EURASIAN JOURNAL OF MATHEMATICAL AND COMPUTER APPLICATIONS
ISSN 2306–6172
Volume 14, Issue 2 (2026) 52 – 66

ARTIFICIAL INTELLIGENCE FOR SECURE MOBILITY

Csorgoova V., Varkonyi-Koczy A., Shayakhmetov A. [1], Sabdenaliyev B., Baipakbayeva S.

Abstract Greater cybersecurity requirements are imposed on intelligent mobility systems by artificial intelligence. Digital transport infrastructure is protected to support safety, reliability, and resilience. Cybersecurity applications are assessed through a structured review and scientometric analysis. Intelligent transport, autonomous vehicles, sustainable mobility, and transport optimization are examined. Traffic control, prediction, anomaly detection, and system coordination are improved by artificial intelligence. Secure transport is strengthened by machine-based, federated, and deep reinforcement methods. Adoption, cybersecurity integration, standardization, and explainability are still limited. Further research is required for scalable, secure, and context-sensitive mobility solutions.

Keywords: Intelligent Mobility, Autonomous Vehicles, Connected Vehicles, Machine Learning, Intelligent Transport Systems, Federated Learning, Blockchain Security, Smart Cities.

AMS Mathematics Subject Classification: 68T07, 68T09.

DOI: 10.32523/2306-6172-2026-14-2-52–66

1 Introduction

Urban mobility is widely studied because of urban growth, environmental pressure, and greater transport demand. Smart mobility is defined by advanced technologies for efficiency, sustainability, and improved urban life. Mobility as a Service, intelligent transport, and connected platforms are used to reduce congestion and emissions. These systems are supported by digital infrastructure, data exchange, and integrated multimodal services [1, 2]. Before artificial intelligence, mobility is managed through deterministic models, statistical analysis, and rule-based methods. Historical data and manual interpretation are used for traffic models, infrastructure design, and demand estimates [3, 4]. However, nonlinear relations, dynamic behavior, and large datasets are poorly represented by these methods. Complex multidimensional problems are created by integrated transport, energy, and communication networks. Prediction accuracy and adaptability are therefore reduced in complex urban systems [5, 6]. These limitations are addressed through artificial intelligence and machine-learning methods. Accurate forecasts, rapid data analysis, and adaptive decisions are enabled in complex systems. Traffic control, electric vehicle energy use, autonomous vehicle control, and

[1]Corresponding Author.

mobility prediction are improved. System performance is increased through automated pattern detection, scalable analysis, and nonlinear models [7, 8, 9]. The literature is large, diverse, and divided across several mobility domains. Most reviews are restricted to personalization, electrification, or individual technologies. Therefore, comprehensive knowledge across mobility domains is limited [2, 3, 10]. An integrated review is required to classify methods, identify challenges, and assess research trends. Multidisciplinary evidence is combined, and a unified classification of artificial intelligence methods is provided [1]. The remainder of this article is organized as follows. Section 2 presents the methodological approach used for literature selection and analysis. Section 3 reviews artificial intelligence techniques applied in mobility systems. Section 4 discusses application domains and comparative analysis. Section 5 examines current challenges and future research directions.

Table 1 Comparison of State of the Art Research on Artificial Intelligence in Mobility.

Reference	**Focus Area**	**Key Contribution / Progress**	**State of the Art Insight**
Rouky et al. [2]	Mobility as a Service (MaaS)	Systematic classification of AI applications across MaaS integration levels	Progress from basic optimization to advanced AI driven personalized mobility systems
Vermesan et al. [4]	ECAS Vehicles and Green Mobility	Integration of AI with IoT, edge computing, and V2X	Foundation for connected, autonomous, sustainable vehicle ecosystems
Wang et al. [5]	Smart City Mega Mobility Systems	Macro micro integration model for urban mobility analysis	AI enabled multi level modeling for large scale mobility networks
Ali et al. [8]	6G C V2X Networks	Machine learning based mobility management framework	Ultra reliable, low latency communication for next generation vehicular networks
Bou Abboud et al. [6]	5G Mobility Prediction	AI driven prediction models for traffic and network optimization	Proactive resource allocation and real time mobility management
Noor Ali et al. [7]	Electric Mobility and Energy Systems	Machine learning for EV performance and energy management	Intelligent electrification through predictive analytics
Lee et al. [9]	Intelligent Seaport Mobility	Deep learning based computer vision for logistics optimization	Real time infrastructure efficiency in port mobility systems
Ali et al. [10]	Connected Autonomous Vehicles	Federated learning for distributed intelligence	Privacy preserving and decentralized AI in transportation systems

