INSTITUTE FOR HOMELAND SECURITY


# Generative AI for Advanced Security Frameworks in Transportation Networks

**John Aliu**

# Generative AI for Advanced Security Frameworks in Transportation Networks

John Aliu

Clinical Assistant Professor, Engineering Education Transformations Institute, College of Engineering, University of Georgia, Athens, Georgia, USA; Email: john.aliu@uga.edu

ORCID: 0000-0001-5651-4009

**Abstract**

Artificial intelligence (AI) has revolutionized critical infrastructure sectors, enhancing efficiency, safety and decision-making. In transportation, AI has proven valuable in traffic management, autonomous vehicles and logistics optimization. However, as cybersecurity threats become more sophisticated, the integration of AI into transportation security frameworks remains underdeveloped. Generative AI, in particular, has not been fully utilized for threat detection, response and proactive measures. While traditional security measures are well-established, the use of generative AI for enhancing transportation security is still in its early stages and not yet widely adopted. This study aims to bridge this gap by investigating generative AI's role in strengthening transportation security frameworks. Through bibliometric analysis, the research identifies four key clusters where generative AI shows promise: (1) smart routing and traffic control, (2) traffic pattern simulation and prediction, (3) transportation cybersecurity and intelligence and (4) real-time decision support systems. The findings highlight the current state of AI applications in transportation security, revealing both progress and critical gaps. This study also provides actionable insights and practical recommendations for private industry professionals involved in the development, implementation and management of transportation security systems. By identifying the key clusters where generative AI can be most effectively applied, the study offers guidance on how to integrate AI technologies into existing security frameworks. This study is one of the first to conduct a bibliometric analysis of the integration of generative AI into security frameworks within transportation systems. As such, it provides a foundation for future research and development in this emerging area.

**Keywords:** AI-driven solutions, Autonomous vehicles, Cybersecurity, Generative AI, Threat detection, Traffic management, Transportation networks.

## 1. Introduction

Artificial Intelligence (AI) is increasingly transforming global businesses, disrupting industries and providing new ways to enhance efficiency, productivity and decision-making across critical infrastructure sectors. AI, through machine learning, deep learning and natural language processing, has opened up vast opportunities to optimize processes, reduce costs and improve safety in industries such as energy, water management, healthcare, manufacturing and several others. For example, in the energy sector, AI-driven predictive maintenance enables utilities to identify potential equipment failures before they occur, reducing downtime and preventing costly breakdowns (Hamdan *et al.,* 2024). By analyzing real-time data from sensors and historical trends, AI systems can schedule maintenance and suggest repairs, ultimately extending the lifespan of assets and minimizing disruptions. In the healthcare sector, AI-powered diagnostic tools are assisting doctors in detecting diseases early by analyzing medical images, accelerating the diagnostic process and increasing treatment accuracy (Zeb *et al.,* 2024). Similarly, AI in water management uses smart sensors to detect anomalies in water quality and leakage, helping utilities respond faster and more effectively to potential disruptions (Krishnan *et al.,* 2022). Manufacturing industries have also adopted AI for automation and quality control, where AI algorithms continuously monitor and improve production lines, reducing human error and enhancing product quality (Plathottam *et al.,* 2023). With its ability to process and analyze massive amounts of data in real-time, AI is emerging as a critical enabler of efficiency, safety and innovation in these sectors, highlighting its growing importance in enhancing the resilience and sustainability of critical infrastructure worldwide.

In the transportation sector, AI, particularly generative AI, holds tremendous promise in addressing long-standing challenges related to safety, efficiency and infrastructure resilience. Modern transportation systems face numerous hurdles, including traffic congestion, road safety concerns, increasing security risks and aging infrastructure (Lieberthal *et al.,* 2024). For instance, traffic congestion in urban areas not only leads to lost productivity but also exacerbates air pollution and affects public health. Generative AI can offer solutions by using real-time traffic data, weather forecasts and historical patterns to optimize traffic flow and suggest alternate

routes, alleviating congestion and reducing travel times (Yan and Li, 2023). Autonomous vehicles, powered by AI, have the potential to drastically reduce traffic accidents caused by human error, thus, ensuring safer roads. However, with the rise of connected and autonomous vehicles, transportation cybersecurity has become a significant concern. AI can address these vulnerabilities by detecting anomalies in the network, identifying potential cyber threats and responding in real-time to prevent disruptions or breaches (Jihong and Xiang, 2024). Another challenge the transportation industry faces is the maintenance of aging infrastructure, which often results in delays, accidents and costly repairs. Predictive maintenance powered by AI models can help transportation agencies monitor the condition of roads, bridges and railways, allowing them to prioritize repairs before they become critical failures (Malathi *et al.,* 2025). Furthermore, the optimization of logistics, from freight management to public transit schedules, can significantly benefit from AI, improving operational efficiency and reducing costs. By incorporating generative AI technologies, transportation networks can become more intelligent, responsive and sustainable, ensuring safer, faster and more efficient systems for the future (Yan and Li, 2023).

## 2. Gap assessment or problem statement

The use of artificial intelligence (AI) in transportation has significantly advanced in areas such as traffic management, autonomous vehicles and logistics. However, the integration of generative AI specifically for enhancing security frameworks within transportation systems is still in its early stages. Traditional cybersecurity frameworks, like those developed by the National Institute of Standards and Technology (NIST), are being adapted to the transportation sector, but they mainly focus on general cybersecurity measures rather than specifically utilizing generative AI. While generative AI is beginning to show promise in areas like threat detection and response, its application within transportation security frameworks is not yet widespread or fully developed. This gap in application highlights the need for a more focused approach to integrating generative AI into transportation security, which is the central problem addressed by this study. This research aims to explore the potential of generative AI in enhancing security frameworks within transportation systems. Through a bibliometric analysis, the study will assess the current state of generative AI applications in transportation security and identify existing research gaps. The goal is to provide insights into the direction of future research in this field. Additionally, the study

will propose actionable strategies to address the identified gaps, outlining a way forward for the broader integration of generative AI in transportation security. By bridging these gaps, the research aims to contribute to the development of more adaptive, anticipatory security measures within transportation networks, ultimately enhancing their resilience against emerging threats.

## 3. A brief overview of emerging technologies in the transportation sector

The transportation sector has undergone significant transformations in recent years, driven by rapid advancements in emerging technologies. These innovations have not only enhanced the efficiency, safety and sustainability of transportation systems but have also provided new opportunities to address longstanding challenges such as congestion, environmental impact and infrastructure strain.

