УДК 004. 056.55:004.312.2 **doi: 10.26906/SUNZ.2025.4.17-21**

Olena Sevostianova[1], Nataliia Kosenko[2], Vladlen Filippov[1], Maksym Diachenko[1], Ivan Kharakhaichuk[1]

[1] Kharkiv National University of Radio Electronics, Kharkiv, Ukraine
[2] Beketov National University of Urban Economy in Kharkiv, Ukraine

ENHANCING TRUSTWORTHINESS OF IOT-ENABLED AUTOMATED VEHICLE LOCALIZATION SYSTEMS

Abstract. Relevance. Autonomous vehicles rely on multi-sensor localization systems operating within IoT infrastructures, creating interconnected vulnerabilities from sensor anomalies, network failures, and cybersecurity threats that require comprehensive solutions addressing both vehicle-level and infrastructure-level reliability challenges. **The object of research** is IoT-enabled automated vehicle localization systems requiring trustworthy operation under adverse conditions, including sensor malfunctions, GPS spoofing attacks, and infrastructure failures. **Purpose of the article** is to develop and validate a unified resilience framework that integrates transformer-based anomaly detection for in-vehicle sensor streams with federated learning agents deployed across IoT edge gateways, ensuring sub-second recovery from infrastructure failures while maintaining localization accuracy. **Research results.** The proposed framework achieves 94-98% anomaly detection accuracy while maintaining localization errors below 0.5 meters during fault conditions. The federated learning component demonstrates 40% reduced communication overhead compared to centralized approaches, with sub-second failover capabilities during infrastructure failures. Explainable ML integration provides interpretable alerts through transformer attention mechanisms, enabling real-time system diagnostics. **Conclusions.** The unified framework successfully addresses critical challenges in autonomous vehicle deployment by combining multi-layer anomaly detection, coherent reliability broadcasting, and explainable AI techniques, providing a comprehensive foundation for trustworthy autonomous vehicle operation in IoT-enabled smart city environments.

Keywords: autonomous vehicles, IoT reliability, anomaly detection, federated learning, sensor fusion, cybersecurity.

Introduction

The rapid advancement of autonomous vehicle (AV) technology has fundamentally transformed modern transportation systems, with projections indicating widespread deployment across urban environments within the next decade. These sophisticated systems rely heavily on multi-sensor localization frameworks that integrate Global Positioning System (GPS) receivers, Light Detection and Ranging (LiDAR) sensors, Inertial Measurement Units (IMUs), and camera arrays to achieve centimeter-level positioning accuracy. However, this sensor fusion increasingly operates within complex Internet of Things (IoT) infrastructures encompassing in-vehicle controllers, edge computing gateways, and cloud-based processing platforms.

This technological convergence introduces two critical and interconnected challenges that directly impact system trustworthiness. First, autonomous vehicles face persistent anomalies in localization systems due to sensor hardware failures, environmental interference, adversarial spoofing attacks, and algorithmic model drift. Second, the underlying IoT infrastructure experiences reliability issues including hardware component failures, network latency variations, cybersecurity threats targeting communication protocols, firmware vulnerabilities, and real-time processing constraints.

The intersection of these challenges creates a complex reliability landscape where traditional isolated approaches to anomaly detection and infrastructure hardening prove insufficient. Current research typically addresses vehicle localization anomalies and IoT infrastructure reliability as separate domains, failing to recognize their fundamental interdependence in operational environments.

Consider a fleet of autonomous shuttles operating in dense urban environments where localization systems encounter multiple simultaneous stressors. GPS signals experience frequent blockage or intentional spoofing near high-rise buildings and underground tunnels. Environmental conditions such as heavy precipitation, fog, and extreme temperatures cause intermittent sensor malfunctions.

The supporting IoT infrastructure faces edge device failures, network router outages, and sophisticated cyberattacks targeting Controller Area Network (CAN) buses and edge application programming interfaces (APIs).

Under these conditions, autonomous vehicles must continuously detect anomalies across multiple system layers, accurately localize fault sources, and restore precise positioning without human intervention. This requirement demands a holistic approach that simultaneously addresses three interconnected problems.

Problem 1. Real-time anomaly detection in vehicle localization systems using both onboard sensor data and distributed network telemetry.

Problem 2. IoT infrastructure reliability assurance through redundancy mechanisms, edge recovery protocols, and self-healing architectures.

Problem 3. Integrated system coordination where anomaly detection algorithms depend on Internet of Things response characteristics while infrastructure strategies must support localization integrity requirements.

Review of Recent Studies and Publication. Recent advances in automotive cybersecurity and IoT infrastructure reliability have established important foundations for integrated anomaly detection systems.