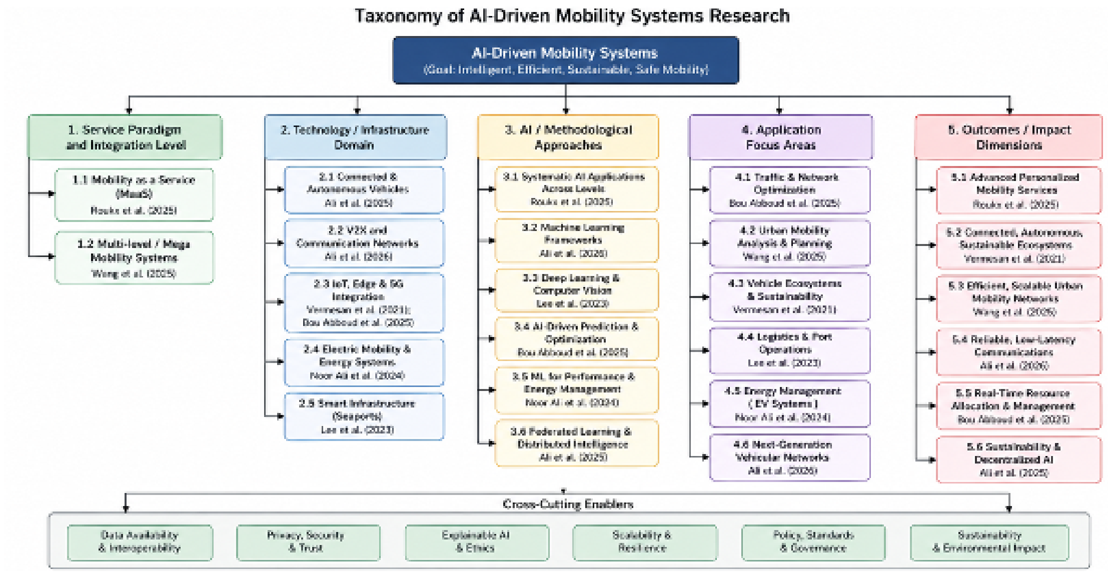

Figure 1: Taxonomy of the review articles on AI and mobility

Figure 1 classifies AI driven mobility applications into five domains, i.e., service models, infrastructure, AI methods, applications, and outcomes. It shows strong research attention on MaaS, connected vehicles, V2X, IoT, machine learning, traffic control, logistics, and sustainable mobility. The taxonomy is useful because technical tools are linked with goals such as efficiency, personalization, and reliability. However, it is static and does not show research maturity or relation strength between domains. Human factors, governance, cybersecurity, data management, and sustainability metrics are underrepresented. Major gaps are identified in explainable AI, field deployment, federated models, and inclusive mobility. Further study is required for EV grid integration, cyber resilience, digital twins, and benchmark datasets. Strong technical progress is reported, but system-level integration is still limited. Artificial intelligence research in mobility is extensive, yet the literature is fragmented. Several reviews are restricted to Mobility as a Service or general smart mobility [2, 1]. Other studies are limited to connected vehicles, smart cities, and communication networks [4, 5, 8, 6]. Electric vehicles, seaports, and federated models are also examined as isolated domains [7, 9, 10]. Cross-domain integration is therefore insufficient across the current evidence base. A comprehensive analysis of research trends and structured classification is absent. This gap is addressed through scientometric analysis and a taxonomy of artificial intelligence applications. Systematic comparison, research pattern identification, and unified field interpretation are thereby supported.

2 Research methodology

In this study we explore Scopus database for methods and applications of Artificial Intelligence and Cybersecurity in Mobility. To explore the AI methods and applications the queries of search includes the fundamental AI keywords, as proposed by former studies e.g., [11, 12], in addition to mobility keywords, i.e., transport and mobility. The search results in 5750 documents for the period of 2016 to 2026 which is conducted (April 27, 2026). With this number of research articles, we conduct scientometrics analysis. We applied several criteria to finalize the list of eligible publications. We ensure that from one source of publications won't include numerous articles. In the case of numerous publications only the most cited ones are selected. We apply several limitations Scopus search is the only database of the search. We excluded 2026 articles for the scientometrics analysis. For the screening of the relevant articles we follow an improved PRISMA methodology adapted from [11, 12]. The steps are as follows.

Figure 2 presents the screening flowchart to reduce the articles and exclude less relevant articles. The study selection process starts with a comprehensive search in the Scopus database. Titles, abstracts, and keywords are initially searched, which produces 5,750 records. Broad coverage of relevant literature is thereby ensured. The search is then restricted to titles. The dataset is reduced to 1,209 records, and topical relevance is improved. Additional filters are applied in the third step. Irrelevant keywords are excluded, and the search is limited to studies that address cybersecurity or "cyber securit*". Only English-language publications are retained, and the source type is restricted to journal articles. This step results in 415 records. In the fourth step, an adapted PRISMA approach is followed to guide the screening and eligibility process. In the final step, detailed examination of the manuscripts and further selection criteria are applied. This process leads to a final set of 30 studies that meet the inclusion requirements.

3 Scientometrics analysis

In this section several aspects of scientometrics analysis of the AI in mobility is discussed. We present these analysis to demonstrate the active territories and source of publications.

Figure 3 presents the progress of AI in mobility for the past decade.

The bar chart in Figure 4 compares the number of documents across selected countries or territories. India records the highest count, with a value slightly above 200, followed by China and the United States with progressively lower totals. A noticeable decline appears after the top three, as Saudi Arabia and the United Kingdom show moderate values. Canada, Undefined, South Korea, Australia, and France each report fewer than 80 documents. A skewed distribution is shown, with most documents produced by a few countries. Comparatively modest publication levels are reported for all other countries.

Figure 5 shows the distribution of documents by publication source. It highlights the journals and publication venues that contribute most frequently to artificial intelligence and mobility research.

4 Results

The study proposes a deep reinforcement learning model for traffic signal control with connected and autonomous vehicles. It improves coordination between infrastructure and vehicles and reduces waiting time significantly. Nghiem et al. [13] propose a deep-reinforcement-learning traffic-signal controller for cooperative connected and autonomous vehicles and report improved traffic efficiency in simulation. Viktor and Kiss [14] examine generational differences in the acceptance of self-driving vehicles, including the roles of trust and perceived safety. Liang et al. [15] analyze risk preferences and reference-dependent choices between autonomous-vehicle alternatives; their study informs the human-factors dimension of adoption rather than evaluating cybersecurity controls directly. It improves detection accuracy and provides transparency in decision processes. This study directly contributes to cybersecurity in AI-driven mobility systems [16].The study evaluates the combined effect of intelligent transport systems and citizen engagement on urban performance. Social support is shown as

