Proceedings of CONF-CDS 2026 Symposuim: Data-Centric AI Security: Securing Models, Learning Agents, and Autonomous Systems
DOI: 10.54254/2755-2721/2026.CH35101

Opportunities, Challenges and Future Prospects of Artificial Intelligence in Autonomous Driving

Yuxuan Peng

Faculty of Innovation Engineering, Macau University of Science and Technology, Macau, China
1240002298@student.must.edu.mo

Abstract. The rapid development of artificial intelligence technology has brought new momentum to the autonomous driving industry. The deep integration of these two fields has become a core direction for transformation in the transportation sector. Relying on core technologies such as environmental perception, decision-making and planning, and vehicle-infrastructure cooperation, artificial intelligence effectively enhances the operational efficiency and travel safety of autonomous vehicles. This paper takes the application of AI in the field of autonomous driving as its research object, briefly outlines the core principles of this technology's implementation, and analyzes the current development opportunities for autonomous driving by considering the scale of China's new energy vehicle industry, massive driving data, and policy and infrastructure advantages. The study finds that the large-scale popularization of autonomous driving is still constrained by multiple factors. These include not only technical bottlenecks such as poor adaptability to long-tail scenarios and unstable algorithmic decision-making in extreme situations, but also practical difficulties like lagging laws and regulations, ambiguous accident liability definitions, and imperfect data security and personal privacy protection systems. To address these issues, this paper, drawing on cutting-edge technological architectures, industry policy directions, and data management standards, proposes breaking through technical challenges via multimodal large models and Vehicle-Road-Cloud integrated architecture, and improving the governance system by revising traffic laws, unifying industry standards, and establishing a tiered data protection mechanism. The research results can provide theoretical reference and ideas for achieving safe and compliant large-scale commercial and civilian use in China.

Keywords: Automobile, Artificial Intelligence, Autonomous Driving

1. Introduction

In recent years, with the rapid development of artificial intelligence technology, the global industrial landscape has undergone unprecedented and swift changes. This brings new development opportunities for various industries, becoming the core force driving the new era of technological revolution and industrial transformation. As a typical representative of AI applied in industry, automotive autonomous driving has not only completely changed people's travel methods but is also a key scenario for the deep integration of the digital economy and real economy. Its development level is a frontier intersection and core topic of common concern for the global technology

DOI: 10.54254/2755-2721/2026.CH35101

community, industry, and policymakers. Currently, China has established significant industrial advantages in the field of new energy vehicles, and possesses massive amounts of data and relevant policy support, providing a good carrier and market environment for the implementation of autonomous driving technology. However, the full implementation of this technology still faces many challenges. At the technical level, long-tail problems in complex scenarios, system reliability, and safety remain bottlenecks. At the legal and ethical levels, regulations concerning liability definition, data security, and privacy protection are still incomplete. Based on this, this paper mainly reviews the basic principles of autonomous driving, deeply analyzes the various difficulties encountered in its development, and based on current technology and industrial trends, looks forward to future development paths, aiming to provide theoretical references for promoting the healthy development and large-scale application of autonomous driving technology in China.

2. Basic principles of AI-driven autonomous driving technology application

With the gradual optimization and development of autonomous driving technology, traditional rule-based and physical model-based techniques are gradually showing shortcomings, such as slow response, weak generalization ability, and insufficient adaptability to rare scenarios when facing today's complex, variable, and uncertain traffic environments. However, the introduction of artificial intelligence technology provides powerful capabilities for environmental perception, path planning, and behavioral decision-making for autonomous driving technology, providing technical impetus for the intelligentization of autonomous driving. The application of AI-driven autonomous driving technology mainly consists of three core parts: First, environmental perception, which utilizes multimodal deep neural networks and image processing technology to enhance the system's recognition and understanding capabilities under variable conditions such as complex road conditions, adverse weather, and dynamic obstacles. Second, path planning, which relies on reinforcement learning, evolutionary optimization, and modeling methods to plan optimal driving trajectories for vehicles in real-time that balance safety, efficiency, and executability. Third, behavior prediction and decision-making, which uses imitation learning and trajectory prediction models to accurately infer the intentions of other traffic participants and make decisions and controls close to human driving habits [1].