*Artificial Intelligence (AI) and Machine Learning*: AI and machine learning are revolutionizing several aspects of the transportation sector. From smart traffic management systems to autonomous vehicles, AI plays a pivotal role in optimizing routes, reducing congestion and improving safety. AI algorithms process vast amounts of real-time data from sensors, cameras and GPS devices to predict traffic patterns, detect anomalies and provide actionable insights for operators. In the autonomous driving space, AI is the backbone of self-driving cars, enabling vehicles to make decisions based on real-time inputs from their environment (Lieberthal *et al.,* 2024). Moreover, AI is increasingly used in logistics to streamline supply chains and enhance fleet management, reducing operational costs and improving delivery times.

*Autonomous Vehicles (AVs):* Autonomous or self-driving vehicles represent one of the most significant technological innovations in transportation. These vehicles use a combination of AI, sensors and advanced algorithms to navigate roads and make decisions without human intervention. AVs have the potential to significantly reduce traffic accidents, enhance fuel efficiency and provide mobility solutions for people with disabilities (Qayyum *et al.,* 2020). As of now, several companies, including Tesla, Waymo, and Uber, are actively testing and deploying autonomous vehicles, though the widespread adoption of fully autonomous vehicles is still a work in progress.

*Electric and Connected Vehicles (EVs and CVs):* The rise of electric vehicles (EVs) and connected vehicles (CVs) is transforming the environmental footprint and operational dynamics

of transportation. EVs, powered by sustainable energy sources, are becoming more prevalent due to advancements in battery technology and growing consumer demand for greener alternatives. Coupled with connected vehicle technologies, EVs can communicate with infrastructure and other vehicles, enabling smoother, safer and more energy-efficient journeys (Jeihani *et al.,* 2022). Moreover, EVs can integrate with smart grids and renewable energy sources, contributing to the broader goal of reducing greenhouse gas emissions in the transportation sector.

*Smart Infrastructure and IoT:* The integration of Internet of Things (IoT) devices into transportation infrastructure is enabling more efficient and responsive transportation networks. IoT technology connects vehicles, infrastructure and people, creating a "smart" transportation ecosystem. Sensors embedded in roads, bridges and traffic signals gather data that is used to monitor traffic flow, track vehicle performance and predict maintenance needs. This data can be used for predictive maintenance of infrastructure, helping to avoid costly repairs and downtime. Furthermore, IoT-enabled devices provide real-time updates to travelers, enhancing their overall experience and safety (Bathla *et al.,* 2022).

*Blockchain for Transportation*: Blockchain technology is gaining traction in the transportation sector, especially for its potential to enhance security, transparency and efficiency. In logistics, blockchain enables secure, immutable tracking of goods, improving the supply chain's transparency and trustworthiness. Additionally, blockchain is being explored for its potential to secure payments, validate vehicle identities and facilitate smart contracts for transportation agreements (Jabbar *et al.,* 2022).

*5G and Communication Technologies:* The rollout of 5G technology is poised to enable faster, more reliable communication between vehicles, infrastructure and central control systems. This ultra-fast network promises to support the large amounts of data generated by autonomous vehicles and connected infrastructure, reducing latency and improving real-time decision-making. The enhanced communication capabilities of 5G will also support applications such as vehicle-to-everything (V2X) communication, which allows vehicles to communicate with each other and their environment to improve safety and traffic flow (Aliu and Oke, 2023). Table 1 presents a summary of emerging technologies in the transportation sector, detailing their descriptions, applications, and benefits.

Table 1: Summary of emerging technologies in the transportation sector

| S/N | Technology | Description | Applications | Benefits |
|---|---|---|---|---|
| 1. | Artificial Intelligence (AI) | Use of algorithms and machine learning to simulate human cognitive functions. | Traffic management, autonomous vehicles, predictive maintenance, route optimization, security systems. | Improved efficiency, reduced human error, better traffic flow, lower operational costs, enhanced security. |
| 2. | Autonomous Vehicles (AVs) | Self-driving vehicles use sensors, cameras and AI to navigate and make decisions without human input. | Passenger transport, freight and delivery services, last-mile logistics, shared mobility. | Reduced accidents, increased mobility for non-drivers, efficient transport, cost savings from reduced labor. |
| 3. | Urban Air Mobility (UAM) | Air transportation systems for passengers and cargo using small, electric aircraft. | Air taxis, urban delivery services, emergency medical transport. | Reduced traffic congestion, faster transportation, and reduced environmental impact. |
| 4. | Electric Vehicles (EVs) | Vehicles powered by electric motors rather than internal combustion engines. | Passenger vehicles, buses, delivery trucks, and even freight transport. | Lower emissions, reduced fuel consumption, cost savings on fuel, and better energy efficiency. |
| 5. | 5G Connectivity | High-speed, low-latency mobile network technology enables faster communication. | Real-time vehicle communication, smart traffic lights, vehicle-to-everything (V2X) communication. | Improved safety, real-time data sharing, enhanced automation and efficiency in transport. |
| 6. | Blockchain Technology | A decentralized, secure digital ledger technology used for transparent transactions. | Supply chain management, vehicle ownership tracking, toll systems, and smart contracts. | Enhanced transparency, fraud prevention, reduced administrative costs, and more secure transactions. |
| 7. | Internet of Things (IoT) | Network of interconnected devices that communicate and exchange data. | Smart infrastructure, real-time vehicle diagnostics, tracking systems, traffic management. | Improved operational efficiency, enhanced real-time data collection, and better resource allocation. |
| 8. | Drones | Unmanned aerial vehicles used for transport, delivery, and surveillance. | Parcel delivery, traffic monitoring, infrastructure inspection, and surveying. | Faster deliveries, reduced traffic congestion, and improved monitoring of infrastructure. |
| 9. | Smart Infrastructure | Advanced technologies are integrated into roads, bridges, and other infrastructure to optimize performance and safety. | Intelligent traffic systems, dynamic tolling, condition monitoring, and adaptive lighting. | Improved safety, reduced traffic delays, cost-effective maintenance, and better resource management. |
| 10. | Connected Vehicles | Vehicles are equipped with sensors and communication technology that enable them to exchange data with other vehicles and infrastructure. | Vehicle-to-vehicle (V2V) communication, vehicle-to-infrastructure (V2I), smart traffic signals. | Reduced accidents, smoother traffic flow, improved safety, and real-time communication for traffic management. |
| 11. | Mobility-as-a-Service (MaaS) | An integrated system that combines different modes of transport into a single accessible and customer-friendly digital platform. | Multi-modal transport, public transport integration, ride-sharing, and carpooling services. | Seamless travel experiences, reduced reliance on private cars, better urban mobility, and environmental benefits. |
| 12. | Smart Traffic Management | Advanced systems that use real-time data and predictive analytics to manage traffic flow more efficiently. | Adaptive traffic signals, congestion management, incident detection, and predictive route planning. | Reduced congestion, lower emissions, improved travel times, and enhanced driver safety. |
| 13. | Fleet Management Systems | Software solutions that monitor, manage, and optimize the performance of vehicle fleets. | Delivery services, logistics, public transport, and shared vehicle fleets. | Cost savings, fuel efficiency, maintenance optimization, better route planning, and enhanced customer service. |

