Autonomous Vehicle Safety, Security, and Energy Management: A Review, Challenges, and Solutions

Onu Peter and Charles Mbohwa
Department of Quality and Operations Management
Faculty of Engineering and the Built Environment,
University of Johannesburg, P. O. Box 524,
Johannesburg, South Africa.
onup@uj.ac.za

Abstract

This study presents a comprehensive analysis of the challenges and opportunities associated with safety, security, and energy management in the context of autonomous vehicles. It begins by providing an overview of these key aspects and their significance in the domain of autonomous vehicles. A thorough literature review encompassing the current research in these areas was then conducted. Various studies, advancements, and approaches have been explored to address the complex concerns of ensuring autonomous vehicles' safety, security, and efficient energy management. This study delves into the barriers that impede progress in each domain and proposes potential solutions. Safety challenges include the development of robust collision-avoidance systems and emergency response mechanisms. Security challenges involve safeguarding against cyber threats and unauthorized access. Energy management challenges focus on optimizing the power usage and integrating renewable energy sources for sustainability. Opportunities within these domains have also been identified, such as advancements in sensor technologies and the implementation of intelligent energy management systems. Policy and regulatory priorities are outlined, highlighting the need to address data privacy, establish AI and machine learning usage guidelines, protect public infrastructure, manage workforce transitions, and address the impact of emerging technologies. This study offers valuable insights into the challenges, solutions, and policy considerations related to autonomous vehicles' safety, security, and energy management. The aim was to support the successful integration of autonomous vehicles into transportation systems by addressing critical aspects and ensuring their safe and sustainable adoption.

Keywords
Autonomous vehicle safety, Security, Energy Management, Policy, and Regulatory Priorities

1. Introduction

Autonomous vehicles (AV) are becoming increasingly prevalent and affect transportation, safety, security, and energy management considerably. AVs are enabled by technologies that allow them to operate without human input. According to SAE J3016 (SAE 2018), a standard used in the automotive industry, categorizes self-driving vehicles into six levels of autonomy, ranging from level 0 (no self-driving features) to level 5 (fully autonomous driving). AV differs from conventional cars in that they have more sensors to detect their environment, the computer takes over steering control, and they can communicate with other vehicles, infrastructure, and pedestrians through V2X technology (where X represents other vehicles, infrastructure, pedestrians, etc.) (Weiß 2011). This type of technology helps improve efficiency and reduce costs, enhance safety, and reduce the risk of accidents (Onu and Mbohwa 2021). By relying on this technology, AVs can drive more efficiently, providing a better and safer experience for everyone involved. Additionally, AVs have the potential to enhance the efficiency of the transportation system through their ability to perceive and respond to the environment more quickly, leading to the ability to maintain smaller distances between vehicles and thereby increasing road capacity (Shi and Prevedouros 2016). The sensors on an AV, such as radar, camera, and Light Detection and Ranging (LiDAR) technology, play a crucial role in detecting the vehicle's movements and surrounding environment.

These sensors help determine the vehicle's location, speed, distance to nearby cars, road conditions, and traffic signs (Zhang et al. 2014). However, if the AV experiences any failures or attacks can affect other connected vehicles through the VANET (Vehicular Ad Hoc Network). VANET is a network created by communication between vehicles and infrastructure, allowing for information sharing between connected vehicles and roadways. The Intelligent Transportation System (ITS) framework considers VANETs as a key component, as the shared data from these networks are used to improve traffic management and enhance mobility, efficiency, and safety (Eze et al. 2016). The advancement of AVs presents a multifaceted challenge for researchers, regulators, and manufacturers. To effectively navigate this challenge, they must continually assess public perception and stay updated on the latest developments. Moreover, they must consider the possible consequences of implementing AVs on a large scale, such as potential job loss and increasing urban traffic congestion. They must also ensure that the technology is safe and reliable before it is available to the public (Onu et al. 2023a). Studies have shown that scholars have predominantly focused their research on AVs' safety and security aspects, while few publications exist on their energy management. The implementation of AVs also presents numerous policy and planning considerations that must be considered and addressed. This paper aims to provide a comprehensive overview of the safety, security, and energy management issues associated with Avs. It will review the existing AV safety, security, and energy management literature. It explores potential challenges and solutions to address them. Additionally, it discusses the policy and regulatory priorities that need to be considered. Furthermore, the paper identifies research gaps and outlines possible future directions for research in AVs.

