Ethical Implications of Biometric Authentication Systems in Autonomous Vehicle Operations

By Dr. Wei Xu

Associate Professor of Electrical Engineering, Shanghai Jiao Tong University, China

1. Introduction

It has been observed that the increasing rate at which this biometric technology has been adopted, some vital risk factors primarily revolving around privacy and security have been identified. Speculations concerning how such personal biometric information can become vulnerable to abuse needs an urgent consideration. This study intends to address the ethical implication revolving around the BAS in AV operation. Although BAS present an accurate, impersonal, non-transferable and inexpensive solution to personal identity, concerns over security vulnerability suggests that the acquisition, storage and processing of sensitive biometric information makes BAS a valuable resource for attacks, especially arising from the 'insider' threat within autonomous vehicles for malicious intentions or from external actors for bypassing the human presence check in autonomous vehicle operations. Several privacy concerns emerging from the unauthorised access, usage, and handling of biometric information are of interest to regulatory bodies and stakeholders [1].

The deployment of autonomous vehicles has dramatically accelerated over the last couple of decades [2] and has already sparked public debates about ethical issues surrounding the introduction and use of these systems. Among the ethical challenges introduced by autonomous vehicles, some of the most controversy has been elicited by the ways in which these vehicles should behave in emergencies and other life-and-death situations (cf. the "Trolley Problem" in Philippa Foot 1967, Judith Jarvis Thomson 1976, and Thomas Nagel 1976). The "Trolley Problem" describes a series of situations that demand making ethically relevant choices about saving the lives of a group of people while sacrificing the life of another individual. For instance, in one of its variants (Thomson's Loop Variant omitted), the "Trolley Problem" involves a lever that can be pulled to switch the track and send the trolley onto another track, which would save the lives of the people on the initial route, while killing one or more individuals placed on the alternate route. Biometric authentication systems (BAS) have emerged as a strong prospective solution to several identified problems of manual and traditional authentication systems in meeting the requirements of Autonomous Vehicle (AV) operations in an intelligent transportation system [3].

1.1. Background and Significance

Many privacy concerns have been raised around the implementation and use of biometric systems. Due to the presence of a vast amount of personal data, biometric systems have the capability of eroding privacy. Collection, storage, search, and misuse of such sensitive biometric data leads to legal and ethical issues. In the context of autonomous vehicles, biometry is gaining importance as an innovative technology for the next generation of user identification in the car. This paper focuses on biometric authentication mechanisms with regard to their integration into the access control system and use in driver assistance systems of AV [4].

Simultaneously, a range of ethical and legal implications of biometric systems are becoming increasingly recognized. The ethical and legal implications play a crucial role in the adoption of biometric systems in a number of practical applications. The bias against certain demographic groups, capability to invade privacy of persons, ethical implications in the access control system of autonomous vehicles are discussed in [5]. It is important to understand that biometric systems are not error-free, and result in statistical errors. It is therefore important to append the results of biometric systems with demographic constraints. The accuracy rates of a particular biometric system may also vary due to physical disabilities, skin conditions, cultural variations and different expression. .

1.2. Research Objectives

Therefore, the overall objective of the current work is to systematically investigate the ethical implications of biometric authentication systems in autonomous vehicle operations in various driving and non-driving scenarios. Specifically, we will: (i) review existing advanced driver-assistance systems (ADAS) and information system literature in order to identify and describe the challenges of biometric, especially face recognition, systems in autonomous vehicles; (ii) conceptually discriminate between in-car and post-ride biometric solutions and identify driving and non-driving scenarios, ethically critically analyzing the specifics of biometric systems; (iii) propose an ecosystem approach for handling different legal and ethical relevance of information according to user preference (privacy) evaluations, meaningful consent handling, and benefits for operators.

Biometric systems used for passenger authentication in autonomous vehicles have been gaining increasing interest in recent years [5]. The use of biometric systems ensures secure and seamless passenger identification, which, in turn, mitigates the risk of unauthorized persons accessing AV. However, in realistic scenarios, biometric systems generally have to operate in a similar manner to systems outside an AV. In this respect, the ethical considerations ensuing in autonomous vehicles could be expected to be similar to those in any other public context, and, thus, there should be no need for ethical challenges exclusive to biometric systems used in AV. However, this assumption is a naïve one, as the concept of autonomous driving itself is in the process of fundamentally changing the way tracking and personal identification are carried out outside the vehicle.