| | | | | |
|---|---|---|---|---|
| 14. | V2X (Vehicle-to-Everything) | Communication systems enable vehicles to interact with each other and with infrastructure elements. | Traffic safety, vehicle coordination, autonomous driving, infrastructure support. | Improved safety, better coordination between vehicles and infrastructure, and reduced accidents. |
| 15. | Quantum Computing | An advanced computing technology based on quantum-mechanical phenomena to solve complex problems. | Traffic flow optimization, logistics optimization, real-time data processing for autonomous systems. | Potential for handling complex calculations much faster than classical computers, improving traffic management and autonomous driving capabilities. |
| 16. | Hyperloop | A new form of high-speed transportation using pressurized pods in near-vacuum tubes. | Long-distance travel, intercity transport. | Significantly faster than traditional rail and air travel, reducing travel times between cities. |
| 17. | Augmented Reality (AR) | Technology that overlays digital information on the real world. | Navigation assistance, training for drivers and operators, maintenance support. | Improved user experience, enhanced navigation, better decision-making, and reduced training time. |
| 18. | Advanced Driver Assistance Systems (ADAS) | Safety systems that assist drivers by automating and improving vehicle functions. | Lane-keeping assist, adaptive cruise control, automatic emergency braking, parking assistance. | Increased safety, reduction in accidents, and support for semi-autonomous driving. |
| 19. | Electric Vertical Take-Off and Landing (eVTOL) | Aircraft that can take off and land vertically, powered by electric motors. | Urban air mobility, aerial taxis, cargo transport, and emergency response. | Reduces urban traffic congestion, enables quicker travel, and reduces the carbon footprint of transportation. |

## 4. Research methodology

The main aim of this research is to explore the application of generative AI in enhancing security frameworks within transportation systems. To achieve this, a bibliometric analysis was conducted to assess the current state of generative AI applications in transportation security. Bibliometric analysis, as highlighted by Sajovic and Boh Podgornik (2022), is an effective tool for visualizing knowledge structures and identifying emerging trends in research. This analysis examined key themes and geographical research distribution, providing a holistic view of the state of AI-driven security research in transportation networks. To conduct this analysis, the study used VOSviewer software for data visualization of the bibliometric data. Scopus was selected as the primary database due to its broad coverage and capacity to handle large datasets (Zhao *et al.,* 2018). The bibliometric analysis specifically targeted research published between 2014 and 2024, using a search string that included terms such as “generative AI,” “AI-driven security,” “transportation networks,” “intelligent transportation systems,” “autonomous vehicles,” “machine learning,” “deep learning,” “data privacy,” “security frameworks,” and “critical infrastructure security.” The search was conducted through Scopus to ensure the inclusion of the most relevant and up-to-date studies. By identifying frequently explored themes

and collaboration patterns, this quantitative approach complements the qualitative review by offering a broader understanding of the state of research and pinpointing areas where further innovation is needed.

## 5. Results and discussion

### *5.1. Publication per year on studies*

Figure 1 presents the distribution of published studies per year on the integration of generative AI into transportation security frameworks. The data indicates minimal research activity before 2020, with no recorded publications from 2014 to 2017. A slight emergence of interest appeared in 2018 and 2019, with only one document published each year. There was a notable increase in publications in 2020, with nine studies, suggesting a growing recognition of the potential applications and challenges of generative AI in transportation security. A significant surge is observed in 2023, with 20 published studies, followed by a substantial peak in 2024, where research activity more than doubled, reaching 47 publications. This sharp rise suggests that generative AI's role in transportation security has gained substantial academic and industry attention, likely due to technological advancements, increased funding and growing concerns over cybersecurity and infrastructure resilience. The overall trend highlights a recent acceleration in research efforts, pointing to a rapidly evolving field with increasing scholarly interest.

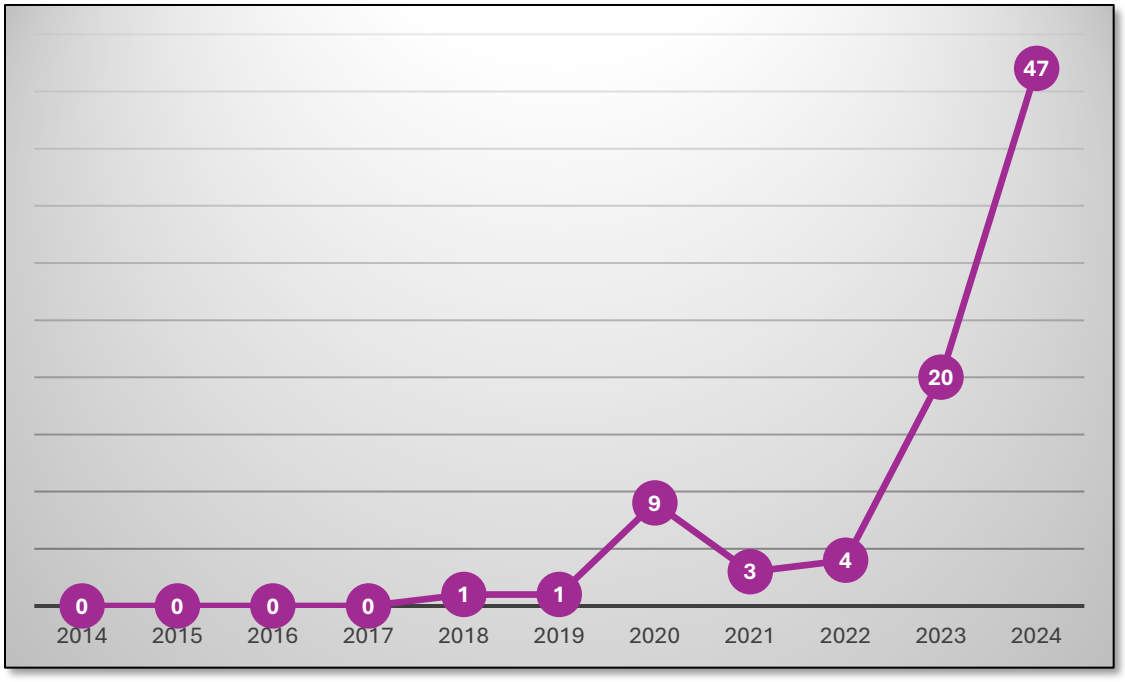

Figure 1: Publication per year on studies around generative AI in transportation networks

(Source: Author's creation)