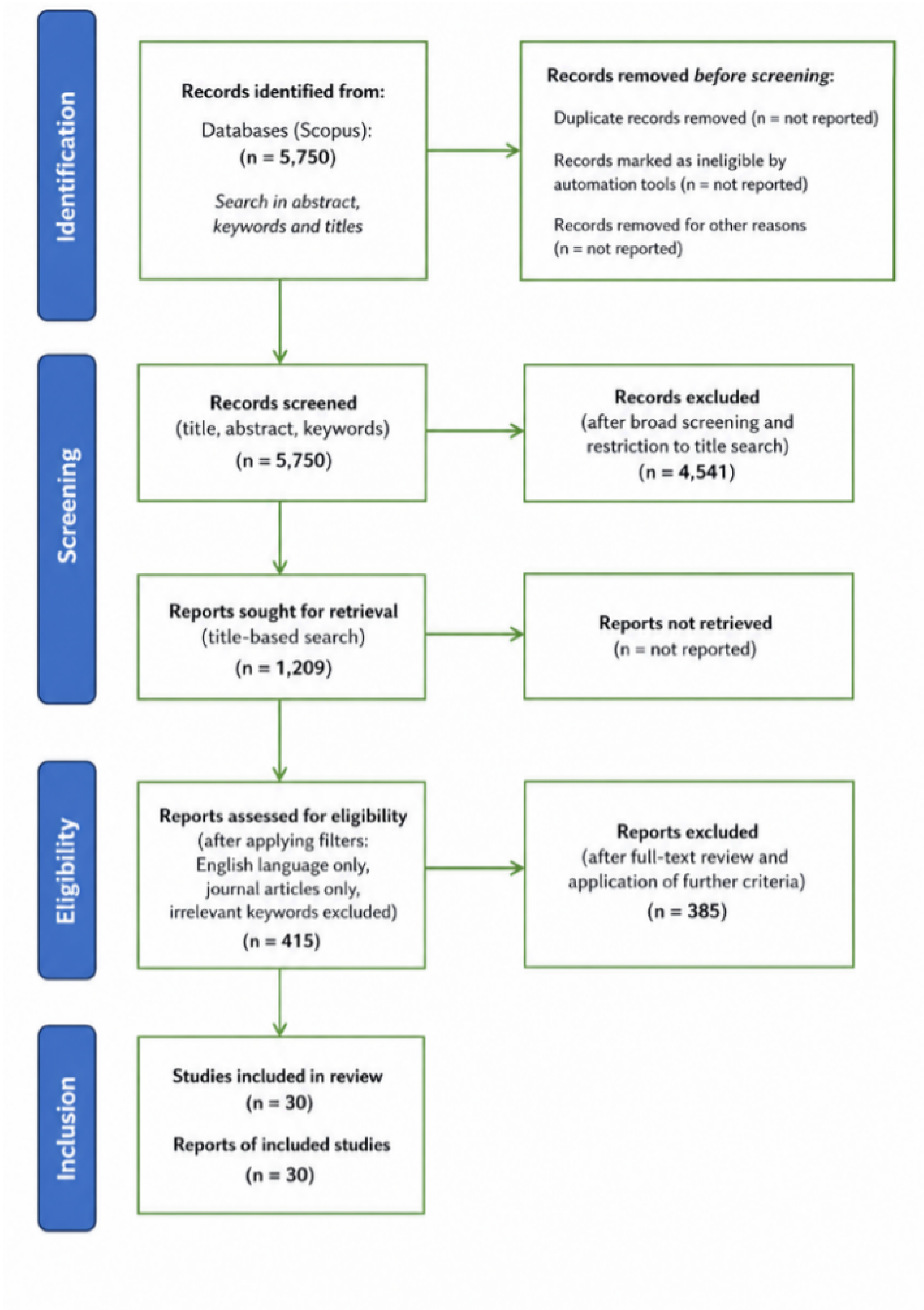

Figure 2: An improved version of PRISMA screening for AI and cybersecurity in mobility