2. Biometric Authentication Systems in Autonomous Vehicles

The ability to recognise the driver sitting at the car's steering wheel is not a problem when the car is driven in an old-fashioned way, i.e., by a human driving the car. Then, the identity of the driver can be easily verified not only with help of the seatbelt-mounted sensor ensuring the presence of the user at the driver's seat, but also with the driver's surveillance camera [6]. One may license the driver by checking his/her personal driving license at the first-time driving the car or getting into the car. However, the car users do not love being forced to put the seatbelt on every time they drive the car and they are not also fond of every car having installed some costly surveillance system. How then can the user be recognized in a car as he/she sits in the car, puts his/her bare hands on the wheel, without having to tie up with a seatbelt?

There has been a surge in biometric research in the automotive industry, with one particularly strategic area for the implementation of biometric systems being driver monitoring systems (DMS). In autonomous cars, where users relinquish direct control over the vehicle in favor of the AI, the issue of user's presence and capability to operate the car safely becomes crucial. The classic biometric measurements for this purpose, which are disseminated by fever of today's clever cars, range from body posture, gaze, face expressions recognition, through voice pattern analysis [7]. Highly advanced forms of biometrics at the steering wheel encompass physiological body changes, such as galvanic skin response, heart rate and blood pressure, etc. [8]. They all embrace one commonality: they assume the driver exists and is present at the driver's seat. As cars get smarter and more autonomous, the role of human driver is diminishing. This results in a new, challenging situation, that is, it is difficult for such sensor-technology to correctly recognize events in which driver becomes inactive, that is, lethargic, sleepy, or unconscious.

2.1. Overview of Biometric Authentication Systems

Nonetheless, despite numerous security applications, there still exist loopholes rendering the available biometric systems vulnerable to several types of attacks varying from virtual attacks through digital systems to physical attacks, targeting the biological features of the individual. In case the biometric data of the user is stolen by an adversary, it will then be permanently available with the adversary, and the user would not be able to change the same as we change our bank password in regular intervals. The privacy requirements of the biometric data are hence, different from other traditional security measures, and the same becomes a chief cause of concern for the user. As such, any compromise the biometric data of the user would be a severe breach of privacy and raises ethical concerns. Different countries have framed very stringent laws to handle biometrics. The new generation of semiconductor devices in smart phone applications integrate high-performance and efficient security functions controlled and processed by a single chip, such as touch ID to unlock the device, Apple Pay, and other security functions for biometric authentication. Several types of biometrics are explored and compared, for the next generation security. Biometric identification is a hot topic as it offers a secure method to access a smart phone without requiring the user to remember a PIN or password.

The primary focus of biometric authentication systems is to establish and verify the unique identity of their user through the biological and behavioral characteristics possessed by the user. It offers a much more reliable mode of identity management as it helps prevent theft and restrict access to only authorized personnel [9]. The most prominent examples of biometric authentication are present in our daily lives in the form of facial recognition and fingerprint sensors in smart phones and the sensors found in smart watches and other healthcare wearables. Besides, several facilities and shopping platforms have incorporated biometric authentications for restricting access for unauthorized personnel. The major advantage that the biometric system provides over traditional methods of security is that the user need not remember the password or carry any kind of identification proof to access his or her device or data; the system is biological and can not be replicated artificially.

2.2. Integration of Biometric Systems in Autonomous Vehicles

When it comes to autonomous vehicles, the role that the driver would play is uncertain. This becomes a problem when discussing biometric authentication systems in autonomous cars. Some people wonder whether it is necessary to include biometrics in autonomous vehicles, while others believe that the cars should have biometric authentication systems exclusively to avoid hacking [10]. This is a characteristic of Level 3 and Level 4 systems and can solve some security problems, especially with remote control, but it can also create great ethical concerns. If a biometric platform is created specifically for this vehicle, with the belief that it is safer than any other system, the potential for hacking increases. If we get used to the fact that some ADAS are unlocked only once the vehicle recognizes us, it can be said that the biometric data of the driver ends up in the file that the vehicle keeps on him/her. In addition, drivers would have to be careful about the information the autonomous driving system receives and uses [11]. When people think that they're identified in a way that goes beyond what they look like, such as with biometrics, their attitude changes. Therefore, while perceptual studies would be very interesting to understand the effect of biometric authentication systems, it can be anticipated that a major concern is the lack of privacy. All manufacturer vehicles are easy to hack, as they are connected to the cloud, and the data can easily be downloaded and stolen from the vehicle file. In addition, not all people want the vehicle to continuously monitor their physical state. Finally, if autonomous vehicles locked or unlocked based on the advice given by their passengers, they would not provide the biggest responsibility a driver faces, after all, which is to unlock the vehicle and respond to check calls.