3. Real-world development opportunities enabled by AI in autonomous driving

3.1. New energy industry and massive data fuel provide optimal development carriers

Based on China's industrial and environmental advantages, more opportunities are provided for the development of AI-enabled autonomous driving. In 2024, China's electricity generation was 10086.9 TWh (10.08 trillion kWh), accounting for 32.3% of the global share, ranking first in the world; the USA generated 4634.8 TWh (second), and India generated 2030.2 TWh (third) [2]. This lays a solid foundation for China's development of the new energy industry and AI technology. In 2025, China's production and sales of new energy vehicles reached 16.626 million and 16.49 million units, respectively, ranking first globally for 11 consecutive years, with exports reaching 2.615 million units [3]. This has built the world's largest base of intelligent connected vehicles, and this vast industry is precisely the source of massive, high-quality data. Research shows that a car equipped with autonomous driving technology can generate 300 TB of data per year [4]. When tens of millions of such cars drive through complex scenes in developed cities and rural roads, they converge into a super data stream rich in long-tail scenarios unique globally. This is the key fuel

DOI: 10.54254/2755-2721/2026.CH35101

driving qualitative change in artificial intelligence. The performance of AI models based on deep learning is strongly correlated with the scale and quality of training data. China possesses both multimodal training data and massive electricity generation capacity as support, providing an irreplicable training environment for algorithm optimization and generalization, enabling rapid development of automotive autonomous driving technology.

3.2. Policy and infrastructure synergy create a friendly development accelerator

Forward-looking policy guidance and systematic infrastructure construction create an efficient "accelerator" for autonomous driving development. The 2026 Chinese "Two Sessions" (National People's Congress and Chinese People's Political Consultative Conference) mentioned artificial intelligence multiple times, indicating the government's emphasis on AI development. On the other hand, regarding the automotive and new energy sectors, suggestions from representatives and committee members focused on the unclear legal status and responsibility attribution of L3 and above autonomous driving, and inconsistent testing requirements and data standards across different regions, increasing duplicate investment costs for enterprises. Therefore, there is an urgent need to promote the revision of the *Road Traffic Safety Law*, and establish nationally unified test scenario databases, data interfaces, and certification standards, thereby clarifying basic rules such as "whether it can be driven on the road, who is responsible for accidents, and how data should be used according to law." Simultaneously, conditional cities should be supported in conducting L4-level pilot projects in limited scenarios, along with improving corresponding insurance, data sharing, and liability determination mechanisms, allowing high-level autonomous driving to move beyond individual case demonstrations towards replicable and scalable large-scale deployment [5]. Such policies not only drive the implementation of current roadside supporting facilities but also set construction standards for next-generation transportation infrastructure. Furthermore, the Ministry of Industry and Information Technology clearly adheres to the Vehicle-Road-Cloud integration development route [6], providing clear national-level policy guidance for autonomous driving development. This model operates through collaborative coordination between vehicle-side perception and execution, roadside environmental monitoring, and cloud-based intelligent scheduling, breaking the limitations of single-vehicle autonomous driving and becoming a core technical support for improving travel safety and efficiency [7].

4. Core difficulties in autonomous driving development

Although advances in AI have injected strong momentum into autonomous driving technology, there are still obstacles on the path to large-scale adoption. Technical reliability in extreme scenarios, lack of legal regulation, and imperfect user privacy data protection have become the three core difficulties hindering the large-scale popularization of autonomous driving. If these difficulties are not systematically addressed and resolved, they will severely restrict the process from demonstration to popularization.

4.1. Adaptability to long-tail scenarios and algorithmic decision uncertainty in extreme situations

Although deep learning-based AI large models perform excellently in routine driving scenarios, they still face significant difficulties when dealing with extremely low-probability, long-tail events. For example, current computer vision systems may cause perception and decision errors when

DOI: 10.54254/2755-2721/2026.CH35101

encountering extreme adverse weather conditions [8]. This can seriously impact road safety. Therefore, improving model robustness in long-tail scenarios is a critical issue that autonomous driving technology urgently needs to solve.

