Autonomous Vehicle Navigation: Integrating Large Language Models for Real-Time Decision Making." *Journal of AI-Assisted Scientific Discovery* 3.1 (2023): 1-20.
3. Tatineni, Sumanth, and Sandeep Chinamanagonda. "Leveraging Artificial Intelligence for Predictive Analytics in DevOps: Enhancing Continuous Integration and Continuous Deployment Pipelines for Optimal Performance". Journal of Artificial Intelligence Research and Applications, vol. 1, no. 1, Feb. 2021, pp. 103-38, https://aimlstudies.co.uk/index.php/jaira/article/view/104.