### *5.2. Occurrence and cluster analysis*

***Cluster 1***, represented by the red node, contains 21 keywords, with "generative adversarial networks (GANs)" as the focal term. GANs exhibit strong link strength (LS) with "autonomous vehicles" (LS = 35), "traffic control" (LS = 29) and "large language models (LLMs)" (LS = 27), emphasizing the role of generative AI in optimizing transportation security frameworks, particularly in traffic management, predictive analytics, and autonomous mobility. The prominence of "urban transportation" and "real-time systems" suggests researchers are actively exploring AI-powered traffic solutions for smart cities, where AI-driven models enhance mobility, reduce congestion and improve road safety. Other key terms include "Internet of Things (IoT)," "diffusion models," "metaverses," "traffic congestion" and "urban planning," reflecting a research focus on leveraging AI and IoT for real-time traffic monitoring, AI-based simulations for traffic control, and the emerging use of metaverse environments for testing transportation policies. Studies within this cluster highlight how LLMs and GANs process vast traffic datasets and generate synthetic traffic scenarios to optimize congestion management and predict future traffic patterns (Yan and Li, 2023). The connection to "autonomous vehicles" and "motor transportation" suggests AI applications are extending into self-driving vehicle decision-making, where real-time AI models enable dynamic route optimization and enhanced road safety (Jihong and Xiang, 2024). Strong links to "traffic congestion" and "traffic control" align with AI-powered adaptive traffic management systems, where predictive models preemptively adjust signal timing and reroute vehicles to alleviate congestion (Malathi *et al.,* 2025). The inclusion of "IoT" and "highway administration" indicates researchers are examining how AI can integrate with sensor-based traffic monitoring and highway management for efficient transport planning. By leveraging AI-driven real-time control mechanisms, traffic agencies can mitigate bottlenecks, reduce accidents and enhance road efficiency. Based on these interconnections, this cluster is named ***Smart Routing and Traffic Control***.

***Cluster 2***, represented by the green node, contains 19 keywords, with "deep learning" as the focal term. It exhibits strong link strength (LS) with "reinforcement learning" (LS = 33), "predictive models" (LS = 30) and "intelligent transportation" (LS = 28), emphasizing the role of

AI-driven predictive models in transportation security frameworks. These technologies support vehicle-to-vehicle communication, forecasting and autonomous decision-making, making transportation systems more adaptive and efficient. The connection to "reinforcement learning" and "deep reinforcement learning" highlights AI's ability to optimize real-time traffic flow, autonomous navigation, and adaptive control mechanisms in self-driving vehicles (Malathi *et al.,* 2025). "Adversarial machine learning" is also prominent, indicating its importance in detecting vulnerabilities in AI-powered models and enhancing cybersecurity within transportation networks (Qayyum *et al.,* 2020). These learning models contribute to improving decision-making capabilities, allowing intelligent transportation systems to respond effectively to dynamic traffic conditions. Other key terms include "contrastive learning," "autoencoders" and "neural networks," which point toward the development of self-learning AI models for anomaly detection, predictive traffic modeling and intelligent vehicle systems. These AI techniques help simulate traffic patterns, forecast congestion and optimize real-time route planning, thus, enhancing overall transportation efficiency. Additionally, the presence of "job analysis" and "task analysis" suggests research into AI's role in workforce transformation, particularly in human-AI interactions within transportation security operations (Loske and Klumpp, 2021). As AI-driven systems become more sophisticated, integrating AI with human decision-making will be critical for operational efficiency. Given the strong focus on predictive modeling, traffic forecasting, and intelligent adaptation, this cluster is named ***Traffic Pattern Simulation and Prediction***.

***Cluster 3***, represented by the blue node, contains 15 keywords, with "artificial intelligence" as the focal term. It has strong link strength (LS) with "machine learning" (LS = 32), "generative adversarial networks (GANs)" (LS = 28), and "computer vision" (LS = 27), emphasizing AI's role in transforming transportation systems through enhanced security, operational efficiency and automation. The connection to "network security" and "adversarial networks" highlights growing concerns about securing AI-driven transportation networks. As AI models become essential for traffic management and autonomous vehicle operations, their vulnerability to adversarial attacks must be addressed (Malathi *et al.,* 2025). GANs play a crucial role in cybersecurity by simulating cyberattacks, and helping to develop more resilient defense mechanisms for transportation infrastructures (Yan and Li, 2023). These networks also generate synthetic data for training AI systems, improving their ability to detect and respond to real-time threats. The presence of "big data," "data set" and "predictive models" signals a shift toward utilizing large-scale datasets and

AI-driven predictive analytics to enhance transportation security. AI is increasingly applied in processing real-time traffic data, optimizing traffic flow, predicting maintenance needs, and improving system resilience (Malathi *et al.,* 2025). Furthermore, the term "learning systems" underscores AI's ability to continuously adapt to evolving traffic conditions, environmental factors, and infrastructure performance, ensuring more accurate and efficient real-time decision-making. The inclusion of "intelligent transportation" and "intelligent vehicle highways" highlights AI's growing application in autonomous vehicles and smart infrastructure. AI-powered systems enable real-time navigation, vehicle-to-infrastructure communication and adaptive traffic management, enhancing safety and reducing congestion (Bathla *et al.,* 2022). Given the cluster's focus on AI-driven security and predictive analytics, it is named ***Transportation Cybersecurity and Intelligence***.

***Cluster 4***, represented by the yellow node, consists of 11 keywords, with "artificial intelligence (AI)" as the focal term. It has strong link strength (LS) with "decision making" (LS = 34), "machine learning" (LS = 30) and "deep neural networks" (LS = 28), emphasizing AI's role in enhancing decision-making processes within transportation security frameworks. The connection to "decision making" highlights AI's ability to automate complex processes, such as traffic management, route optimization, and security risk assessment, by analyzing vast amounts of real-time data (Malathi *et al.,* 2025). The presence of "machine learning" and "deep neural networks" suggests AI-driven models are being used for predictive analysis, optimizing vehicle performance, and strengthening transportation infrastructure. The term "emerging technologies" indicates the adoption of advanced innovations, such as the integration of AI with the Internet of Things (IoT), to create intelligent transportation systems capable of anticipating and mitigating potential security threats (Loske and Klumpp, 2021). "Federated learning" points to decentralized AI models that enable secure data-sharing across transportation networks without compromising privacy, making it a crucial component in large-scale, interconnected systems. Additionally, the terms "interpretability" and "learning algorithms" highlight ongoing research into making AI-driven decision-making systems more transparent and explainable. Ensuring that AI models can be interpreted by human operators is essential for trust, accountability, and regulatory compliance in transportation security applications. Given the cluster's emphasis on AI-driven automation, predictive analytics and secure decision-making frameworks, it is named ***Real-Time Decision Support Systems***.