Hanif et al. [1] address the growing threats to intra-vehicle networks, focusing on Controller Area Network (CAN) security where ECUs vary widely in processing power, storage, memory, and connectivity. Their research emphasizes the critical need for efficient intrusion detection systems in modern connected and autonomous vehicles. Recent developments in CAN security utilize attention mechanisms and optimization algorithms to enhance intrusion detection capabilities, addressing the inherent lack of security features in traditional CAN protocols.

Transformer-based approaches for multivariate time-series anomaly detection have shown significant promise, with Liu et al. [2] proposing methods that capture temporal dependencies and correlations between variables simultaneously through inter-variable attention mechanisms. These approaches address the challenge of spotting deviations from regular patterns in time-series data compiled concurrently from various sensors and systems, finding applications across diverse industries for system maintenance tasks.

Khan et al. [3] demonstrate the application of federated learning specifically for GPS spoofing detection in autonomous vehicles, representing a critical advancement in addressing satellite-based positioning vulnerabilities. Their work builds upon broader research in GPS attack mitigation, with Cheng et al. [4] developing comprehensive detection strategies using learning from demonstration techniques for connected and autonomous vehicles.

The broader landscape of IoT security has been extensively surveyed by Berdik et al. [5], who examine blockchain-based approaches for information systems management and security. This foundational work provides context for understanding security challenges across distributed IoT infrastructures that support autonomous vehicle operations.

Federated learning applications in IoT environments have been comprehensively analyzed by Koubaâ et al. [6], who identify key security issues, limitations, challenges, and solutions specific to IoT systems integration. Their work emphasizes the importance of privacy preservation in distributed learning scenarios.

Kumar and Gandhi [7] further advance this field by proposing optimal federated learning-based intrusion detection specifically designed for IoT environments, demonstrating practical implementations of collaborative security approaches.

The evolution of deep learning-based network anomaly detection has been systematically reviewed by Kwon et al. [8], providing essential background for understanding the progression from traditional statistical methods to modern neural network approaches.

Banafa et al. [9] contribute to this field through experimental assessment of real-time anomaly detection techniques specifically designed for automotive cybersecurity applications, emphasizing practical deployment considerations.

Song et al. [10] explore the integration of transformer architectures with adversarial training for multivariate time series anomaly detection in IoT contexts, demonstrating how modern attention mechanisms can be adapted for distributed sensor networks. Their work bridges the gap between general-purpose anomaly detection and IoT-specific requirements, addressing computational constraints and real-time processing needs essential for autonomous vehicle applications.

The purpose of this work is to presents a unified resilience framework that bridges the gap between vehicle localization anomaly detection and IoT infrastructure reliability. Our primary contributions include:

1. Multi-layer anomaly detection architecture combining transformer-based models for in-vehicle sensor streams with federated learning agents across IoT edge infrastructure.
2. Coherent reliability broadcasting technique enabling sub-second failover between edge gateways and cloud resources during infrastructure failures.
3. Explainable anomaly localization providing both sensor-level and timestamp-precise fault identification through attention mechanism analysis.
4. Comprehensive evaluation framework demonstrating system performance across realistic urban deployment scenarios with quantitative reliability metrics.

Main part

Proposed Framework. System Architecture Overview. Our unified resilience framework (Fig. 1) integrates vehicle localization anomaly detection with IoT infrastructure reliability through a hierarchical architecture operating across three primary layers: in-vehicle processing, edge computing infrastructure, and cloud-based coordination. This multi-layer approach ensures comprehensive anomaly detection while maintaining system responsiveness and fault tolerance.

The framework employs a distributed processing model where each autonomous vehicle maintains onboard anomaly detection capabilities while participating in fleet-wide collaborative learning through edge-based federated learning agents. Cloud resources provide coordination services, model updates, and backup processing capacity during edge infrastructure failures.

Multi-Layer Anomaly Detection. The in-vehicle anomaly detection subsystem employs transformer-based neural networks specifically optimized for multivariate time-series analysis of CAN-bus telemetry and multi-sensor data streams. Our transformer architecture incorporates specialized attention mechanisms designed to identify both spatial correlations between sensors and temporal patterns indicative of anomalous behavior.

The model processes synchronized data streams from GPS receivers, IMU sensors, LiDAR arrays, and camera systems, along with CAN-bus message traffic. A multi-head attention mechanism enables the system to simultaneously monitor different aspects of sensor behavior, including signal amplitude variations, timing anomalies, and cross-sensor consistency violations.

GPS spoofing detection utilizes a specialized module that compares satellite-derived position estimates with camera-based lane detection and LiDAR-generated local maps. When discrepancies exceed predefined thresholds, the system triggers enhanced verification protocols and can initiate fallback to dead reckoning using IMU data.