3. Ethical Considerations in Autonomous Vehicle Operations

At last, the technical complexity involved in these issues should not be underestimated. An understanding of the potentially far-reaching ethical and psychological harms that can be associated with implementations of affective technology in cars is necessary. A user that had the ability to continually fool the affective system into thinking that they were successfully being detected as vigilant, essentially circumventing the system and ensuring that they do not need to take over driving control, would be of great concern. In that context, all considerations would need to be re-evaluated, as the purpose of affective computing was to prevent exactly that. As affective systems develop and change, more considerations of psychological well-being and how such a history of below-par performance on the part of the system should be taken into account reside in the outcomes considered in operational, unexpected driving mode rests only on the vigilance detection system to facilitate a smooth transition from system control to driver control [12].

In addition to technical and legal requirements and standard ethical considerations, the usage of biometric authentication systems also raises psychological and sociocultural issues in the specific context of autonomous vehicle operations. Implementing biometric authentication and affective computing systems to verify and to influence the passengers' attention, vigilance, and emotions may be legally and technically necessary, yet it could also bring about unintended as well as far-reaching undesired effects regarding data analysis, data protection, and psychological well-being. For instance, car manufacturers will gain access to profoundly sensitive information about the individuals using their products which, if exposed, have the potential to cause severe harm to individuals [13]. Furthermore, passengers' manipulating the verification systems proactively or reactively to "trick" the vehicle into inappropriate driving behavior or to "authenticate" another entity not actually present in the car must be considered a source of previously unforeseen ethical problems in autonomous traffic. The more general consequences of using artificially intelligent systems in cars have primarily been discussed in the context of attention and the psychological wellbeing of the driver, e.g., [2].

3.1. Privacy Concerns

Trends in Building Automation Systems (BASs) demonstrate that AVs are becoming increasingly sophisticated. In turn, building management system (BMS) are increasingly likely to use bio signals for access control. In their New Pillars for A Seamlessly Connected and Integrated Multi-Layered and Cross-Sectoral Data Privacy Protection, the need for general data privacy attests to continuing access control sensors. The authors challenge connective inferences that would result from out-of-sight surveillance systems and lack of individual contact. This is what we refer to as the philosophy of privacy by design. Privacy by design is exhibited implicitly in the application of less invasive biometric readings, including electrocardiogram and magneto-encephalography [14].

In level 3.1, we focus on some of the potential privacy concerns that emerge in the interaction between automotive systems and their drivers, yielding potentially unauthorized data transferring and storage of traveler's biometric information without their knowledge and consent. An interesting paper intended to summarize in a holistic manner all aspects of AV privacy. This survey reviews and classifies the literature in terms of the privacy concerns emerging in the AV systems according to the personal vehicle components. The authors present in-depth discussions about all the types of personal vehicle privacy, encompassing their subcategories in this work [15]. Based on these discussions, they could derive a comprehensive personal vehicular privacy framework to categorize and overview the existing evaluation methods and solutions.

3.2. Data Security and Ownership

Considering the protection of the security and privacy of the users of the autonomous cars and simultaneously to create a demand for the example of autonomous cars at a level allowing safety measures and maintenance of the quality of this concept in the market in the long-term, it is noticeable that the requirements for the safety of users are the main values. Thus, the approach of automotive companies is ambiguous, although they know that sometimes to the automation of the movement of cars only it is possible to ensure necessary level of safety. Interest connected with the implementation of mechanisms that would prevent the use by unauthorized entities and technologies of autonomous Instant Messaging, technologies whose main features would allow obtaining information concerning the position, speed, direction of movement and the remaining parameters of inhabitants, are parts (since only thanks to active cooperation of such specialists it would be possible to develop an instrument that would enable the implementation of regulations affecting the lack of access to autonomous. Different legal regulations related to the protection of personal data and privacy, particularly the General Data Protection Regulation in Europe, whose penalties will probably exceed 30 million euro, significantly influence the safety features of autonomous cars, the absence of those penalties puts protection of proprietary materials in the sphere of algorithm of autonomous technologies which are developed without the participation of specialists notwithstanding from the of opinions and functional models.