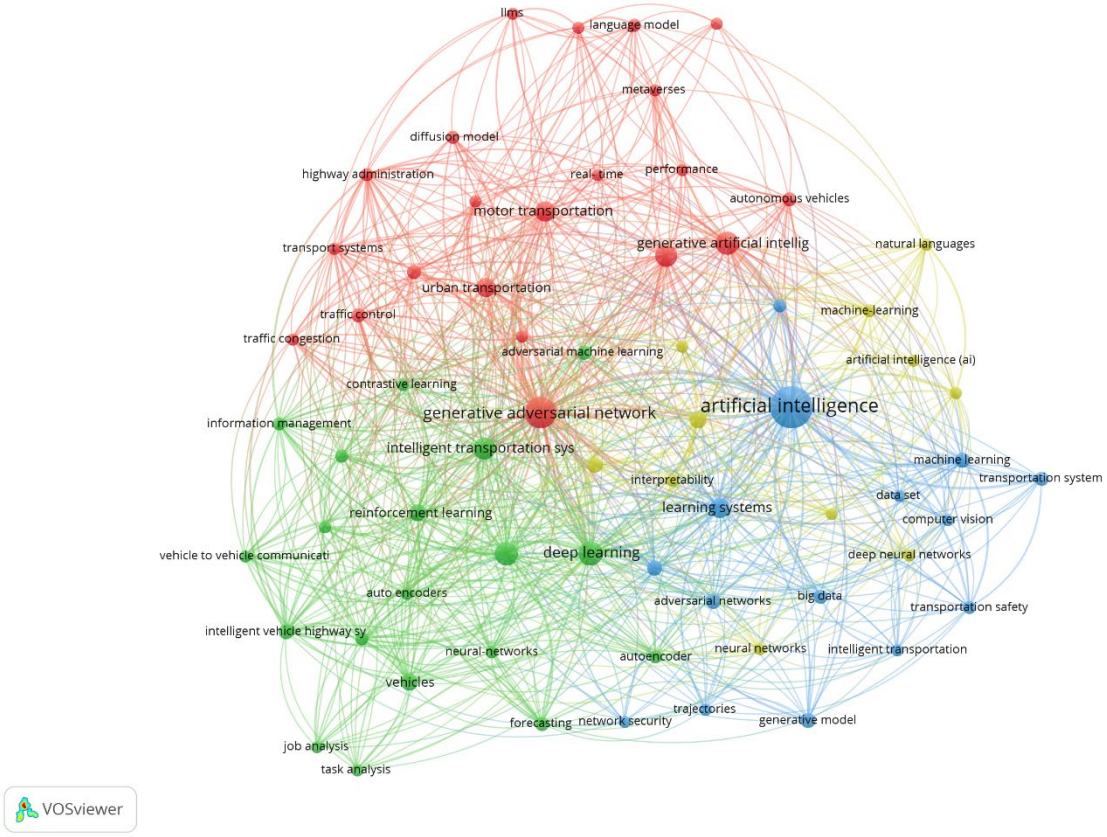


Figure 2: Network visualization of co-occurring keywords in generative AI studies on transportation security

### *5.3. Directions and Gaps*

Further assessment of the overlay visualization map generated by VOSviewer and presented in Figure 3. The visualization, structured as a network graph, showcases the relationships between different keywords over the timeline from 2022 to 2024. The nodes in the graph represent keywords, with their sizes indicating relative importance or frequency of occurrence. Additionally, the color gradient, transitioning from blue (2022) to yellow (2024), provides insight into the temporal progression of research focus areas. Connections between nodes represent co-occurrences, highlighting interdependencies among concepts. The early research phase, characterized by blue nodes, predominantly focused on foundational concepts. The emphasis during this period was on understanding transportation challenges, task structuring and fundamental AI applications. However, security-related terms such as “network security” and

“adversarial machine learning” remained peripheral, suggesting that while security concerns were acknowledged, they were not yet a central theme in generative AI applications for transportation.

The subsequent period, represented by green nodes, marked a shift towards the integration of advanced AI techniques. This transition signifies a growing interest in leveraging sophisticated AI methodologies for transportation challenges. Concurrently, security considerations became more pronounced, with “adversarial machine learning” and “network security” emerging as more interconnected with AI and transportation concepts. In the most recent phase, illustrated by yellow nodes, “real-time performance” and “autonomous vehicles” have gained traction, highlighting the growing need for AI solutions capable of dynamic and automated decision-making in transportation systems.

Despite these advancements, several research gaps remain. One notable gap is the lack of explicit security frameworks tailored specifically for generative AI in transportation. While “adversarial machine learning” and “network security” are present in the visualization, they do not indicate the development of dedicated security architectures addressing generative AI-related vulnerabilities. Furthermore, there is an absence of explicit mentions of “data privacy” and “trustworthy AI,” which are critical given the data-intensive nature of generative AI models in transportation networks. Another key gap is the limited focus on explainability and interpretability. The visualization does not prominently feature “explainable AI” (XAI), a crucial aspect in ensuring transparency and accountability in AI-driven transportation systems. Additionally, while “real-time performance” is acknowledged, considerations regarding scalability and the real-world deployment of generative AI-based security solutions in complex transportation networks remain underexplored. Also, the visualization does not explicitly reflect interdisciplinary collaboration, which is essential for effectively addressing security challenges in AI-driven transportation systems. The integration of expertise from AI researchers, transportation engineers, cybersecurity specialists and policymakers is necessary to develop comprehensive and robust security solutions. Finally, as discussed in the previous section, existing studies have predominantly focused on four key clusters which include: (1) smart routing and traffic control, (2) traffic pattern simulation and prediction, (3) transportation cybersecurity and intelligence and (4) real-time decision support systems. While these areas have garnered significant attention,

other potential applications, such as urban planning and smart city integration or behavioral analysis and fraud detection, remain underexplored and present opportunities for further investigation.