2. State of the Art: Vehicle Safety, Security and Energy Management

This review summarizes noteworthy literature on Autonomous vehicle safety, security, and energy management involve using technologies, strategies, and regulations to ensure that AVs are safe and secure while also optimizing the vehicle's energy efficiency. Autonomous vehicle safety consists of using advanced sensors, artificial intelligence, and machine learning to detect and react to external stimuli. Autonomous vehicle security consists of encryption, authentication, and authorization protocols to protect the vehicle and its data from unauthorized access. AVs pose unique security and safety risks due to their complexity. Suppose one component of an AV malfunctions or is compromised. In that case, it can potentially expose the on-board computer, or "brain" of the vehicle, to the risk of issuing the wrong command and jeopardizing traffic safety.

2.1 Autonomous Vehicle Safety

Autonomous vehicle safety involves using advanced sensors, artificial intelligence, and machine learning to detect and react to external stimuli. This includes detecting other vehicles, pedestrians, and objects in the environment, as well as the ability to accurately interpret and respond to changing road conditions. Autonomous vehicle safety also involves simulation and testing to ensure the accuracy of the vehicle's decision-making and navigation systems (Cui and Sabaliauskaite 2019). Additionally, autonomous vehicle safety requires the development of algorithms and protocols to detect and respond to potential hazards and the development of regulations and standards to ensure the safety of AVs (Weiß 2011). The influence of AVs on pedestrian safety must still be explored and measured, taking into account the unique characteristics of AV-pedestrian interactions and the situational context (Fayish and Gross 2010). Indicators such as time-to-collision (TTC) and post-encroachment time (PET) have been widely used in numerous safety applications in the literature to evaluate the severity of traffic conflicts (Stipancic et al. 2021; Zhang et al. 2019).

2.2 Autonomous Vehicle Security

The communication systems utilized by AVs are susceptible to a range of attacks that have the potential to degrade road network performance, alter ITS decisions, or cause damage to infrastructure (Abdallah et al. 2017). As these attacks are becoming increasingly sophisticated, their detection becomes more difficult. Given the expected vast size of future AV networks, adopting a cutting-edge communication design that can accurately verify and disseminate authentic traffic information across the entire network is necessary. Security goals are frequently met using cryptography-enabled control mechanisms involving key generation and management (Chattopadhyay et al. 2021; Karnouskos and Kerschbaum 2018). Securing AV networks using traditional centralized security protocols is challenging due to a large number of frequently changing vehicular parameters. As a result, decentralized trust models that verify information critical to AV network functionality, such as traffic congestion control and accident warnings, are becoming more prevalent (Nanda et al. 2019). Conventional centralized security methods are further limited by the instability of AVs, making them inadequate for providing sufficient flexibility and mobility support. Recently, several studies have explored the implementation of secure authentication methods (Changalvala and Malik 2019; Onu and Mbohwa 2021; Zhao et al. 2021) and trusted certificates, as well as resource testing-based strategies (Abdulkader et al. 2018), to prevent the transmission of false data from malicious entities, thus mitigating the risk of false data infusion, Sybil attacks, Collusion attacks, etc.

2.3 Autonomous Vehicle Energy Management

Autonomous vehicle energy management involves using predictive algorithms, energy optimization strategies, and charging technologies to reduce power consumption and maximize battery life (Sarvaiya et al. 2021). This includes the use of algorithms to optimize the vehicle's powertrain and the use of charging technologies to ensure that the vehicle has enough energy to complete its tasks. Autonomous vehicle energy management requires the development of algorithms and protocols to detect and respond to potential energy management issues and the development of regulations and standards to ensure the efficient use of energy by AVs (Saiteja and Ashok 2022). Overall, implementing practical solutions for energy management strategies (EMS) poses several challenges, such as collecting and analyzing data from various sources, anticipating the energy needs of vehicles in both space and time and understanding the features and capabilities of vehicle control systems. Energy management strategies must also be able to anticipate and respond to changes in the environment, such as weather conditions, traffic flow, and road infrastructure, including improving the mechanical efficiency of the motor, adjusting the electric control voltage level, and enhancing the transmission's thermal efficiency, which can significantly improve the energy-saving potential of AVs (Peter and Mbohwa 2019).