Figure 3: The progress of AI in mobility research

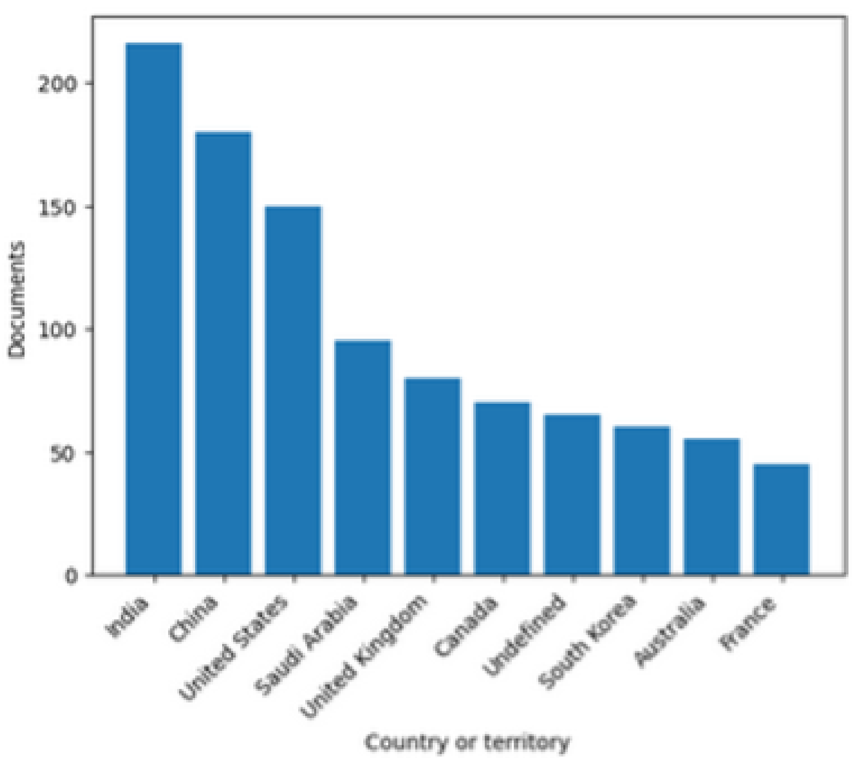

Figure 4: Number of articles by country

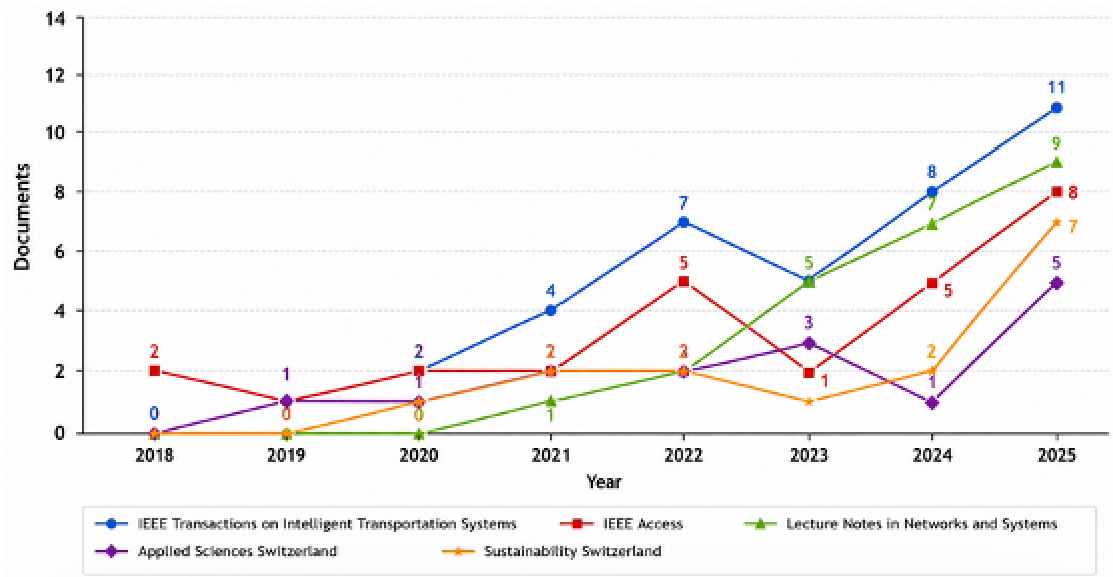

Figure 5: The number of documents by source of publications

necessary for effective technological solutions and secure mobility deployment [17]. A machine-learning model is developed for electric vehicle adoption and emission forecasts. Sustainable mobility planning is supported through data-based analysis [18]. Federated learning is reviewed as a privacy-preserving method for intelligent transportation systems. Data security and system efficiency are addressed in distributed mobility networks [19]. A graph neural network is proposed for anomaly detection in vehicular communication. Detection under dynamic traffic conditions is improved [20]. A trust-aware edge model is proposed for threat detection in IoT transport systems. Data security and communication reliability are strengthened [21]. Autonomous vehicle adoption is shown to depend on user risk preferences [15]. A generative AI method is introduced for connected-vehicle vulnerability detection. Complex security flaws are identified with high accuracy [22]. Automated smart contracts are deployed through generative AI and blockchain. Security, transparency, and service adaptability are improved [23]. Malicious VANET nodes are detected through machine-learning methods. Trust management and communication security are improved [24]. Transport resilience is supported by generative AI, but reliability and governance risks are identified. This study links AI capabilities with cybersecurity and system safety [25].The study proposes a secure design method for the Internet of Drones in transportation systems. It addresses vulnerabilities and improves risk assessment. This work supports cybersecurity in emerging mobility technologies [26].The paper presents a low-cost vehicle rebalancing method for mobility-on-demand systems. It improves efficiency and reduces waiting time. This study supports AI-based optimization in smart mobility operations [27].

Table 2. State of the art review of the results.

Reference	Year	Title	Journal / Source	Keywords
Jiang et al. [17]	2026	Modeling the synergistic impact of intelligent transport systems and citizen engagement on urban outcomes: A simulation-based analysis using artificial neural networks	Sustainable Cities and Society	Artificial neural networks; Economic growth; Intelligent transportation systems; Smart cities; Smart transport; Traffic management
Babar et al. [19]	2026	Federated learning for intelligent transportation systems: Emerging trends, challenges and future directions	Computer Science Review	Artificial intelligence; Data privacy; Federated averaging; Federated learning; Intelligent transportation systems
Ibrahim [20]	2026	Spatiotemporal Graph Neural Network-Driven Anomaly Detection for Cooperative Vehicle Messaging in Dense VANET Corridors	Transactions on Emerging Telecommunications Technologies	anomaly detection; cooperative messaging; GNN; intelligent transportation systems; spatiotemporal modeling; VANET security
Alshudukhi et al. [21]	2026	Edge Driven Trust Aware Threat Detection for IoT Enabled Intelligent Transportation Systems	Sensors	artificial intelligence; edge computing; Internet of Things; security; vehicular networks
Liang et al. [15]	2025	The effects of risk preferences on consumers' reference-dependent choices for autonomous vehicles	Risk Analysis	autonomous vehicles; discrete choice analysis; prospect theory; reference-dependent choices; risk preferences
Abiko et al. [22]	2026	GenSecure-CAEV: A generative AI framework for proactive vulnerability discovery in connected autonomous electric vehicles	Future Generation Computer Systems	Autonomous vehicles; Connected vehicles; Cybersecurity; Generative AI; Intelligent transportation systems; Large language model; Vulnerability discovery
Siddiqui et al. [23]	2026	Autonomous smart contract deployment through generative AI and Blockchain in smart urban mobility	Cluster Computing	Blockchain; Generative AI (GenAI); Guardrail; Smart cities; Smart contract; V2X
Erskine [24]	2026	Machine Learning-Based Approach for Malicious Node Security and Trust Provision in 5G-Enabled VANET	AI (Switzerland)	5G; blackhole; DoS attacks; false injection; intelligent transportation system (ITS); LightGBM Random Forest (RF); machine learning; malicious node; malicious vehicular nodes (MVN); security; sybil; trustworthiness; VANET; XGBoost
Wu et al. [25]	2026	Generative artificial intelligence and urban transport resilience: Rethinking sustainable mobility	Safety Science	Disaster risk management; Generative artificial intelligence; Large language models; Smart cities; Transport resilience; Urban governance
Marques et al. [26]	2026	Manna SafeioD: A Framework and Roadmap for Secure Design in the Internet of Drones	Applied Sciences (Switzerland)	drones; internet of drones; privacy; risk assessment; security; UAV
Viadero-Monasterio et al. [27]	2026	Low-Cost vehicle rebalancing control for an autonomous mobility on demand system	Journal of the Franklin Institute	Autonomous mobility-on-demand; Intelligent transportation systems; Rebalancing; Urban traffic; Vehicles