There is very little tradition in the area of intellectual property related to IoT. That lack of tradition results in uncertainty, because this concept does not comfortably fit with a system of intellectual property protection based on legal rules developed for traditional copyright, designs, patents or trade mark protection. Intellectual property rights which would be a useful means of ensuring protection of the mass of information gathered by the IoT are a sum of technical knowledge and proprietary data. For the proper functioning of the IoT it is crucial to develop solutions ensuring the balance between economic interests of the entities developing equipment, together with technological solutions for the IoT, and the interests of the users purchasing and using the Internet of Things. It would be beneficial to recognise the existence of derived rights to the sum of knowledge consisting in technical knowledge and proprietary materials created to implement this knowledge, with respect to the Internet of Things, to enable identification of the creators and to make settlements and create ways of distributing the rights related to the infrastructure of the IoT [16].

4. Hybrid Models for Threat Detection in Autonomous Vehicle Networks

In recent times, a software-defined network (SDN)-based secure autonomous vehicle (SAV) network is registered with the U.S. Department of Commerce on May 30, 2000 [17]. Many sectors are constantly performing implementation and methodological evaluation using such SDN. It is crucial because some traditional vehicle functions are enumerated for successful inconsistent effort and have replaced expectedly by digital vehicular services through software programs. Therefore, traditional approaches of automotive network are not ideal for building up security and trust where the main functions of vehicle operating systems are vulnerable for attacks and hard to detect intruders. There are multiple modes and turning points to detect malicious activities to disrupt or reduce deliberate intent of gatherings.

Hybrid intelligent model IT3_SDN_ExtremeGrant (IM3_SDN_AI) is proposed for threat detection in Software Defined Networking (SDN)-based autonomous vehicle (AV) networks. In today’s age of digital transformation, machine learning, deep learning, natural language processing, computer vision, and speech processing have revolutionized hardware, software, services, and applications to a large extent [12]. The strengths of artificial intelligence (AI) are combined with the combined skills, intelligence, and powerful cognitive execution with extensive capabilities of human being where AI helps a human to accomplish task work efficiently [16]. The same concept is deployed into the unknown dangerous, connected, and complex operations of SDN networks for AV networks to get an intelligent model IM3_SDN_AI. The working and empirical validation of the proposed model outside of real-world and practical driving automotive units have been evaluated through state-of-the-art simulators where an overall mean increase of 29.32% is observed for detection scenarios for each attack.

4.1. Importance of Threat Detection

Software security of an autonomous car has advanced dramatically with updates; however, hardware security, e.g., cameras, sensors, and engines are more susceptible to adversarial attacks today than ever before. Threat models used to generate adversarial perturbations in an autonomous system often assume that the attacker has full access to the training data and to the prediction model, which is not a good model for hardware or physical attacks. Although some adversarial attacks can deceive the system by changing pixels on road signs or stop lights, the generative mechanism of the adversarial perturbations is not necessarily applicable to the aforementioned pixel changes. That is, an attacker seeking to cause a physical attack is restricted to output perturbations without access to the internal parameter of the model, i.e., the pixels of elements that are not correlated to the sensed data. Further, manipulation of double lens cameras does not require bad intent and the threat could be an artifact of optometry examinations [18].

Threat detection has become of growing importance [19] to society as information is becoming increasingly valuable and dangerous. Understanding potential threats in information systems can help to mitigate their impact. Autonomous cars are examples where a human-in-the-loop threat detection mechanism cannot be realized, and the development of autonomous vehicles equipped for cyber as well as physical adversaries is pertinent [20]. As cars become more autonomous and ultimately driverless, there is an even greater emphasis on security.