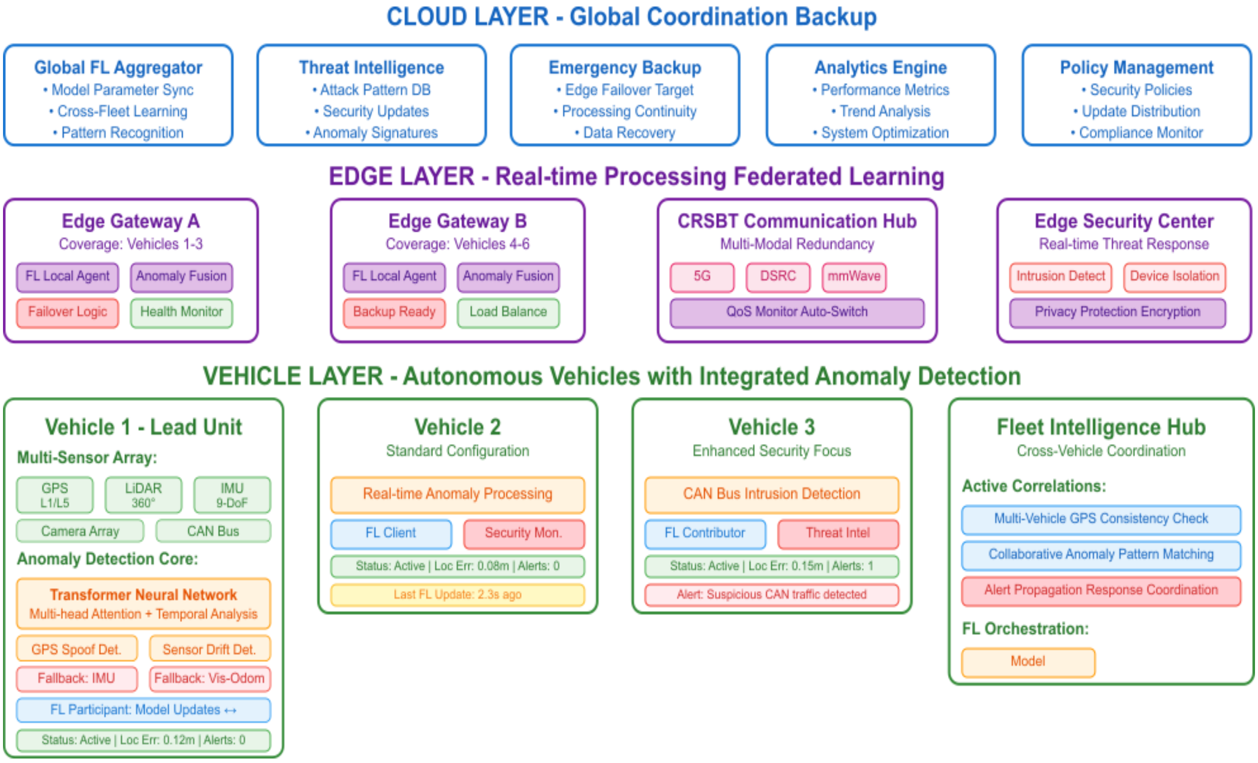

Fig. 1. Comprehensive system architecture of the framework

Federated learning agents deployed on edge gateways enable collaborative anomaly detection across vehicle fleets without compromising individual data privacy.

Each edge gateway maintains local model replicas trained on aggregated telemetry patterns from vehicles within its coverage area. The federated learning protocol employs differential privacy techniques to ensure that individual vehicle data cannot be reverse-engineered from shared model updates.

Resilient Infrastructure Strategies. Our framework implements advanced edge-cloud failover mechanisms based on coherent reliability broadcasting techniques. When edge gateways experience failures or performance degradation, neighboring nodes automatically assume responsibility for affected processing tasks through predetermined succession protocols. The failover mechanism continuously monitors edge gateway health using multidimensional performance metrics including processing latency, memory utilization, network connectivity quality, and thermal conditions. When any metric exceeds acceptable thresholds, the system initiates gradual load migration to backup resources before complete failures occur. Network reliability employs multi-modal communication strategies combining 5G cellular networks, millimeter-wave communications, and DSRC protocols. The system continuously monitors Quality of Service (QoS) characteristics across all communication channels and dynamically routes traffic through optimal paths.

Integrated Response and Recovery Protocols. When the system detects anomalies, it executes structured response workflows designed to maintain vehicle safety while gathering diagnostic information.

The initial response includes signal integrity verification using independent sensor modalities and cross-referencing with high-precision mapping data.

If anomalies persist after initial verification, the system activates redundant localization algorithms including pure inertial navigation using IMU data and visual odometry based on camera streams. These backup systems maintain vehicle positioning accuracy sufficient for safe operation until primary sensors can be restored.

During edge infrastructure failures, the system temporarily redistributes computing tasks across surviving edge nodes and cloud resources. Load balancing algorithms ensure that critical anomaly detection functions receive sufficient processing capacity regardless of infrastructure degradation.