3. Challenges and Opportunities

3.1 Safety Challenges and Solutions in AVs

The potential threats to AVs and road users can be classified into two categories: (1) failures related to AV components (VF) and (2) failures related to infrastructure (IF) (Aoude et al. 2012; Bhavsar et al. 2017). The VF category encompasses various types of failures, including hardware system failures (such as integration platforms, sensors, actuators, and controller failures), software failures, vehicle mechanical failures, communication system failures (such as V2X and in-vehicle communication systems), and failures that could compromise the safety of other road users. These failures can negatively impact the performance of the AV. Software failures are software errors or bugs in the vehicle (Keller et al. 2011); Communication system failure, involving the failure of communication between the vehicle and its environment; and interaction system failure involve incorrect or unreliable input from the driver, failure of the vehicle's display systems, or incorrect feedback from the vehicle's autonomous system (Edirisinghe et al. 2015); Pedestrians and other road users, such as bicyclists, motorcycles, and other vehicles, can also present unexpected obstacles or changes to the road environment (Tao et al. 2019). AVs must respond accurately to these road users to ensure safe and reliable operation. Solutions to the failures related to AV components must combine multi-sensor fusion and runtime monitoring to enhance information accuracy and prevent hardware and software failures (Chitnis et al. 2017). Notably, a driver's behavior can significantly impact an AV's energy consumption, as different driving styles can result in varying energy use even under similar driving conditions.

3.2 Security Challenges and Mitigation Strategies in AV

The primary security requirements for AVs, vehicular ad hoc networks (VANETs), and intelligent transportation systems (ITS) are the protection of data and assets exchanged between vehicles, vehicles, and the infrastructure, and vehicles and cloud services. This includes authentication, non-repudiation, integrity, and confidentiality/privacy as follows (Jan et al. 2021; Manvi and Tangade 2017): Verification of identity, source, and location, Immediate availability of information. Protecting the trust and integrity of data and ensuring privacy and confidentiality. In addressing security challenges, it is important to consider various factors such as authentication, non-repudiation, integrity, and confidentiality/privacy. Strong methods such as biometric and multi-factor authentication can be implemented to ensure that only authorized users have access to the vehicle (Zhu et al. 2014). Non-repudiation can be achieved through digital signatures and hashing, allowing for the detection of any tampering or modification of data transmitted between the vehicle and other systems. Data integrity checks and error detection/correction algorithms can be used to maintain data integrity and control systems, along with secure communication protocols such as HTTPS and SSL. Encryption technologies such as AES and TLS can be employed to protect sensitive data, along with strict access controls and data minimization practices (Liu et al. 2019).

3.3 Management Challenges and Amelioration in AVs

Autonomous vehicle energy management involves using predictive algorithms, energy optimization strategies, and charging technologies to reduce power consumption and maximize battery life (Manne et al. 2021; Phan et al. 2021). However, several challenges must be addressed to ensure the efficient use of energy by AVs. These challenges include the accurate prediction of energy usage, the precise interpretation of energy optimization strategies, and the development of protocols to detect and respond to potential energy management issues. Additionally, there are challenges related to AVs' efficient use of energy. Group vehicles' repeated acceleration and slowing down consume more energy and limit driver comfort and road safety. At the same time, the limitations of the battery, such as the maximum state of charge and charging power, must also be considered. The battery's condition, including the state of charge, energy, health, and temperature, is critical in this system and can affect the system's performance (Sarvaiya et al. 2021; Seo et al. 2021). Batteries in AV can become unusable when they reach 20% capacity due to aging (Temporelli et al. 2020). This can impact the performance of the Energy Management System (EMS). To ensure the optimal energy efficiency of AVs, it is essential to establish comprehensive solutions that can collect and analyze various data from different sources, predict power requirements in other regions and times of the journey, and identify the capabilities of vehicle control systems. This data can then be used to determine the vehicle's energy requirements in each part of the journey, as well as provide insights into the best driving strategies and control systems to optimize energy efficiency for AVs.