The table summarizes recent studies on artificial intelligence and cybersecurity in intelligent mobility systems and demonstrates the diversity of methods and applications across the field. Artificial neural networks are applied for intelligent transportation analysis and urban mobility optimization in smart city environments [17]. Federated learning is assessed as a privacy-preserving method for intelligent transport and decentralized data management [19]. Graph neural networks and trust aware edge artificial intelligence methods are used for anomaly detection, threat identification, and communication security in vehicular networks and Internet of Things based transportation systems [20, 21]. Other studies investigate human centered mobility analysis through discrete choice and risk preference models for autonomous vehicles [15]. Generative artificial intelligence and blockchain based methods are also introduced for vulnerability discovery, resilient mobility systems, and secure smart contract deployment in connected transportation infrastructure [22, 23, 25]. Machine learning methods such as LightGBM, Random Forest, and XGBoost are further applied for malicious node detection and trust management in 5G enabled VANET systems [24]. In addition, secure design approaches for the Internet of Drones and low-computational-cost vehicle rebalancing control methods demonstrate the expansion of advanced computational approaches into emerging mobility technologies and autonomous transportation services [26, 27].

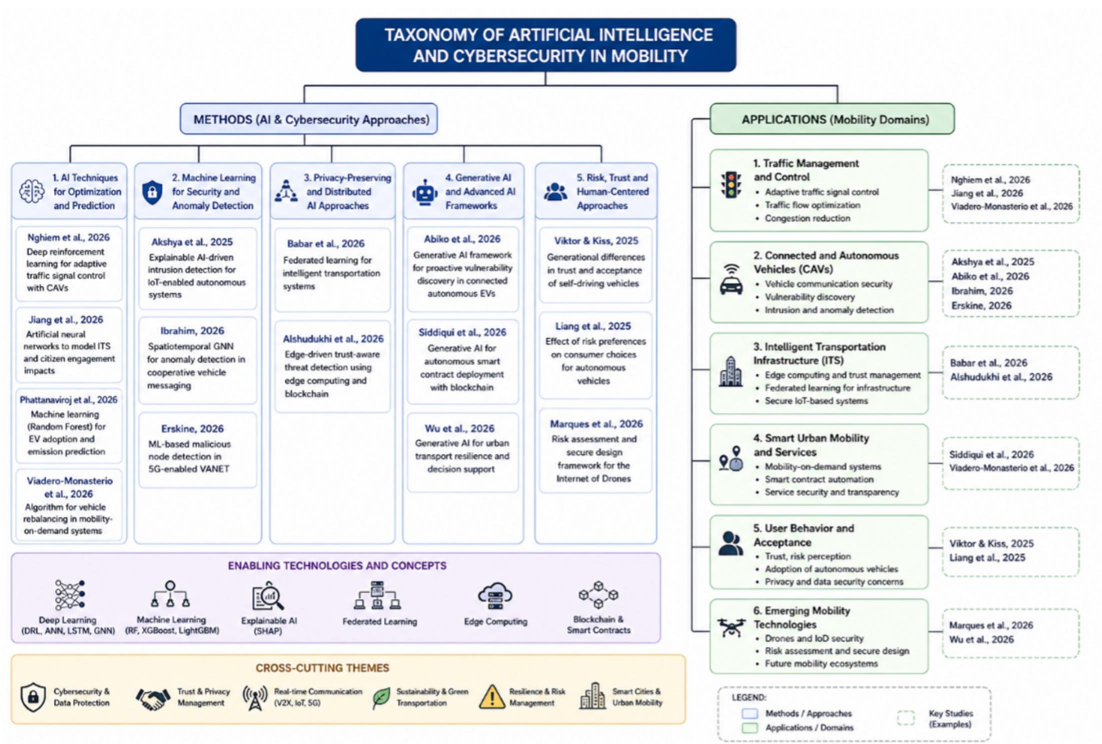

Figure 6: Taxonomy of AI and cybersecurity in mobility

Figure 6 presents a taxonomy of artificial intelligence and cybersecurity in mobility systems. Literature is organized into methods and applications. The methods dimension includes optimization and prediction techniques. Deep reinforcement learning and neural networks are applied in traffic control and performance improvement. Security methods include anomaly detection, intrusion detection systems, and graph based models. These methods address vulnerabilities in vehicular networks. Federated learning and edge computing are applied for privacy, scalability, and decentralized data protection. Generative artificial intelligence and blockchain are used for secure automation and threat detection. Human-centered and risk-based methods are applied to trust and behavioral assessment. Real-world mobility applications are included within the taxonomy. Traffic management is improved, while congestion and resource use are reduced. Secure communication and resilient operation are required for connected and autonomous vehicles. Data exchange and system coordination are supported by intelligent transportation infrastructure. Adaptive urban services are enabled through blockchain and automated systems. System adoption and cybersecurity perceptions are affected by user behavior. Internet of Drones and resilient urban systems are identified as emerging areas. Artificial intelligence and cybersecurity are required across these mobility domains. Technical methods are linked with practical applications in the proposed taxonomy. Recent methods and applications are compared in Figure 7.