4.2. Lack of laws, regulations, and regulatory means

With the advanced development of autonomous driving technology, regulating it with existing laws and regulations is no longer realistic. The primary difficulty is the ambiguity in identifying the responsible subject. The current *Road Traffic Safety Law*context still treats the driver as the sole controllable subject. When driving authority dynamically switches between human and machine, or even enters a gray area of human-machine co-driving or system dominance, it becomes unclear whether responsibility for related autonomous driving accidents should fall on the driver, the vehicle manufacturer, or the algorithm provider. This is very detrimental to subsequent accident handling and insurance claims [9]. Road testing, demonstration operations, and accident reviews heavily rely on enterprise self-certified data such as logs, sensor records, in-vehicle video, etc. However, the collection standards, chain of custody, anti-tampering verification, and admissibility rules for such evidence are still under development. Coupled with varying access standards across regions, this creates uncertainty regarding the identification and validity of evidence in court rulings [10].

4.3. Imperfect data security and privacy protection systems

The operation of automotive autonomous driving systems heavily relies on massive, multimodal data. While AI empowers autonomous driving by amplifying the advantages of data-driven decision-making, it also significantly increases the risks of data leakage and privacy breaches. During operation, autonomous driving systems need to collect extensive multi-dimensional data, including road environment, driver behavior, vehicle status, and geographical location, inevitably involving personal private information and sensitive traffic data. If the system lacks efficient and systematic protective measures, it is highly prone to data leakage, tampering, or illegal misuse. This not only severely infringes upon user privacy but could also be maliciously exploited to interfere with or deceive autonomous driving decisions, thereby triggering major traffic safety risks [11]. Additionally, deep learning models are vulnerable to adversarial attacks. Adversarial attacks involve generating adversarial samples by adding small perturbations to input data, causing models to produce erroneous judgments. Under the influence of this technique, adversarial samples can lead to severe misjudgments through minor input perturbations, such as incorrectly identifying obstacles [1].

5. Future outlook: exploring paths towards trustworthy autonomous driving

Current autonomous driving development has entered a phase interwoven with opportunities and difficulties. To achieve reliable large-scale applications in the future, overcoming core difficulties such as long-tail scenarios, regulatory lag, and data security requires not just linear breakthroughs in single technologies but a synergistic evolution of technology pathways, system architectures, and governance systems. To address the insufficient adaptability of autonomous driving in long-tail scenarios, current efforts focus on reshaping perception and decision-making capabilities by introducing Transformer architectures and multimodal large models. The Transformer architecture allows visual perception to upgrade from simple object bounding box classification to understanding scene logic, potentially increasing the success rate of unprotected left turns by 40%. Furthermore,

DOI: 10.54254/2755-2721/2026.CH35101

using multimodal large models can improve the generalization ability of autonomous vehicles in long-tail scenarios by up to three times compared to traditional methods, with particularly significant optimization effects under extreme adverse weather [1]. Meanwhile, the 2026 National Two Sessions proposed promoting the revision of the *Road Traffic Safety Law* and establishing nationally unified test scenario databases, data interfaces, and certification standards. Support should also be given to conditional cities for conducting L4-level pilots in limited scenarios, along with improving corresponding insurance, data sharing, and liability determination mechanisms [5]. This is also an important guarantee for reassuring consumers about using autonomous driving. When it comes to data security, building a tiered data classification management system entails evaluating and categorizing data based on its importance, implementing dynamic encryption for both storage and transmission, and regulating access to user data through permission-based controls. This systematic approach effectively mitigates risks of data leakage, tampering, and unauthorized use [11]. By gradually optimizing and solving these core issues and seizing the development opportunities of the current era, autonomous driving technology can progressively achieve large-scale commercial or civilian use in the future.