3.4 Benefits of a Safe, Secure, and Energy-Efficient AV

AVs can recognize and react to potential hazards, such as other vehicles, pedestrians, and obstacles, in real-time thanks to sensors, cameras, and sophisticated algorithms. Significantly, this higher level of safety will save lives and lower the financial costs of traffic accidents, such as lost productivity, medical expenses, and property damage (Onu et al., 2023b). Moreover, using data from vehicles can also help improve the accuracy of claims by providing a more detailed and comprehensive view of the circumstances surrounding an accident. This can lead to more accurate claims assessments, resulting in fairer compensation for policyholders and reduced disputes between insurance companies and policyholders. The use of AVs has the potential to increase energy efficiency and lower greenhouse gas emissions, as well as fuel consumption (hybrid-electric vehicles) (Li et al. 2022). AVs can lessen traffic congestion and unnecessary driving by optimizing speed, route, and traffic patterns. The energy efficiency of AVs can also be increased by incorporating energy-saving technologies into their design, such as electric motors, regenerative braking, and aerodynamics. Additionally, AVs can potentially create new opportunities for people with disabilities to have access to transportation and open up the opportunity for more people to participate in the economy as mobility is no longer a barrier as they no longer need to worry about the burden of driving and can instead focus on their other needs. This opens up several possibilities, not only in terms of transforming the driving systems but also in terms of improving the overall efficiency of our transportation systems and helping to reduce air pollution associated with traditional transportation methods (Onu and Mbohwa 2019; Peter et al. 2023).

4. Policy and Regulatory Priorities for Autonomous Vehicle

The following are some crucial policy factors that our study considers tenable for developing the rules and policies for using AVs. We have not attempted to address the subject of legal obligations and insurance regulations. Nonetheless, as safety standards for AVs can vary from country to country, some common standards are widely recognized as being necessary for the safe operation of these vehicles (shown in Table 1). The study suggests policies and regulations meet safety, security, data privacy, energy efficiency, use of advanced computer capabilities (e.g., AI and ML), protection of public infrastructure, a displaced workforce, and the impact of the development of new technologies to ensure the safety, convenience, and affordability of AVs. In conclusion, establishing guidelines for AVs is essential for securing their safety, efficiency, and overall security. Considering these regulations in future legislation, including pilot testing, is imperative. These regulations will play a significant role in shaping the future of AVs, promoting their responsible and sustainable growth.

Table 1. Mitigating Autonomous Vehicles Security Risks: Strategies, Approaches, and Implications

Challenges	**Policy measures**	**Regulatory priorities**	**Opportunities**
Safety	Crash-worthiness	To design vehicles to protect passengers and other road users in an accident.	It will ensure that the vehicles are equipped with advanced safety systems, such as airbags and crumple zones, to absorb the impact of a collision.
	Emergency Response Systems	To design vehicles with backup systems and technologies that can respond in the event of a failure of the primary systems.	It will ensure that the vehicle system includes backup power systems, redundant communication systems, and manual

			controls that a human operator in an emergency can use.
	Obstacle Detection and Response	Design vehicles with sensors and cameras that can detect obstacles and respond appropriately to avoid collisions.	Will ensure that the vehicle system includes features such as lane departure warning systems, automatic emergency braking, and pedestrian detection systems.
	Human Factors	To design vehicles so that they are safe and easy to use for all users, including those with disabilities.	It will ensure that the vehicles are equipped with user-friendly interfaces and accessible to all users, regardless of their physical abilities.
Security	Cybersecurity	To design vehicles to be secure against hacking and other forms of cyber-attacks.	It will ensure that the vehicles are equipped with secure communication, data storage, and cybersecurity measures to prevent unauthorized access to the vehicle's systems.
	Physical security	Design a vehicle to protect against physical threats, such as theft or tampering (e.g., tamper-proofing the vehicle's electronic systems and implementing secure keyless entry systems).	It will ensure that the vehicle system is secure and can be used by a human operator in an emergency.
	Network security	AVs must meet the minimum security of the network to ensure the safety of the cars and their passengers.	It will prevent hacking and other malicious attacks, including danger to passengers.
	Incident response	To design vehicles equipped with robust incident response systems to handle accidents, malfunctions, and other events.	Will promote performance criteria for safety-critical systems.
Energy Efficiency	Fuel Efficiency Standards	AVs must meet minimum fuel efficiency or a minimum electric car range standard.	This will encourage the development of more fuel-efficient vehicles with lower emissions.
	Emissions Standards	AVs must meet minimum emissions standards.	It will reduce the environmental impact of AVs and promote sustainable transportation.
	Renewable Energy Use	AVs must incorporate renewable energy sources to power their systems and recharge their batteries.	This will reduce the environmental impact of AVs and promote sustainable transportation.
	Energy-Efficient Technologies	AVs must incorporate energy-efficient technologies like regenerative braking systems and energy-efficient motors.	It will improve energy efficiency and can serve to promote the use of sustainable transportation and reduce the environmental impact of AVs.
Data Privacy	Data Security	Data generated by AVs must be secured using encryption and other security measures.	This will prevent unauthorized access to the data and ensure it is not used maliciously.
	Data Privacy	Data generated by AVs must be kept private and not shared with third parties without the consent of the vehicle owner or user.	It will protect the privacy of the data and ensure that it is not used for purposes, not in the public interest.
	Data Use	Data generated by AVs must be used for purposes that are in the public interest. E.g., traffic management, road safety, and environmental monitoring.	This will ensure that the data is used to benefit the public.
	Data Access	Data generated by AVs is to be accessible to government agencies and other organizations that need it for purposes that are in the public interest.	It will ensure data accessibility to law enforcement agencies investigating accidents or crimes.