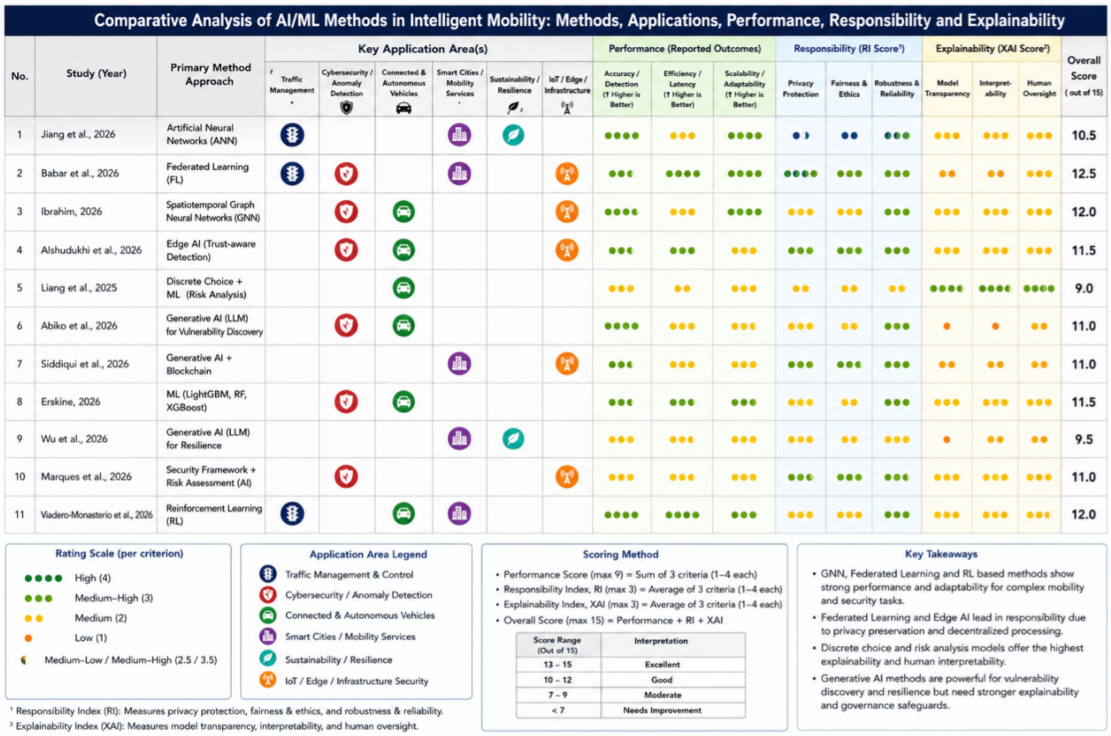

Figure 7: Comparative analysis of the methods and applications

Selected studies are classified by methods, applications, performance, responsibility, and explainability. Strong attention is given to neural networks, federated methods, reinforcement learning, and blockchain. Traffic control, anomaly detection, autonomous vehicles, smart cities, and IoT security are examined. Greater dependence on artificial intelligence is observed in transport automation and coordination. Strong adaptability is reported for graph neural networks and reinforcement methods. Privacy is improved through federated methods, while centralized data exposure is reduced. Reliable communication and threat detection are supported by edge artificial intelligence. Vulnerability detection and automated tasks are supported by generative artificial intelligence. However, limited explainability is reported for generative models. Greater interpretability is provided by discrete-choice and risk-analysis methods. Trust and governance are improved through explainable and human-supervised approaches. Balanced performance is shown by federated methods, blockchain, and explainable detection models. Security, accountability, and reliability are strengthened through these approaches. However, transparency, fairness assessment, and governance support remain limited. Responsible deployment is not ensured by technical performance alone. Explainable methods, ethical governance, standard evaluation, and secure integration are therefore required.

5 Cybersecurity

Artificial intelligence is applied across modern mobility systems and smart city infrastructure. Prediction, route selection, and coordination are supported in connected vehicles. Real-time data analysis is used to improve transport efficiency and system control. Cybersecurity risks are increased by greater digital connectivity across mobility networks. Attack surfaces are expanded by cloud platforms, sensors, and Internet of Things devices. Mobility systems are exposed to ransomware, spoofing, interception, and denial-of-service attacks. Passenger safety and transport reliability are threatened by these attacks. Secure communication and trusted data exchange are required for system stability. Artificial intelligence is used for both protection and exploitation in cybersecurity. Anomaly detection and intrusion detection are improved by machine learning. Threats are identified earlier through predictive analysis. Incident response is improved by automated systems. Privacy is preserved in distributed environments through federated learning. Edge intelligence reduces centralized data dependence. However, adversarial attacks and model poisoning remain serious risks. Sensor manipulation reduces system reliability. Generative artificial intelligence increases phishing, malware, identity fraud, and disinformation. Zero Trust architecture is increasingly applied in mobility cybersecurity. Perimeter based security is no longer sufficient. Continuous verification is required for all users and devices. Authentication and authorization are enforced for every request. Continuous validation supports secure system operation. Zero Trust improves resilience in intelligent transportation systems through identity verification. Encrypted communication, micro segmentation, and behavioral monitoring are applied. Vehicle to everything communication, cloud services, edge computing, and autonomous platforms are protected. Artificial intelligence strengthens Zero Trust through adaptive authentication and dynamic risk assessment. Real time anomaly detection is improved. Attacker movement is reduced across transportation networks. Incident spread is limited within connected systems. We observe stronger cybersecurity performance under combined AI and Zero Trust use. Future mobility systems integrate AI automation with Zero Trust principles. Secure and sustainable infrastructure is supported through this integration. Governments define regulations for AI governance and cybersecurity certification. Privacy protection and accountability are required in autonomous mobility systems. Secure by design strategies are applied in developing economies. Cybersecurity is integrated before deployment stages. Universities provide interdisciplinary education in artificial intelligence and cybersecurity. Transportation engineering, ethics, and governance are included in training programs. Specialists are prepared for emerging cyber threats.Autonomous mobility, smart cities, and six G networks increase system complexity. Explainable artificial intelligence is required for transparency and trust. Blockchain security and resilient edge intelligence are applied. Zero Trust supports cyber resilience in connected infrastructure. Public trust and operational reliability are maintained through these measures.