6. Conclusion

The integrated development of AI and autonomous driving is reshaping modern transportation modes. It represents a typical practice of the deep integration of the digital and real economies and is a key area of competition in the global intelligent transportation industry. This paper systematically reviews the technical principles of AI empowering autonomous driving, combines domestic industry status, policy environment, and infrastructure conditions, comprehensively analyzes the current development opportunities, existing difficulties, and future development paths of the industry, presenting a complete picture of the current development landscape where opportunities and challenges coexist. Leveraging its globally leading new energy vehicle production capacity, massive vehicle driving data resources, continuously implemented supportive policies, and Vehicle-Road-Cloud integration infrastructure, China has built a uniquely advantageous development platform for the iteration and implementation of autonomous driving technology, providing the basic conditions for leapfrog development in this industry. However, it is undeniable that autonomous driving still faces significant resistance on its path to full popularization. Technologically, traditional deep learning algorithms struggle to adapt to low-probability long-tail scenarios such as extreme weather and sudden road conditions; system stability and reliability require improvement. Institutionally, current traffic laws and regulations cannot adapt to new models like human-machine co-driving or fully autonomous driving, with obvious gaps in areas such as accident liability division, road testing standards, and evidence admissibility rules. In terms of security, the massive amount of road condition, location, and user behavior data collected by autonomous driving systems carries risks of leakage, tampering, and adversarial attacks; privacy protection and data security defense systems need further strengthening. Looking ahead, the healthy development of the autonomous driving industry cannot rely on breakthroughs in a single domain but must achieve coordinated upgrades in technology, institutions, and security systems. Technologically, new-generation AI technologies represented by Transformer architectures and multimodal large models can significantly enhance vehicle scene understanding and generalization capabilities, compensating for the shortcomings of traditional algorithms. Institutionally, promoting the revision of the *Road Traffic Safety Law*, unifying national industry standards, and opening up pilot programs for high-level autonomous driving can build clear operational rules for the industry. In terms of security, implementing tiered data classification management and encryption protection strategies can solidify data and privacy

DOI: 10.54254/2755-2721/2026.CH35101

security defenses. Guided by both technological innovation and institutional improvements, autonomous driving will gradually shed its developmental constraints, continue advancing towards being safe and trustworthy, and ultimately achieve large-scale deployment, contributing to the construction of smart transportation systems and convenient travel for the public.

References

[1] Liao, Y., Wei, Y., Li, S., Luo, Y., & Liu, H. (2026). Current Status, Challenges, and Trends of AI-Assisted Unmanned Vehicles. Information and Control, pp. 1-16. https: //doi.org/10.13976/j.cnki.xk.2025.1282.

[2] Energy Institute. (2025). Statistical Review of World Energy 2025 [R]. London: Energy Institute. https: //www.energyinst.org/statistical-review/home.

[3] Zheng, X. Q. (2026). Domestic NEV Sales Reached 16.49 Million Units in 2025. Automotive Review, (2), 110-111.

[4] Chougule, A., Chamola, V., Herencsar, N., & Yu, F. R. (2026). How Safe Is Your Data in Connected and Autonomous Cars: A Consumer Advantage or a Privacy Nightmare? Jan 18. arXiv preprint arXiv: 2601.12284.

[5] Editorial Office. (2026). Standards Voices from the 2026 Two Sessions. China Standardization, (6), 6-35.

[6] Editorial Department. (2023). MIIT: Adhere to Vehicle-Road-Cloud Integrated Development Route to Promote Intelligent Connected Vehicle Industry Forward. Automobile & Parts, (11), 70.

[7] Long, Y., & Wan, K. M. (2026). Exploration of Urban Autonomous Driving Operation Practices under the Vehicle-Road-Cloud Integration Model: Based on the Chengdu Driverless Project Sample. People's Public Transportation, (10), 45-47. https: //doi-org.libezproxy.must.edu.mo/10.16857/j.cnki.cn11-5903/u.2026.10.004.

[8] Lu, K., Zhao, F., Xu, X., & Zhang, Y. (2023). An object detection algorithm combining self-attention and YOLOv4 in traffic scene. PLoS ONE, 18(5), e0285654.

[9] Sun, J. F. (2024). Challenges and prospects of AI to criminal norms: The case of automated driving systems. Zhihui Fazhi Anthology, 2, 1-17.

[10] Chen, Z., Li, J. T., Guo, H., & Xu, X. Q. (2025). A Safety Assessment Method for AI-Powered Automated Driving Systems. Chinese Journal of Automotive Engineering, 15(4), 457-467.

[11] Luo, X., & Li, Y. (2026). Application of Artificial Intelligence Technology in Automotive Autonomous Driving Systems. Times Auto, (08), 28-30.