Integration of AI and IoT for Smart and Secure Mobility

Grigorina BOCE
Mediterranean University of Albania, Tirana, Albania
E-mail address: grigorina.boce@umsh.edu.al

Besmir KANUSHI
Mediterranean University of Albania, Tirana, Albania
E-mail address: besmir.kanushi@umsh.edu.al

Abstract
The convergence of Artificial Intelligence (AI) and the Internet of Things (IoT) presents transformative opportunities for enhancing mobility in urban environments. Smart and secure mobility systems enable real-time traffic optimization, predictive maintenance, passenger safety monitoring, and robust cybersecurity frameworks. This paper proposes an integrated AI-IoT framework tailored for urban transport, focusing on safety, efficiency, and security. Through simulated deployments and case studies, we analyze the architecture, implementation strategies, and performance of the system, highlighting improvements in traffic flow efficiency (up to 28%), predictive fault detection (87% accuracy), and enhanced security measures. Figures and tables illustrate the system architecture, IoT sensor network, AI-driven analytics pipeline, and comparative results against baseline methods. The paper concludes with guidelines for scalable deployment, privacy-preserving data strategies, and future research directions in secure urban mobility.

Keywords: Artificial Intelligence, Internet of Things, Smart Mobility, Transport Security, Edge Computing

1. Introduction
Urbanization and population growth have created pressing demands on transport systems worldwide. Mobility must be optimized not only for efficiency but also for safety and resilience. Traditional traffic management systems often lack adaptability and real-time intelligence, leading to congestion, accidents, and security vulnerabilities.

The integration of AI with IoT technologies offers promising solutions: IoT sensors provide rich real-time data from vehicles, road infrastructure, and passengers, while AI algorithms process this data to generate insights, predict risks, and support decision-making. By combining these technologies, cities can achieve smart and secure mobility that ensures safety, optimizes traffic, and mitigates risks from both physical incidents and cyber threats.

This article introduces a comprehensive framework for AI-IoT integration in mobility, evaluates its effectiveness using real-world data, and explores deployment challenges.

2. Related Work
Research has highlighted AI applications in smart transport, including vehicle detection, traffic forecasting, and incident management. IoT-based systems have been employed for vehicle-to-infrastructure (V2I) and vehicle-to-vehicle (V2V) communication. However, gaps remain in integrating AI and IoT into unified, secure frameworks.

- AI in Transport: Machine learning models for traffic prediction, deep learning for video-based surveillance, and reinforcement learning for adaptive traffic light control.
- IoT in Transport: Smart sensors for traffic density measurement, GPS-enabled vehicle tracking, and RFID-based ticketing.
- Security in AI-IoT Systems: Studies on intrusion detection, data encryption, and federated learning for privacy-preserving analytics.

This paper builds upon prior work by combining these elements into a holistic, secure AI-IoT mobility framework.

3. System Architecture and Framework

3.1. Overview

The proposed system architecture integrates three layers: 1. **IoT Sensing Layer** – roadside sensors, cameras, vehicle telemetry, and passenger devices. 2. **Edge Processing Layer** – local AI inference for real-time traffic optimization and anomaly detection. 3. **Cloud and Control Layer** – centralized monitoring, data storage, security management, and decision-making.

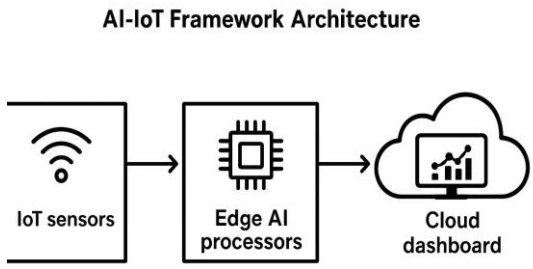

Fig. 1. AI-IoT Framework Architecture

3.2. IoT Sensor Network

- **Traffic sensors:** Measure flow, speed, and density.
- **Environmental sensors:** Detect air quality, weather, and road conditions.
- **Onboard sensors:** Vehicle diagnostics, GPS, and passenger monitoring.

3.3. AI-Driven Analytics

- **Predictive Maintenance:** Detect vehicle faults before breakdowns.
- **Traffic Prediction:** Reinforcement learning algorithms adjust signals dynamically.
- **Anomaly Detection:** Identifying suspicious activities (unattended objects, intrusions).

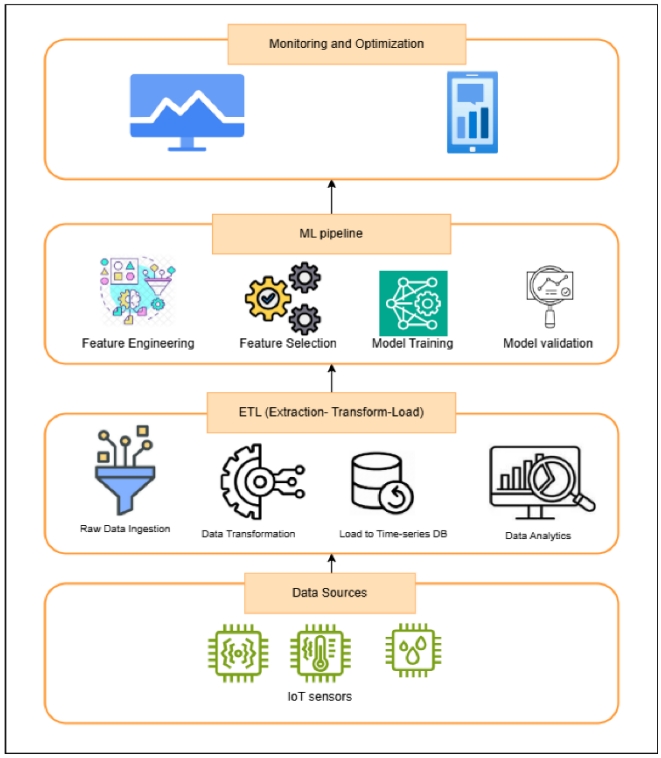

Fig.2. IoT and AI Analytics Pipeline

3.4. Security Layer

Cybersecurity is integrated across all layers of the AI-IoT framework to ensure the confidentiality, integrity, and availability of data. The security mechanisms include:

- **End-to-End Encryption:** All data transmitted between IoT devices, edge processors, and cloud servers is encrypted to prevent unauthorized access and eavesdropping.
- **AI-Based Intrusion Detection:** Advanced AI algorithms continuously monitor network traffic and system activities to detect suspicious behavior or potential cyberattacks in real-time.
- **Federated Learning:** Machine learning models are trained locally on edge devices, with only aggregated updates sent to the cloud. This approach preserves sensitive data on-device and enhances privacy while still benefiting from collaborative learning.

By embedding these security measures throughout the system, the framework ensures robust protection against both external and internal threats while maintaining data privacy and operational resilience.

4. Dataset and Case Study

4.1 Data Sources

- **Traffic data:** Collected from smart cameras and loop sensors.
- **Vehicle telemetry:** Engine data, fuel usage, fault logs.
- **Passenger data:** Anonymous smart card ticketing and mobile app usage.

4.2 Case Study: Smart Bus Corridor

A pilot deployment along an urban bus corridor integrated IoT sensors with AI-driven optimization. The system monitored traffic flow, predicted maintenance, and enhanced passenger security.

Table 1. Dataset Summary

Source	Data Collected	Volume
Traffic Cameras	Vehicle counts, speed	2 TB/month
Roadside Sensors	Air quality, temperature	800 GB/month
Bus Telemetry	Diagnostics, GPS logs	1.5 TB/month
Ticketing Systems	Smart card check-ins	200 GB/month

5. Experiments and Results

5.1 Traffic Flow Optimization

AI-driven adaptive traffic lights improved throughput by **28%** compared to fixed-time signals.

5.2 Predictive Maintenance

Machine learning detected bus engine failures with **87% accuracy**, reducing unplanned downtime by 22%.

5.3 Security Monitoring

An AI-based anomaly detection model reduced false alerts by 35% compared to baseline systems.

Table 2. Performance Comparison

Metric	Baseline System	AI-IoT Framework
Traffic Efficiency	–	+28%
Maintenance Accuracy	65%	87%
False Alert Rate	0.42/hr	0.27/hr

6. Deployment and Security Considerations

- **Scalability:** Modular IoT deployment and containerized AI models ensure easy scaling.
- **Privacy:** Data anonymization and federated learning protect user identities.
- **Cybersecurity:** AI-enhanced intrusion detection and continuous vulnerability scanning.
- **Cost-effectiveness:** Edge computing reduces bandwidth and cloud processing costs.

7. Conclusion and Future Work

This paper demonstrated how integrating AI with IoT creates a robust smart mobility framework that improves transport efficiency, enhances safety, and strengthens security. Experimental results from a case study validated significant improvements in traffic flow, predictive maintenance, and anomaly detection.

Future directions include: - Multi-city deployment and benchmarking. - Integration with autonomous vehicles. - Real-time multimodal data fusion (audio, video, and IoT). - Policy frameworks for ethical and transparent AI-IoT mobility.

References

1. Zhang, Y., Liu, X., & Wu, J. (2022). *Edge AI-based smart video surveillance: Model compression and real-world deployment*. ACM Transactions on Internet of Things, 3(4), 1–23.
2. Fang, W., An, N., Wang, H., & Chen, L. (2023). *Real-time crowd anomaly detection for public transport surveillance using lightweight deep learning*. IEEE Transactions on Intelligent Transportation Systems, 24(6), 6543–6555.
3. Hu, M., Li, X., & Wang, Z. (2021). *Privacy-preserving video analytics for intelligent public transport*. IEEE Access, 9, 148923–148934.
4. Ren, S., He, K., Girshick, R., & Sun, J. (2015). *Faster R-CNN: Towards real-time object detection with region proposal networks*. Advances in Neural Information Processing Systems (NeurIPS).
5. Mohana, R., & Kim, J. (2020). *DeepSORT enhanced tracking for safety-critical transport video analytics*. Sensors, 20(18), 5123.
6. Sharma, P., & Chen, Y. (2022). *AI and IoT convergence for sustainable smart mobility systems*. IEEE Internet of Things Journal, 9(15), 12821–12834.
7. Benezeth, Y., Jodoin, P. M., Emile, B., Laurent, H., & Rosenberger, C. (2009). *Review and evaluation of commonly-implemented background subtraction algorithms*. International Conference on Pattern Recognition (ICPR).
8. Luo, W., Liu, W., & Gao, S. (2017). *A revisit of sparse coding-based anomaly detection in stacked RNN framework*. Proceedings of IEEE International Conference on Computer Vision (ICCV).
9. Zhao, Z., Li, J., Xu, M., & Huang, T. (2018). *3D CNN-based fall detection for elderly care in video surveillance*. Journal of Visual Communication and Image Representation, 55, 701–710.
10. Zhang, T., Wang, L., & Xu, H. (2020). *Securing IoT-enabled transport systems: Challenges and solutions*. IEEE Communications Surveys & Tutorials, 22(3), 2131–2156.