Use of advanced computer capabilities	Potential for bias and discrimination	Ensure that data used to train AI and ML systems is diverse, representative, and discrimination-free.	This will prevent data constraints and biases.
	Transparency and accountability	To ensure that the AI and ML systems are designed to be transparent and auditable.	It will ensure data accessibility to law enforcement agencies investigating accidents or crimes.
	Reliability and safety	To ensure vehicles are designed with security in mind and that the technical requirements, as per testing and validation protocols, are reliable and safe.	It will prevent hacking and other malicious attacks.
Protection of Public Infrastructure	Optimization of existing infrastructure	To ensure that road networks and transportation systems are designed to accommodate the safe integration of the unique needs of AVs, such as dedicated lanes and specialized signage, etc.	Will promote performance criteria for safety-critical systems.
	Design, construction, and operation	To support existing transportation systems, such as public transit, to maximize the efficiency of these systems, including the data they generate.	It will ensure the resilience of AV systems with existing road networks and protect against hacking and cyber threats.
Worker's transition or displaced workforce	Retraining programs	To provide retraining programs for workers with the skills and knowledge required to transition to new roles or industries, such as those related to AV technology or maintenance.	It will ensure that deploying AVs is a responsible and sustainable process.
	Unemployment benefits and forms of support	To provide unemployment insurance and job search assistance to workers who lose their jobs due to the deployment of AVs. These may include wage subsidies, tax credits, and other financial incentives for workers transitioning to new roles or industries.	It will provide financial support to help workers during the transition period and helps to mitigate the economic impact of job loss. And encourage workers who complete retraining programs and transition to new ones.
Development of new technologies	New versus existing technology systems	To ensure the growth, coexistence, and protection of industries that support the deployment of these vehicles.	Will expand new business opportunities for companies involved in developing charging networks, battery manufacturing, and other related industries.

5. Research Gaps and Future Research Directions

The development and deployment of AVs present numerous challenges and opportunities. To ensure AVs' safety, security, and efficiency, it is important to understand the current challenges and opportunities related to safety, security, and energy management. This paper has reviewed the current literature on AV safety, security, and energy management and discussed the policy and planning priorities that must be considered. Going forward, further research is needed to conduct an in-depth assessment of the challenges and opportunities identified in this paper and develop the policy and regulatory framework necessary to ensure AVs' safe and efficient deployment. Street detection, a crucial aspect of autonomous vehicles, is achieved through various sensors, such as cameras and LIDARs. Each sensor has its own set of requirements, and combining different sensors can compromise the strengths of each.

One of the primary challenges self-driving vehicles faces is accurately determining their location, which can be improved by integrating data from GPS, gyroscopes, speed sensors, accelerometers, and other similar devices. Furthermore, it is possible to identify external deterrents with reasonable accuracy using deep learning. Numerous researchers have conducted some studies using PC vision and autonomous intelligent vehicle object recognition; however, these studies findings are not publicly available.