4.2. Challenges in Traditional Detection Techniques

It is essential to enhance Worker Authentication Systems in automotive systems. Traditional detection techniques and behavioral biometric methods are the prevailing authentication means. Though these techniques authenticate a valid user account, they fail to address the situation when a user gets comporomised. In this case, the IN-Vehilce-Intrusion Detection System is required to monitor and prevent a user account from posing risk to the vehicle. These systems can prevent a user account from tampering electronic control units, power-train management modules, wireless communication modules and other on-board networks

[21]. There exist some techniques that rely on hidden cameras, microphones, sensors and several other traditional detective techniques to actively monitor driver's activities and surroundings. In some cases, these traditional techniques are efficient enough to authenticate the real-time, in-vehicle driver with non-compromized user account. Each time, respective hidden cameras and microphones record the driver's behaviour evidence and behaviour biometrics respectively (e.g., voice, face, iris, keystrokes, and driving paradigms). The challenge is to meliorate the driver's dynamic boundaries for multimodal authentication through embedded UNITS while keeping the operation costs minimum [22].

4.3. Proposed Hybrid Models

The Classification Reframed Generative Adversarial Network (GAN-CAN) is designed, which crafts impairments and attackors effectively for GBDrID models to generate fraudulent deepfakes and vulnerability masks. The proposed attacker explores offensive and defensive advantages for the stepwise adversarial liveness detection attack on learner and privacy-preserving methods. Generated adversarial sensors and privacy masks preserve the trajectory continuity and personal information privacy of closely approximate subjects, respectively. The personified behavioral condition generator imitates the authentic driving style of a given new sample's label condition for all initial-learner targets, from a fleet of unobserved synthesized deepfake clustering participants. Evasion attacks based on negative affect detection are demonstrated to be effective by concerning Copenhagen and Aachen. [22]

Biometric authentication-based driver identification solutions, are substitute for traditional cryptographic protocols for secure multifactor authentication in recently developed autonomous vehicle systems. Although biometric authentication has added value to the secure and convenient authentication of legitimate users, it brings unintentional and purposeful security and safety hazards and vulnerabilities as well. General behavior-based driver identification (GBDrID) techniques provide a best fusion and yolov3-based recommendation for evading these vulnerabilities. The binary classification ....in these models, it has been observed that marginal and major road users face unauthorized and intentional fraudulent access to a fixed-lane vehicle as well as social dilemma situations, respectively, owing to reckless, and cautious driving cues of drowsy and drunk drivers. An advanced conditional generative adversarial network (GAN-

CAN) in a data-starvation environment to demonstrate the vulnerabilities of GBDrID schemes toward permutation attacks.

5. Conclusion

Market-oriented societies must value AV technologies and work for social common public interest. Ethics is inevitable in any consumption of products and services, and AV technologies is no exception. The car has been in the subjectivity of liberal social orders, and when an AV makes an ethical decision that prioritizes one party or one of two parties, according to its tracking of the automotive norms, it may lose the autonomy and trust in it, by appearing ethical and unacceptable. This is not to deny the importance of the technical feasibility of ethical design and its reliable development and programming, but rather to argue that the ethical decision made by the AV follows the current norms of the automotive world to look ethically moved and accepted. When the private agency with advanced AV technology interacts with human beings and the common public use, this backwash may act as a sandbag to flood the whole society with its unfinished ethical behaviors [12]. The other and most important ethical dilemma is on the part of the developer of the transport robots code, because they should follow a pattern of ethical principles among them to avoid ethical insufficiency. Ethical insufficiency is a code for which many ethical problems can be deduced and thereby can be declared as an unethical code. Therefore, new ethical codes are needed in the course of the development an AV for ethical completeness.

Drivers have to be prepared to take over control from autonomous vehicles (AVs) at any time. They also have to pay attention and monitor the operation of the system during periods of being responsible, which must surely be unengaging and boring. Monitoring the automation process closely may lead to an attention deficit in case the driver has to take control when driving again. A costly and delayed offloading of control could arise from a perceived inability and reluctance to disengage from non-driving tasks and initiate a takeover maneuver when required [23]. The AV hardware will give continuous monitoring of the condition of the driver including visual tracking of the drivers' eyes, monitoring the present glance path taken by the rim of the eyes, and measuring the size of the eyelids. These features can be associated and correlated with contemporary computer games and do not distract the driver and this avoids data privacy and surveillance issues.