6 Responsible AI

Responsible AI is required in the advanced mobility systems. In fact the transportation infrastructure relies on automated decisions and real time data exchange. AI improves traffic management, coordination, energy use, and mobility prediction. However, fairness, transparency, and security remain essential for social acceptance. Human factors, governance, cybersecurity, and sustainability are underrepresented in current studies. Technical progress alone does not ensure reliable mobility systems. Biased data and unequal decisions affect service access and mobility planning. Explainability and accountability remain major concerns in mobility cybersecurity systems. Explainable intrusion detection and transparent anomaly detection are reported in studies. These methods improve trust among operators and regulators. Opaque models reduce accountability during cyber incidents and system failures. Explainable artificial intelligence supports transparency and risk assessment. Accountability is shared among developers, operators, providers, and governments. Human supervision remains required for unexpected threats and dynamic environments. Sustainability is also considered a key dimension of responsible artificial intelligence [28]. Furthermore, literature shows that artificial intelligence supports sustainable urban mobility. Traffic optimization, electric vehicle management, and emission reduction are improved. Intelligent energy coordination is also supported in transportation systems. Machine learning increases efficiency and reduces congestion in smart cities. However, AI infrastructure increases energy use and computational demand. Digital dependency also introduces operational concerns. Unequal adoption is observed across different countries. Benefits of technology remain unevenly distributed. Future mobility systems require balanced integration of innovation and resilience. Cybersecurity, governance, and sustainability must be combined. Responsible artificial intelligence supports secure and transparent transport systems. Inclusive and energy efficient mobility is required in smart cities. Public trust and long term social benefit are maintained through such systems.

7 Research Limitations

This study includes several limitations that affect interpretation of findings. Literature was retrieved only from the Scopus database which provides broad coverage, yet complete inclusions is not ensured. Scientometric analysis excludes publications from 2026. This exclusion maintains consistency in citation and trend evaluation. Strict screening criteria were applied through an adapted PRISMA approach. The final dataset was reduced to thirty studies. Relevance and quality were improved through this selection process. However, some relevant studies may have been excluded during filtering. Manuscript selection bias may also be present in the dataset. Rapid changes in artificial intelligence and cybersecurity affect research relevance. New developments may appear after the review completion. Source selection is limited to English language journal articles. Conference papers, reports, books, and white papers are excluded. Only reputable journals and publishers are selected to support research quality. This criterion improves reliability but limits coverage of recent innovations. Industrial advances, regional cases, and early technologies are therefore underrepresented. The analysis is mainly restricted to technical and scientometric aspects. Social, legal, ethical, and policy dimensions receive limited attention. Broader interdisciplinary perspectives are therefore required. Future research should use multiple databases and wider publication sources. Evidence from real-world deployment should also be included. A comprehensive understanding requires interdisciplinary and policy-oriented analysis.

8 Discussions

A growing role is assigned to artificial intelligence in secure mobility systems. Traffic control, mobility forecasts, anomaly detection, and communication efficiency are improved. Strong results are reported for deep, federated, graph-based, and reinforcement methods. Cybersecurity is required because transport depends on digital infrastructure, cloud services, and vehicle networks. Edge environments and artificial intelligence models must also be protected. A substantial rise in research output is reported over the last decade. Greater activity is recorded in digitally advanced economies. Adoption is limited in less developed regions by technical, financial, and institutional barriers. Trust is reduced when artificial intelligence decisions cannot be interpreted. Explainable methods and human oversight are therefore required for accountable security operations. Further risks are created by adversarial attacks, data poisoning, malware, and identity manipulation. Protection is therefore required for both infrastructure and artificial intelligence models. Shared cybersecurity responsibility is assigned to developers, operators, and governments. Secure architectures, regulation, system oversight, and incident response are required. Multilevel governance is supported for complex mobility ecosystems. Strong potential is shown by blockchain, federated methods, and Zero Trust architectures. Artificial intelligence adoption must be aligned with cybersecurity readiness and institutional capacity. Ethical governance, workforce preparation, and continuous evaluation are also required. Public and private cooperation should be strengthened through international standards and resilience strategies. Interdisciplinary university education and practical simulations should also be expanded. Secure, reliable, and sustainable mobility systems are supported by these measures. Artificial intelligence is confirmed as valuable for mobility efficiency, sustainability, resilience, and security. However, research is divided across isolated technical applications. Cybersecurity integration, explainability, standardization, benchmark datasets, and large-scale validation are still insufficient. Further research is required on transport, communication, and energy coordination. Ethical governance, human trust, and adversarial resilience must also be strengthened. Future digital economies, smart cities, and autonomous transport are shaped by these technologies. Transparent governance, responsible adoption, and sustained institutional cooperation are required for progress.

Conclusions

An expanded role is confirmed for artificial intelligence in mobility and cybersecurity. Traffic control, mobility forecasts, energy management, and anomaly detection are improved by machine learning. Secure communication is also supported across intelligent transportation systems. Strong research growth is identified during the last decade. Connected vehicles, smart cities, and sustainable mobility are identified as major topics. Digital infrastructure, cloud services, IoT devices, and communication networks are exposed to cyber risks. System resilience, forecast accuracy, and operational coordination are improved by artificial intelligence. However, explainability, governance, interoperability, and large-scale deployment are still constrained. Stronger links among artificial intelligence, cybersecurity, sustainability, and governance are required. Current research is divided across separate technical domains. System-level integration and benchmark datasets are considered insufficient. Further attention is required for explainable artificial intelligence and standardized cybersecurity practices. Adoption differences across countries are shaped by infrastructure and institutional capacity. Transparent models and privacy protection technologies are strongly recommended. Zero Trust principles and interdisciplinary cooperation are also required. Fairness, accountability, sustainability, and public trust should be supported by responsible artificial intelligence. Scalable cyber-resilient systems and ethical governance should be prioritized in future research. Real-world validation and secure infrastructure integration should also be prioritized.

Acknowledgments

Assistance from large language models, such as ChatGPT, is used for text refinement and grammar correction. These tools are also used for material summaries, language improvement, and structural clarification. All conceptual development, methodological design, and interpretation are conducted by the authors. Every AI-assisted output is reviewed and verified by the authors. Accuracy, originality, and academic integrity are thereby ensured. Full responsibility for the manuscript is assumed by the authors.

References

[1] D. Mitieka et al. "Smart mobility in urban areas: A bibliometric review and research agenda". In: *Sustainability* 15.8 (2023).

[2] N. Rouky et al. "Artificial intelligence applications for smart and sustainable mobility as a service concept: A systematic literature review". In: *Future Transportation* 5.3 (2025).