The challenges associated with collecting data must be considered when training a network to forecast traffic flow. This is particularly true for vehicles traveling at very slow or high speeds and situations where roads may be empty during the forecast period. These difficulties are often not addressed in studies, leading to incomplete and corrupted data. To overcome these issues, it is necessary to implement a sophisticated method of measuring forecasting errors. Most studies rely on loop detectors and sensors to collect data on traffic flow (Kim and Coifman 2017).
However, owing to nascent technologies, GPS-based systems offer a more comprehensive and dynamic picture of traffic flow due to their high-dimensional, non-linear, and spatial-temporal features. Additionally, GPS technology has a low cost of installation compared to other data sources, making it an attractive option for analysis. Moreover, those onboard AVs must maintain communication with the vehicle. Further research examining the interaction between humans and AVs in mixed-traffic scenarios is imperative.

6. Conclusions

This paper comprehensively reviews the current literature on autonomous vehicle (AV) safety, security, and energy management. It gives an overview of the strategies involved and highlights the policy and planning considerations that must be considered. The review identifies the challenges and opportunities related to improving AVs' safety, security, and energy efficiency. The authors also discuss the need to address several key policy and planning considerations, such as data privacy, the use of AI and ML in AVs, the protection of public infrastructure, the transition of workers, and the impact of new technological advancements. The paper comprehensively examines Autonomous Vehicle Safety, Security, and Energy Management: A Review, Challenges, and Solutions.

References

Abdallah, E. G., Zulkernine, M., Gu, Y. X., & Liem, C., Towards defending connected vehicles against attacks. *ACM International Conference Proceeding Series*, 2017, https://doi.org/10.1145/3123779.3123794.

Abdulkader, Z. A., Abdullah, A., Abdullah, M. T., & Zukarnain, Z. A., A survey on sybil attack detection in vehicular ad hoc networks (VANET). *Journal of Computers (Taiwan)*, 2018, https://doi.org/10.3966/199115992018042902001.

Aoude, G. S., Desaraju, V. R., Stephens, L. H., & How, J. P., Driver behavior classification at intersections and validation on large naturalistic data set. *IEEE Transactions on Intelligent Transportation Systems*, 2012, https://doi.org/10.1109/TITS.2011.2179537.

Bhavsar, P., Das, P., Paugh, M., Dey, K., & Chowdhury, M., Risk analysis of autonomous vehicles in mixed traffic streams. *Transportation Research Record*, 2017, https://doi.org/10.3141/2625-06.

Changalvala, R., & Malik, H., LiDAR Data Integrity Verification for Autonomous Vehicle Using 3D Data Hiding. *2019 IEEE Symposium Series on Computational Intelligence, SSCI, 2019*, https://doi.org/10.1109/SSCI44817.2019.9002737.

Chattopadhyay, A., Lam, K. Y., & Tavva, Y., Autonomous Vehicle: Security by Design. *IEEE Transactions on Intelligent Transportation Systems*, 2021, https://doi.org/10.1109/TITS.2020.3000797.

Chitnis, K., Mody, M., Swami, P., Sivaraj, R., Ghone, C., Biju, M. G., Narayanan, B., Dutt, Y., & Dubey, A., Enabling functional safety ASIL compliance for autonomous driving software systems. *IS and T International Symposium on Electronic Imaging Science and Technology*, 2017, https://doi.org/10.2352/ISSN.2470-1173.2017.19.AVM-017.

Cui, J., & Sabaliauskaite, G., US 2 : An unified safety and security analysis method for autonomous vehicles. *Advances in Intelligent Systems and Computing*, 2019, https://doi.org/10.1007/978-3-030-03402-3_42.

Edirisinghe, M., Dilhani, Y. H. N., & Kangara, K. M. J. C. B., Performance Capabilities and Detection Efficiency of Vehicle Backup Proximity Sensors for Narrow Objects. *International Letters of Chemistry, Physics and Astronomy*, 2015, https://doi.org/10.18052/www.scipress.com/ilcpa.52.134.

Eze, E. C., Zhang, S. J., Liu, E. J., & Eze, J. C., Advances in vehicular ad-hoc networks (VANETs): Challenges and road-map for future development. In *International Journal of Automation and Computing*, 2016, https://doi.org/10.1007/s11633-015-0913-y.

Fayish, A. C., & Gross, F., Safety effectiveness of leading pedestrian intervals evaluated by a before-after study with comparison groups. In *Transportation Research Record*, 2010, https://doi.org/10.3141/2198-03.