5.1. Summary of Findings

[24], [12]In a practical application, biometric authentication procedure replaces the reliance on passwords which are increasingly considered to be outdated in terms of security and user-friendliness issues. Biometric systems bind authentication to the characteristics inherent to individuals, enhance security, and provide a better user experience. Autonomous vehicle systems are envisioned to operate in various configurations: individual humans and other vehicles can be passengers or road users, with crowd behavior and on-road human drivers adding to the systems' complexity. %So AV systems development needs to keep in mind the physical, psychological, and cultural characteristics of humans. The collaboration between humans and autonomous systems needs from each part to adapt to the other, so that the risk of accidents is effectively diminished. Our work aims at integrating a human-awareness system to address the mentioned issues. The goal is to help the rapid advance of overall safe autonomous vehicle operation in human environments through effective sharing of knowledge on issues related to detection, recognition, interpretation, prediction, and decision support for pedestrian behavior and human-aware driver-assistance systems during driving.[3] Since modern vehicles come with the latest technology and different sensors, the future of cars will be one hundred per cent autonomous. The shift from manual driving to autonomous driving will increase the issue of road safety and other ethical concerns related to this shift from manual driving to autonomous driving. This specific concern of this thesis came up when two Uber engineers were killed in March 2018 when the self-driving car they were testing in Arizona hit a pedestrian. The real problem was that The Volvo self-driving car did not stop due to a fault in the software. There was no driver to take control of the car. That's why the car did not stop itself – it relied too much on the Volvo's technology. This incident of physical failure raises various ethical questions that developers, stakeholders and legislators need to consider before they deploy self-driving technology on the streets.

5.2. Future Research Directions

Furthermore, this study has drawn from empirical data in the sections on "ethics", "design science research method", and, to a lesser degree, on "sustainable development". By focusing on every element of ethical reasoning using criteria to solve problems, Rasmussen and Kim [25] have addressed why empirical data is significant for technoethics. It is worth mentioning that the study's "ethics" and "design science" prospectuses majorly indicated the theoretical exploration of the controversies and issues linked with the subject matter of 'ethical' methodologies. It surely is becoming difficult to rely on ethical perspectives that are theoretically thought to be perfect. This kind of research with an empirical single-growth approach can only induce creative thinking for data analysis. Ethics-wise, the link between culture and privacy in biometric authentication on autonomous and Intelligent Vehicles' interactions still needs to be scrutinized more, in order to design reasonable and judicious biometric authentication systems for novel societies.

[16]This thesis has only begun to scratch the surface of the ethical issues that surface when integrating biometric authentication features into the management of Intelligent and autonomous Vehicles (IAVs). As was evident throughout, autonomous driving functionalities have an important bearing on the well-being, safety and ecosystems of society. While much has been discussed in this dissertation, a number of potential opportunities for further research remain. For instance, ethical reflections on BIASs may be focused, on the one hand, on uncovering and addressing the specific risks of BIASs in the context of IAVs, or, on the other hand, on identifying any general risks of IAVs as filtered through the prism of the study's module of BIAS. The latter may get generously substantiated when examined in the context of recent debates on "empirical ethics" within the fields of technoethics as well as sustainable technology.

6. References

1. [1] L. V. Bonfati, J. J. A. Mendes Junior, H. Valadares Siqueira, and S. L. Stevan, "Correlation Analysis of In-Vehicle Sensors Data and Driver Signals in Identifying Driving and Driver Behaviors," 2022. ncbi.nlm.nih.gov
2. [2] S. Paiva, M. Abdul Ahad, G. Tripathi, N. Feroz et al., "Enabling Technologies for Urban Smart Mobility: Recent Trends, Opportunities and Challenges," 2021. ncbi.nlm.nih.gov
3. [3] A. Shah, "Adversary ML Resilience in Autonomous Driving Through Human Centered Perception Mechanisms," 2023. [PDF]
4. Tatineni, Sumanth. "Beyond Accuracy: Understanding Model Performance on SQuAD 2.0 Challenges." *International Journal of Advanced Research in Engineering and Technology (IJARET)* 10.1 (2019): 566-581.
5. Vemoori, V. "Towards Secure and Trustworthy Autonomous Vehicles: Leveraging Distributed Ledger Technology for Secure Communication and Exploring Explainable

Artificial Intelligence for Robust Decision-Making and Comprehensive Testing". *Journal of Science & Technology*, vol. 1, no. 1, Nov. 2020, pp. 130-7, https://thesciencebrigade.com/jst/article/view/224.