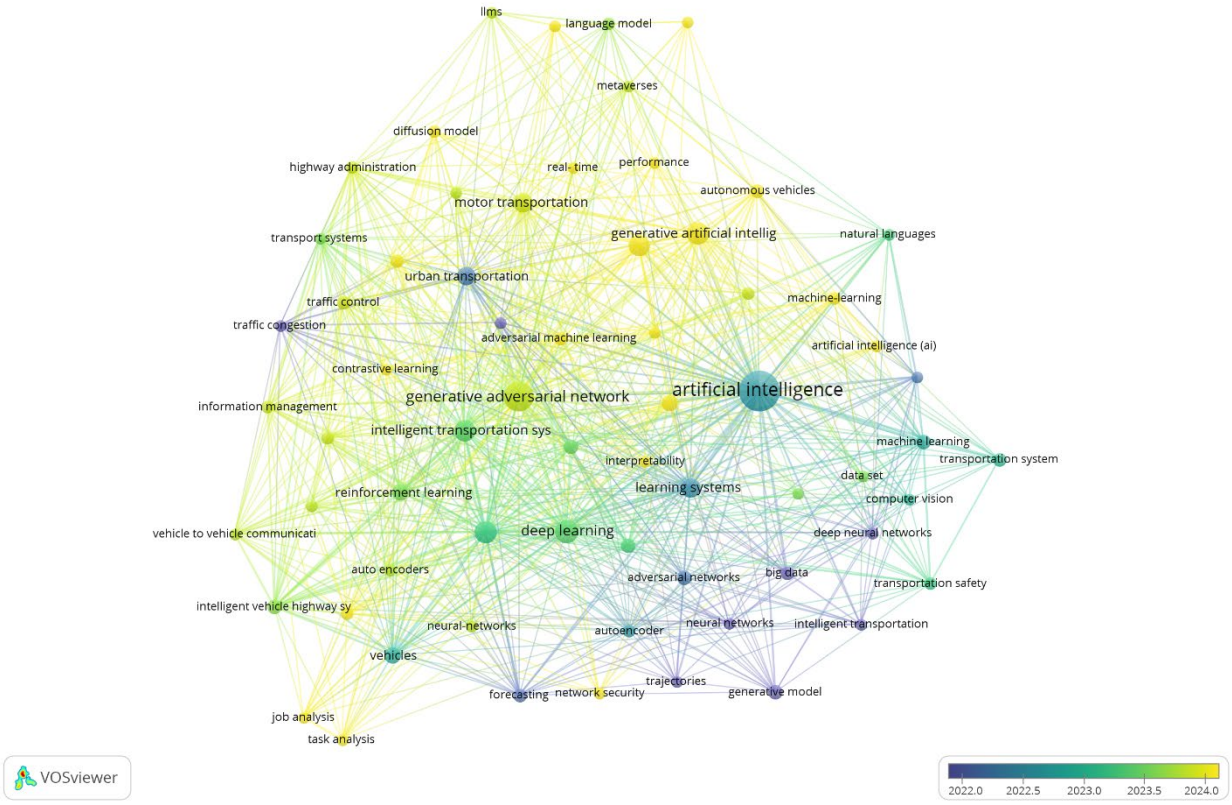


Figure 3: Overlay visualization of co-occurring keywords showing trends and possible gaps

### *5.4. The way forward to address these gaps*

To address the gaps identified in the previous section of the report, several strategic actions must be taken.

- **Development of tailored security frameworks**

A major gap in current research is the lack of explicit security frameworks designed specifically for generative AI in transportation. Given the unique vulnerabilities introduced by AI, particularly in adversarial attacks and data manipulation, it is essential to develop robust and adaptive security architectures. For instance, generative adversarial networks (GANs) could be used to simulate potential attack scenarios, helping to identify weaknesses in AI-driven systems

before they are deployed. Companies like Tesla, which utilize AI in autonomous vehicles, are beginning to explore the need for more rigorous security measures to prevent attacks such as data poisoning, which could manipulate the vehicle's decision-making processes (Fu *et al.,* 2024). Therefore, future research should focus on creating security protocols that anticipate and counteract AI-specific vulnerabilities in transportation systems.

- **Strengthening data privacy and building trust**

As generative AI models rely on vast amounts of data, the protection of this data is paramount. The absence of explicit mentions of "data privacy" and "trustworthy AI" in current research indicates a significant gap. To address this, future work should focus on strengthening data privacy measures to comply with regulations like the General Data Protection Regulation (GDPR) in Europe or the California Consumer Privacy Act (CCPA) in the U.S. For example, using federated learning, where data remains decentralized, can help mitigate privacy risks by enabling AI models to learn from data without directly accessing it. This approach is already being tested by companies like Google, which applies federated learning in mobile devices to enhance privacy while improving machine learning models. Implementing such privacy-preserving techniques will not only ensure legal compliance but also build public trust in AI applications in transportation.

- **Fostering explainability and interpretability in AI**

The lack of explainability and interpretability is another critical gap in the application of generative AI in transportation. AI systems often operate as "black boxes" (Felder, 2021), making it difficult for operators to understand how decisions are made, which is problematic for safety-critical applications like autonomous driving. To enhance transparency, future research must focus on integrating Explainable AI (XAI) techniques that provide clear insights into the decision-making processes of AI models. For instance, in autonomous vehicles, operators and passengers must understand why a vehicle chose one route over another or how it responded to an obstacle. Companies like Waymo are exploring the integration of interpretable AI to ensure that autonomous vehicles' decision-making processes can be understood and audited. Developing these systems will increase accountability and help ensure the safety of AI-driven transportation networks.

- **Focusing on scalability and real-world deployment**

While generative AI has demonstrated significant potential in controlled environments, scaling these solutions to work in real-world transportation networks remains a challenge. The scalability of AI-based security solutions must be tested in complex, large-scale transportation systems. For example, AI-driven traffic management systems, which optimize traffic flow in real-time, need to be capable of handling the vast number of variables present in urban settings, such as unpredictable traffic conditions, accidents, or weather. Cities like Singapore have successfully implemented AI-based traffic control systems that analyze traffic patterns in real-time and adjust signals to reduce congestion. Future research should aim to develop similar solutions that are not only effective in simulation but also capable of handling the complexity of real-world environments. This includes ensuring that AI systems are adaptable and reliable across different transportation infrastructures.

- **Encouraging interdisciplinary collaboration**

The complexity of securing AI-driven transportation systems highlights the importance of interdisciplinary collaboration. Current research does not explicitly reflect the collaboration between AI researchers, transportation engineers, cybersecurity experts and policymakers, which is critical for creating widespread and practical security solutions. For example, the collaboration between AI experts and transportation authorities in the development of autonomous vehicle regulations is essential to address both technical and ethical concerns. A real-world example of such collaboration can be seen in the work of the U.S. Department of Transportation, which partners with various research institutions and private companies to shape policies that ensure the safety and security of autonomous vehicles. Encouraging collaboration across disciplines will help address the multifaceted challenges of securing AI-driven transportation systems.

## 6. Practical applicability of findings

The findings of this study provide key insights for private industry professionals engaged in the development, deployment and management of generative AI technologies in transportation networks. By focusing on the four key clusters obtained in this study, industry stakeholders can apply AI-driven solutions to enhance operational efficiency, improve safety and address emerging security challenges. Generative AI's potential in optimizing smart routing systems is

particularly relevant for private companies working in traffic management and urban mobility solutions. AI-driven routing systems, powered by reinforcement learning and deep learning models, can dynamically adapt to changing traffic conditions, improving flow and reducing congestion. For example, companies like Waymo and Tesla are already integrating real-time traffic data into their autonomous vehicle systems to optimize routing decisions. Private industry professionals can adopt similar AI-driven solutions to manage large-scale transportation systems, integrating generative AI into traffic signal systems or smart traffic lights to reduce wait times and increase traffic throughput. Also, AI can be used to predict traffic disruptions and suggest alternative routes for drivers, improving efficiency across urban transportation networks. This would be especially beneficial for large logistics and transportation companies such as FedEx and UPS, who rely heavily on efficient route optimization to manage their fleet operations.