Jan, S. A., Amin, N. U., Othman, M., Ali, M., Umar, A. I., & Basir, A., A Survey on Privacy-Preserving Authentication Schemes in VANETs: Attacks, Challenges and Open Issues. *IEEE Access*, 2021, https://doi.org/10.1109/ACCESS.2021.3125521.

Karnouskos, S., & Kerschbaum, F., Privacy and integrity considerations in hyperconnected autonomous vehicles.

Proceedings of the IEEE, 2018, https://doi.org/10.1109/JPROC.2017.2725339.

Keller, C. G., Dang, T., Fritz, H., Joos, A., Rabe, C., & Gavrila, D. M., Active pedestrian safety by automatic braking and evasive steering. *IEEE Transactions on Intelligent Transportation Systems*, 2011, https://doi.org/10.1109/TITS.2011.2158424.

Kim, S., & Coifman, B., Assessing the performance of SpeedInfo radar traffic sensors. *Journal of Intelligent Transportation Systems: Technology, Planning, and Operations*, 2017, https://doi.org/10.1080/15472450.2016.1273779.

Li, J., Zhou, Q., He, Y., Williams, H., Xu, H., & Lu, G., Distributed Cooperative Energy Management System of Connected Hybrid Electric Vehicles With Personalized Non-Stationary Inference. *IEEE Transactions on Transportation Electrification*, 2022, https://doi.org/10.1109/TTE.2021.3127142.

Liu, J., Yu, Y., Jia, J., Wang, S., Fan, P., Wang, H., & Zhang, H., Lattice-based double-authentication-preventing ring signature for security and privacy in vehicular Ad-Hoc networks. *Tsinghua Science and Technology*, 2019, https://doi.org/10.26599/TST.2018.9010131.

Manne, S., Lydia, E. L., Pustokhina, I. V., Pustokhin, D. A., Parvathy, V. S., & Shankar, K., An intelligent energy management and traffic predictive model for autonomous vehicle systems. *Soft Computing*, 2021, https://doi.org/10.1007/s00500-021-05614-7.

Manvi, S. S., & Tangade, S., A survey on authentication schemes in VANETs for secured communication. In *Vehicular Communications*, 2017, https://doi.org/10.1016/j.vehcom.2017.02.001.

Nanda, A., Puthal, D., Rodrigues, J. J. P. C., & Kozlov, S. A., Internet of Autonomous Vehicles Communications Security: Overview, Issues, and Directions. *IEEE Wireless Communications*, 2019, https://doi.org/10.1109/MWC.2019.1800503.

Onu, P., & Mbohwa, C., Renewable Energy Technologies in Brief. *INTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH*, *8*(10), 1283–1289, 2019.

Onu, P., & Mbohwa, C., Industry 4.0 opportunities in manufacturing SMEs: Sustainability outlook. *Materials Today: Proceedings*, 2021, https://doi.org/10.1016/j.matpr.2020.12.095.

Onu, P., & Mbohwa, C., Reimagining the future: Techno innovation advancement in manufacturing. *Materials Today: Proceedings*, 2021, https://doi.org/10.1016/j.matpr.2020.12.100.

Onu, P., Pradhan, A., & Mbohwa, C., The potential of industry 4.0 for renewable energy and materials development – The case of multinational energy companies. *Heliyon*, 2023, https://doi.org/10.1016/j.heliyon.2023.e20547

Onu, P., Pradhan, A., & Mbohwa, C., Potential to use Metaverse for future teaching and learning. *Education and Information Technologies, Springer Nature*, 2023 https://doi.org/10.1007/s10639-023-12167-9

Peter, O., & Mbohwa, C., Industrial energy conservation initiative and prospect for sustainable manufacturing. *Procedia Manufacturing*, 2019, https://doi.org/10.1016/j.promfg.2019.05.077.

Peter, O., Pradhan, A., & Mbohwa, C., Industrial internet of things (IIoT): opportunities, challenges, and requirements in manufacturing businesses in emerging economies. *Procedia Computer Science*, *217*, 856–865, 2023, https://doi.org/10.1016/j.procs.2022.12.282.