6. Mahammad Shaik. "Reimagining Digital Identity: A Comparative Analysis of Advanced Identity Access Management (IAM) Frameworks Leveraging Blockchain Technology for Enhanced Security, Decentralized Authentication, and Trust-Centric Ecosystems". Distributed Learning and Broad Applications in Scientific Research, vol. 4, June 2018, pp. 1-22, https://dlabi.org/index.php/journal/article/view/2.
7. Vemori, Vamsi. "Towards Safe and Equitable Autonomous Mobility: A Multi-Layered Framework Integrating Advanced Safety Protocols, Data-Informed Road Infrastructure, and Explainable AI for Transparent Decision-Making in Self-Driving Vehicles." *Human-Computer Interaction Perspectives* 2.2 (2022): 10-41.
8. [8] A. Bastola, J. Brinkley, H. Wang, and A. Razi, "Driving Towards Inclusion: Revisiting In-Vehicle Interaction in Autonomous Vehicles," 2024. [PDF]
9. [9] J. Yeboah, V. Adewopo, S. Azumah, and I. Okpala, "Evaluation of User Perception on Biometric Fingerprint System," 2022. [PDF]
10. [10] P. Cornelio, P. Haggard, K. Hornbaek, O. Georgiou et al., "The sense of agency in emerging technologies for human–computer integration: A review," 2022. ncbi.nlm.nih.gov
11. [11] S. H. Katsanis, P. Claes, M. Doerr, R. Cook-Deegan et al., "U.S. Adult Perspectives on Facial Images, DNA, and Other Biometrics," 2021. ncbi.nlm.nih.gov
12. [12] L. Chen, Y. Li, C. Huang, Y. Xing et al., "Milestones in Autonomous Driving and Intelligent Vehicles Part I: Control, Computing System Design, Communication, HD Map, Testing, and Human Behaviors," 2023. [PDF]
13. [13] A. McStay and L. Urquhart, "In Cars (Are We Really Safest of All?): Interior Sensing and Emotional Opacity," 2021. osf.io
14. [14] R. Alrawili, A. Abdullah S. AlQahtani, and M. Khurram Khan, "Comprehensive Survey: Biometric User Authentication Application, Evaluation, and Discussion," 2023. [PDF]
15. [15] C. Xie, Z. Cao, Y. Long, D. Yang et al., "Privacy of Autonomous Vehicles: Risks, Protection Methods, and Future Directions," 2022. [PDF]
16. [16] M. Aminul Islam and S. Alqahtani, "Autonomous Vehicles an overview on system, cyber security, risks, issues, and a way forward," 2023. [PDF]

17. [17] S. Günther, G. Rein, and C. Straub, "A Birman-Schwinger Principle in General Relativity: Linearly Stable Shells of Collisionless Matter Surrounding a Black Hole," 2022. [PDF]
18. [18] Y. Shao, S. Weerdenburg, J. Seifert, H. Paul Urbach et al., "Wavelength-multiplexed Multi-mode EUV Reflection Ptychography based on Automatic-Differentiation," 2023. [PDF]
19. [19] A. Kashevnik, A. Ponomarev, N. Shilov, and A. Chechulin, "Threats Detection during Human-Computer Interaction in Driver Monitoring Systems," 2022. ncbi.nlm.nih.gov
20. [20] S. M Mostaq Hossain, S. Banik, T. Banik, and A. Md Shibli, "Survey on Security Attacks in Connected and Autonomous Vehicular Systems," 2023. [PDF]
21. [21] P. Xiong, S. Buffett, S. Iqbal, P. Lamontagne et al., "Towards a Robust and Trustworthy Machine Learning System Development: An Engineering Perspective," 2021. [PDF]
22. [22] E. Efatinasab, F. Marchiori, D. Donadel, A. Brighente et al., "GAN-CAN: A Novel Attack to Behavior-Based Driver Authentication Systems," 2023. [PDF]
23. [23] V. V. Dixit, S. Chand, and D. J. Nair, "Autonomous Vehicles: Disengagements, Accidents and Reaction Times," 2016. ncbi.nlm.nih.gov
24. [24] M. Hernandez-de-Menendez, R. Morales-Menendez, C. A. Escobar, and J. Arinez, "Biometric applications in education," 2021. ncbi.nlm.nih.gov
25. [25] A. Kriebitz, R. Max, and C. Lütge, "The German Act on Autonomous Driving: Why Ethics Still Matters," 2022. ncbi.nlm.nih.gov