The ability to simulate and predict traffic patterns is crucial for both urban planning and day-to-day traffic management. Industry professionals in transportation and logistics can leverage generative AI models to simulate traffic scenarios and predict congestion patterns, enabling proactive decision-making. For instance, AI models can predict peak traffic hours and advise cities or companies on how to manage traffic flows during those times. Companies like Google with their Google Maps application already utilize AI to forecast traffic conditions, but the potential for deeper integration with generative AI models remains largely untapped. Private industry professionals can use these insights to develop more accurate simulations of traffic flows in cities, allowing for better planning of infrastructure projects such as new roads or overpasses. These predictions could also be integrated into fleet management systems, helping companies like DHL or Amazon optimize delivery routes based on traffic predictions, saving time and reducing fuel costs.

With the increasing reliance on AI for transportation systems, ensuring cybersecurity is paramount. This study highlights the need for tailored security frameworks that address vulnerabilities specific to generative AI applications in transportation. For instance, Generative Adversarial Networks (GANs) could be used to simulate cyberattacks, helping companies identify vulnerabilities before they are exploited. Transportation management companies and smart city developers can leverage these techniques to create proactive, self-healing systems that automatically detect and mitigate potential cyber threats. A concrete example is Tesla’s use of AI

for autonomous driving, where constant software updates and vulnerability testing are crucial for maintaining system integrity. Professionals in the transportation sector can collaborate with cybersecurity experts to develop generative AI-driven security systems that predict and defend against potential attacks, protecting both the data and physical infrastructure of transportation networks. These models can also help detect malicious activities in real-time, allowing quick responses to cyber threats that could otherwise disrupt transportation operations.

The ability to make decisions quickly and accurately in real-time is vital for the efficient operation of transportation networks. Generative AI can enhance real-time decision support systems by analyzing massive amounts of data instantly and providing actionable insights. For example, in the context of autonomous vehicles, AI can be used to analyze traffic, weather and road conditions, and make real-time decisions that ensure safe and efficient operation. Uber and Lyft, for instance, rely heavily on AI to optimize ride-sharing routes in real-time. However, with the integration of generative AI, these companies can take this a step further by allowing their systems to adapt autonomously to unforeseen circumstances, such as accidents or road closures, in real-time. Public transportation providers can also use AI to adjust schedules, routes, and vehicle assignments based on real-time passenger demand, ensuring a seamless commuting experience for users. For large-scale operations, AI can assist in optimizing the deployment of resources during peak hours or emergencies, improving service delivery and customer satisfaction.

To fully harness the potential of generative AI in transportation networks, industry professionals must address several critical gaps highlighted in this study. Firstly, there is an urgent need for the development of security frameworks specifically designed to address generative AI-related vulnerabilities in transportation systems. This includes creating proactive and self-healing systems that can detect and mitigate potential cyber threats. Also, the industry must integrate considerations around data privacy and trustworthy AI to ensure that the data-intensive nature of generative AI models does not compromise user privacy and the integrity of transportation systems. Additionally, explainable AI (XAI) needs to be a key focus. The lack of transparency in how AI systems make decisions is a significant challenge, especially in safety-critical applications like autonomous driving. Industry stakeholders must invest in making AI models more interpretable and transparent, ensuring that operators and regulators can understand the

decision-making process. This will also help address public concerns around the accountability of AI-driven systems. Finally, there needs to be a stronger emphasis on real-world deployment and scalability. While AI models show great promise in simulations, real-world applications, especially at the scale required for large transportation networks, remain underexplored. Collaboration between AI researchers, transportation engineers, cybersecurity professionals and policymakers is essential to design robust and scalable solutions that can be effectively deployed in complex environments.

## 7. Conclusion

The main aim of this research is to explore the application of generative AI in enhancing security frameworks within transportation systems. Using a bibliometric analysis approach, the study reviewed existing literature and revealed key themes and research clusters, including smart routing and traffic control, traffic pattern simulation and prediction, transportation cybersecurity and intelligence and real-time decision support systems. Despite the growing interest in these areas, several critical gaps were identified, particularly around security frameworks, explainability, scalability and interdisciplinary collaboration.

Practically, the findings from this study can guide policymakers, technology developers and transportation network operators in making informed decisions about how to harness the potential of generative AI. For instance, addressing the security gaps related to generative AI's vulnerabilities, such as developing tailored security frameworks and enhancing real-time decision-making capabilities, can help reduce risks and improve system resilience. Additionally, advancing explainable AI (XAI) will be essential for building trust and ensuring that these technologies are not only effective but also transparent and accountable. The insights from this study can also inform future investments in AI-driven security solutions, including the development of more scalable and real-world deployable systems. Another key contribution of this study is the identification of the research gaps and the categorization of generative AI applications into specific clusters. This approach provides a more structured pathway to understanding the opportunities and possibilities in integrating AI technologies into transportation security. Industry professionals can benefit from this taxonomy by focusing on specific clusters that are most relevant to their operations. For example, a transportation

company focusing on autonomous vehicles could prioritize cybersecurity and intelligence, while a smart city developer might focus on smart routing and traffic control. Researchers can also use this clusterization to design future studies that investigate the impact of generative AI on specific areas of transportation security and infrastructure resilience.

Looking ahead, future research efforts should address several key areas. First, empirical data collection will be crucial to validate the theoretical insights from this study and provide a real-world understanding of the challenges and benefits of implementing generative AI in transportation security. A mixed-methods approach combining surveys and case studies of organizations that have adopted AI-driven solutions could offer deeper insights into the practical implications of these technologies. Furthermore, exploring region-specific challenges and opportunities will allow for more targeted research. For example, the security needs of urban transportation networks may differ from those of rural or remote areas and understanding these distinctions will help in tailoring AI applications for different contexts. Additionally, future studies should explore the potential of generative AI in other under-explored areas, such as urban planning, smart city integration and behavioral analysis. These areas have significant implications for enhancing overall transportation system efficiency and security, but they remain largely unexplored in the current body of literature. Addressing these gaps could open up new avenues for research and innovation that drive the next generation of intelligent transportation systems.