Peter, O., Pradhan, A., & Mbohwa, C., Industry 4.0 concepts within the sub–Saharan African SME manufacturing sector. *Procedia Computer Science*, *217*, 846–855, 2023, https://doi.org/10.1016/j.procs.2022.12.281.

Phan, D., Bab-Hadiashar, A., Fayyazi, M., Hoseinnezhad, R., Jazar, R. N., & Khayyam, H., Interval Type 2 Fuzzy Logic Control for Energy Management of Hybrid Electric Autonomous Vehicles. *IEEE Transactions on Intelligent Vehicles*, 2021, https://doi.org/10.1109/TIV.2020.3011954.

Saiteja, P., & Ashok, B., Critical review on structural architecture, energy control strategies and development process towards optimal energy management in hybrid vehicles. In *Renewable and Sustainable Energy Reviews*, 2021, https://doi.org/10.1016/j.rser.2021.112038.

Sarvaiya, S., Ganesh, S., & Xu, B., Comparative analysis of hybrid vehicle energy management strategies with optimization of fuel economy and battery life. *Energy*, 2021, https://doi.org/10.1016/j.energy.2021.120604.

Seo, M., Song, Y., Kim, J., Paek, S. W., Kim, G. H., & Kim, S. W., Innovative lumped-battery model for state of charge estimation of lithium-ion batteries under various ambient temperatures. *Energy*, 2021, https://doi.org/10.1016/j.energy.2021.120301.

Shi, L., & Prevedouros, P., Autonomous and Connected Cars: HCM Estimates for Freeways with Various Market Penetration Rates. *Transportation Research Procedia*, 2016, https://doi.org/10.1016/j.trpro.2016.06.033.

Society of Automation Engineers (SAE)., J3016B Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles. In *SAE International*, 2018.

Stipancic, J., St-Aubin, P. G., Ledezma-Navarro, B., Labbe, A., Saunier, N., & Miranda-Moreno, L., Evaluating safety-influencing factors at stop-controlled intersections using automated video analysis. *Journal of Safety Research*, 2021, https://doi.org/10.1016/j.jsr.2021.03.006.

Tao, J., Li, Y., Wotawa, F., Felbinger, H., & Nica, M., On the industrial application of combinatorial testing for autonomous driving functions. *Proceedings - 2019 IEEE 12th International Conference on Software Testing, Verification and Validation Workshops, ICSTW,* 2019, https://doi.org/10.1109/ICSTW.2019.00058.

Temporelli, A., Carvalho, M. L., & Girardi, P., Life cycle assessment of electric vehicle batteries: An overview of recent literature, 2020, In *Energies*. https://doi.org/10.3390/en13112864.

Weiß, C., V2X communication in Europe - From research projects towards standardization and field testing of vehicle communication technology. *Computer Networks*, 2011, https://doi.org/10.1016/j.comnet.2011.03.016.

Zhang, C., Chen, F., & Wei, Y., Evaluation of pedestrian crossing behavior and safety at uncontrolled mid-block crosswalks with different numbers of lanes in China. *Accident Analysis and Prevention*, 2019, https://doi.org/10.1016/j.aap.2018.12.002.

Zhang, F., Clarke, D., & Knoll, A., Vehicle detection based on LiDAR and camera fusion. *17th IEEE International Conference on Intelligent Transportation Systems, ITSC,* 2014, https://doi.org/10.1109/ITSC.2014.6957925.

Zhao, C., Comert, G., & Pisu, P., Secure Connected and Automated Vehicles against False Data Injection Attack using Cloud-based Data Fusion. *IFAC-PapersOnLine*, 2021, https://doi.org/10.1016/j.ifacol.2021.11.243.

Zhu, X., Jiang, S., Wang, L., & Li, H., Efficient privacy-preserving authentication for vehicular Ad Hoc networks. *IEEE Transactions on Vehicular Technology*, 2014, https://doi.org/10.1109/TVT.2013.2294032.

Biographies

Peter Onu is a professional who is deeply interested in utilizing the Fourth Industrial Revolution to enhance productivity, improve quality assurance and manage risks associated with operations. His primary area of focus is in Operations Management studies, with a particular interest in Energy and Sustainability (E&S).

Charles Mbohwa is currently a Full Professor of Sustainability Engineering and Engineering Management at the University of Johannesburg, South Africa. Contacted at cmbohwa@uj.ac.za.