[3] Francesco Maria Turno and Irina Yatskiv (Jackiva). "Mobility-as-a-Service: Literature and Tools Review with a Focus on Personalization". In: *Transport* 38.4 (2023), pp. 243–262. DOI: 10.3846/transport.2023.20997.

[4] O. Vermesan et al. "Automotive intelligence embedded in electric connected autonomous and shared vehicles technology for sustainable green mobility". In: *Frontiers in Future Transportation* 2 (2021).

[5] Z. Wang et al. "Analyzing mega mobility systems in smart cities: A macro micro integration with feedback paradigm empowered by artificial intelligence". In: *Research* 8 (2025).

[6] M. Bou Abboud et al. "Optimizing mobility prediction in 5G for enhanced C V2X applications: A multidisciplinary research survey". In: *Computer Communications* 242 (2025).

[7] K. Noor Ali et al. "A mini review of the impacts of machine learning on mobility electrifications". In: *Energies* 17.23 (2024).

[8] M. A. Ali et al. "Towards 6G C-V2X Networks: A Comprehensive Survey on Mobility Management, Multi-RAT Coexistence, and Machine Learning (3M) Framework for C-ITS". In: *Electronics* 15.5, 1042 (2026). DOI: 10.3390/electronics15051042.

[9] H. Lee et al. "AI powered intelligent seaport mobility: Enhancing container drayage efficiency through computer vision and deep learning". In: *Applied Sciences* 13.22 (2023).

[10] A. Ali et al. "Federated learning for connected autonomous vehicles: Enhancing mobility, safety, and sustainability". In: *Physica Scripta* 100.7 (2025).

[11] N. Kalganov et al. "Machine learning in employment research and algorithmic management". In: *Eurasian Journal of Mathematical and Computer Applications* 13.4 (2025), pp. 110–127. DOI: 10.32523/2306-6172-2025-13-4-110-127.

[12] M. Azodinia et al. "Machine learning for pavement performance and service life prediction". In: *Eurasian Journal of Mathematical and Computer Applications* 13.4 (2025), pp. 41–52. DOI: 10.32523/2306-6172-2025-13-4-41-52.

[13] L. D. Nghiem et al. "Enhancing traffic efficiency through deep reinforcement learning-based traffic signal control with cooperative connected and autonomous vehicles". In: *Applied Sciences* 16.5, 2576 (2026).

[14] P. Viktor and G. Kiss. "Generational differences among users of self-driving vehicles". In: *World Electric Vehicle Journal* 16.12, 645 (2025).

[15] Y. Liang et al. "The effects of risk preferences on consumers' reference-dependent choices for autonomous vehicles". In: *Risk Analysis* 45.12 (2025), pp. 4157–4176.

[16] J. Akshya et al. “Explainable AI-driven intrusion detection for securing IoT-enabled autonomous transportation systems”. In: *Cluster Computing* 28.14, 884 (2025).

[17] Z. Jiang et al. “Modeling the synergistic impact of intelligent transport systems and citizen engagement on urban outcomes: A simulation-based analysis using artificial neural networks”. In: *Sustainable Cities and Society* 138, 107193 (2026).

[18] T. Phattanaviroj et al. “A novel predictive framework for green transportation and EV policy towards sustainable mobility and emission reduction”. In: *Green Technologies and Sustainability* 4.1, 100260 (2026).

[19] M. Babar et al. “Federated learning for intelligent transportation systems: Emerging trends, challenges and future directions”. In: *Computer Science Review* 61, 100952 (2026).

[20] A. Z. Ibrahim. “Spatiotemporal graph neural network-driven anomaly detection for cooperative vehicle messaging in dense VANET corridors”. In: *Transactions on Emerging Telecommunications Technologies* 37.4, e70405 (2026).

[21] K. S. Alshudukhi et al. “Edge driven trust aware threat detection for IoT-enabled intelligent transportation systems”. In: *Sensors* 26.4, 1108 (2026).

[22] A. T. Abiko et al. “GenSecure-CAEV: A generative AI framework for proactive vulnerability discovery in connected autonomous electric vehicles”. In: *Future Generation Computer Systems* 182, 108445 (2026).

[23] S. Siddiqui et al. “Autonomous smart contract deployment through generative AI and blockchain in smart urban mobility”. In: *Cluster Computing* 29.4, 215 (2026).

[24] S. K. Erskine. “Machine learning-based approach for malicious node security and trust provision in 5G-enabled VANET”. In: *AI* 7.4, 136 (2026).

[25] J. Wu et al. “Generative artificial intelligence and urban transport resilience: Rethinking sustainable mobility”. In: *Safety Science* 198, 107148 (2026).

[26] L. H. C. M. Marques and L. B. Ruiz. “Manna SafeioD: A framework and roadmap for secure design in the Internet of Drones”. In: *Applied Sciences* 16.1, 505 (2026).

[27] F. Viadero-Monasterio et al. “Low-cost vehicle rebalancing control for an autonomous mobility on demand system”. In: *Journal of the Franklin Institute* 363.2, 108333 (2026).

[28] A. Mosavi et al. “Ethical AI and the Path to Responsible and Explainable Machine Learning”. In: *International Conference on Global Research and Education*. Cham: Springer Nature Switzerland, Sept. 2025, pp. 392–401.

Vivien Csorgoova,
J. Selye University, Komarno, Slovakia

Annamaria Varkonyi-Koczy,
J. Selye University, Komarno, Slovakia;
Faculty of Engineering and Computer Science,
John von Neumann University, Kecskemet, Hungary.

Assanali Shayakhmetov,
L.N. Gumilyov Eurasian National University,
Astana, Kazakhstan
Email: `shayakhmetov_ar@enu.kz`

Berik Sabdenaliyev,
SDU University, Kaskelen, Kazakhstan

Saltanat Baipakbayeva,
Farabi University, Almaty, Kazakhstan

Received 04.02.2026, Accepted 02.06.2026 Available online 30.06.2026.