**References**


Aliu, J., & Oke, A. E. (2023). Construction in the digital age: exploring the benefits of digital technologies. *Built Environment Project and Asset Management*, *13*(3), 412-429. https://doi.org/10.1108/BEPAM-11-2022-0186

Bathla, G., Bhadane, K., Singh, R. K., Kumar, R., Aluvalu, R., Krishnamurthi, R., ... & Basheer, S. (2022). Autonomous vehicles and intelligent automation: Applications, challenges, and opportunities. *Mobile Information Systems*, *2022*(1), 7632892. https://doi.org/10.1155/2022/7632892

Felder, R. M. (2021). Coming to terms with the black box problem: how to justify AI systems in health care. *Hastings Center Report*, *51*(4), 38-45. https://doi.org/10.1002/hast.1248

Fu, T., Sharma, M., Torr, P., Cohen, S. B., Krueger, D., & Barez, F. (2024). PoisonBench: Assessing Large Language Model Vulnerability to Data Poisoning. *arXiv preprint arXiv:2410.08811*. https://doi.org/10.48550/arXiv.2410.08811

Hamdan, A., Ibekwe, K. I., Ilojianya, V. I., Sonko, S., & Etukudoh, E. A. (2024). AI in renewable energy: A review of predictive maintenance and energy optimization. *International Journal of Science and Research Archive*, *11*(1), 718-729. https://doi.org/10.30574/ijsra.2024.11.1.0112

Jabbar, R., Dhib, E., Said, A. B., Krichen, M., Fetais, N., Zaidan, E., & Barkaoui, K. (2022). Blockchain technology for intelligent transportation systems: A systematic literature review. *IEEE Access*, *10*, 20995-21031. https://10.1109/ACCESS.2022.3149958

Jeihani, M., Ansariyar, A., Sadeghvaziri, E., Ardeshiri, A., Kabir, M. M., Haghani, A., & Jones, A. (2022). Investigating the effect of connected vehicles (CV) route guidance on mobility and equity. URL : https://rosap.ntl.bts.gov/view/dot/60931

Jihong, X. I. E., & Xiang, Z. H. O. U. (2024). Edge Computing for Real-Time Decision Making in Autonomous Driving: Review of Challenges, Solutions, and Future Trends. *International Journal of Advanced Computer Science & Applications*, *15*(7). 10.14569/IJACSA.2024.0150759

Krishnan, S. R., Nallakaruppan, M. K., Chengoden, R., Koppu, S., Iyapparaja, M., Sadhasivam, J., & Sethuraman, S. (2022). Smart water resource management using Artificial Intelligence—A review. *Sustainability*, *14*(20), 13384. https://doi.org/10.3390/su142013384

Lieberthal, E. B., Serok, N., Duan, J., Zeng, G., & Havlin, S. (2024). Addressing the urban congestion challenge based on traffic bottlenecks. *Philosophical Transactions A*, *382*(2285), 20240095. https://doi.org/10.1098/rsta.2024.0095

Loske, D., & Klumpp, M. (2021). Intelligent and efficient? An empirical analysis of human–AI collaboration for truck drivers in retail logistics. *The International Journal of Logistics Management*, *32*(4), 1356-1383. https://doi.org/10.1108/IJLM-03-2020-0149

Malathi, D., Alaswad, F., Aljaddouh, B., Ranganayagi, L., & Sangeetha, R. (2025, January). AI-Powered Traffic Management: Improving Congestion Detection and Signal Regulation. In *2025 International Conference on Multi-Agent Systems for Collaborative Intelligence (ICMSCI)* (pp. 899-904). IEEE. http://doi.org/10.1109/ICMSCI62561.2025.10894186

Plathottam, S. J., Rzonca, A., Lakhnori, R., & Iloeje, C. O. (2023). A review of artificial intelligence applications in manufacturing operations. *Journal of Advanced Manufacturing and Processing*, *5*(3), e10159. https://doi.org/10.1002/amp2.10159

Qayyum, A., Usama, M., Qadir, J., & Al-Fuqaha, A. (2020). Securing connected & autonomous vehicles: Challenges posed by adversarial machine learning and the way forward. *IEEE Communications Surveys & Tutorials*, *22*(2), 998-1026. https://doi.org/10.1109/COMST.2020.2975048

Sajovic, I., & Boh Podgornik, B. (2022). Bibliometric analysis of visualizations in computer graphics: a study. *Sage Open*, *12*(1), 21582440211071105. https://doi.org/10.1177/2158244021107110

Yan, H., & Li, Y. (2023). A survey of generative ai for intelligent transportation systems. *arXiv preprint arXiv:2312.08248*. https://doi.org/10.48550/arXiv.2312.08248

Zeb, S., Nizamullah, F. N. U., Abbasi, N., & Fahad, M. (2024). AI in healthcare: revolutionizing diagnosis and therapy. *International Journal of Multidisciplinary Sciences and Arts*, *3*(3), 118-128. https://doi.org/10.47709/ijmdsa.v3i3.4546

Zhao, F., Fashola, O. I., Olarewaju, T. I., & Onwumere, I. (2021). Smart city research: A holistic and state-of-the-art literature review. *Cities*, *119*, 103406. https://doi.org/10.1016/j.cities.2021.103406

**Author Biography**

**John Aliu, PhD,** is currently a Clinical Assistant Professor with the Engineering Education Transformations Institute, College of Engineering, University of Georgia, Athens, Georgia. He has authored and co-authored several publications in top journals in the field of construction digitalization, sustainable construction and engineering education. John is a regular reviewer for different peer-reviewed journals, including the *Journal of Cleaner Production, Engineering, Construction and Architectural Management, Sustainable Development Journal, Frontiers in Built Environment, International Journal of Sustainability in Higher Education, Construction Economics and Building, African Journal of Science, Technology, Innovation and Development, Journal of Construction in Developing Countries, Journal of Engineering, Design and Technology, Journal of Construction Project Management and Innovation, International Journal of Construction Management, Journal of Construction Engineering and Management, Cogent Economics and Finance, Built Environment Project and Asset Management*, and others. He is currently an Associate Editor of ASCE'S *Journal of Civil Engineering Education*.

# INSTITUTE FOR HOMELAND SECURITY

The Institute for Homeland Security at Sam Houston State University is focused on building strategic partnerships between public and private organizations through education and applied research ventures in the critical infrastructure sectors of Transportation, Energy, Chemical, Water / Wastewater, Healthcare, and Public Health.

The Institute is a center for strategic thought with the goal of contributing to the security, resilience, and business continuity of these sectors from a Texas Homeland Security perspective. This is accomplished by facilitating collaboration activities, offering education programs, and conducting research to enhance the skills of practitioners specific to natural and human caused Homeland Security events.

Institute for Homeland Security
Sam Houston State University



Aliu, J. (2025). Generative AI for Advanced Security Frameworks in Transportation Networks (Institute for Homeland Security Report No. 2025-1012). Institute for Homeland Security.

https://doi.org/10.17605/OSF.IO/9VY5C