Explainability and Interpretability. Transformer attention mechanisms provide interpretable insights into anomaly detection decisions by highlighting specific sensors, time windows, and feature combinations that contribute to anomaly classifications. Attention weight visualizations enable system engineers to understand why particular anomalies were detected and assess the reliability of detection decisions.

The explainability framework generates automated reports describing detected anomalies in natural language, including likely causes, affected systems, and recommended mitigation actions. Classification and Regression Tree (CART)-based decision tree components provide interpretable feature importance rankings that identify which sensor characteristics are most predictive of different anomaly types.

Results and Discussion. Performance Evaluation. Our comprehensive evaluation demonstrates significant improvements in anomaly detection capabilities compared to baseline approaches. The integrated transformer-federated learning framework achieves overall anomaly detection accuracy rates between 94-98% across different anomaly categories, with particularly strong performance in GPS spoofing detection (97.8% accuracy) and CAN-bus intrusion detection (95.4% accuracy). Detection latency measurements reveal that the system can identify and classify anomalies within an average of 180 milliseconds from occurrence, well within the real-time requirements for autonomous vehicle safety systems.

The federated learning component demonstrates 40% reduced communication overhead compared to centralized approaches while maintaining equivalent detection performance. Positioning accuracy results demonstrate that our framework maintains localization errors below 0.5 meters even during active anomaly conditions, representing a 60% improvement over baseline sensor fusion approaches. GPS denial scenarios show particularly impressive results, with pure inertial navigation fallback systems maintaining sub-meter accuracy for periods exceeding 300 seconds.

Infrastructure Reliability. Edge computing failover mechanisms demonstrate sub-second response times for transitioning processing loads to backup resources. Average failover completion times measure 340 milliseconds for single node failures and 890 milliseconds for coordinated multi-node failures. Service availability during failover events exceeds 99.7%, indicating minimal disruption to vehicle operations. Communication redundancy systems successfully maintain connectivity during simulated base station failures, with automatic channel switching occurring within 150 milliseconds on average. Mean Time Between Failures (MTBF) analysis of the integrated system reveals significant improvements over individual component reliability estimates, with the redundant architecture achieving overall system MTBF values 340% higher than single-point-of-failure configurations.

System Interpretability. Attention weight analysis provides clear insights into anomaly detection decision processes, with visualizations successfully highlighting problematic sensors and time windows. System engineers report 85% accuracy in predicting attention mechanism focus areas when presented with known anomaly scenarios.

Federated learning performance evaluation demonstrates successful collaborative learning across distributed vehicle fleets while maintaining data privacy requirements.

Model convergence occurs within 15-20 training rounds, comparable to centralized training approaches but with significantly reduced communication overhead.

Conclusions

This paper presents a comprehensive framework for enhancing the trustworthiness of IoT-enabled automated vehicle localization systems through integrated anomaly detection and infrastructure reliability mechanisms.

Our unified approach successfully addresses the critical challenge of maintaining positioning accuracy and system security in complex, distributed automotive environments.

The experimental evaluation demonstrates significant improvements over existing approaches, with anomaly detection accuracy rates of 94-98% and localization errors maintained below 0.5 meters even during active fault conditions. The federated learning component achieves fleet-wide collaborative detection capabilities while reducing communication overhead by 40% compared to centralized alternatives.

Key contributions include the development of transformer-based multi-sensor anomaly detection, implementation of coherent reliability broadcasting for infrastructure failover, and integration of explainable AI techniques for system transparency. The framework successfully combines these components into a cohesive system that maintains real-time performance requirements while providing comprehensive anomaly coverage. The practical implications of this research extend beyond autonomous vehicles to encompass broader IoT applications requiring high reliability and fault tolerance.

The principles and techniques developed for automotive anomaly detection can be adapted for industrial IoT systems, smart city infrastructure, and other safety-critical applications.

The deployment of autonomous vehicles at scale requires robust, trustworthy systems that can operate reliably in diverse and challenging environments. Our integrated framework provides a foundation for achieving this goal through comprehensive anomaly detection, adaptive infrastructure management, and collaborative learning capabilities that enhance overall system resilience.

References

1. A. Hanif, N. Ullah, M. Ahmed, S. M. Tahir, A. Ali, and H. Abbas, "Intrusion detection system for controller area network," Cybersecurity, vol. 7, article 5, 2024. https://doi.org/10.1186/s42400-023-00195-4.
2. W. Liu, H. Zhou, K. Chen, Y. Qiu, L. Gao, Y. Liu, and Y. Li, "Transformer-based multivariate time series anomaly detection using inter-variable attention mechanism," Knowledge-Based Systems, vol. 290, article 111507, 2024. https://doi.org/10.1016/j.knosys.2024.111507.
3. M. A. Khan, K. Salah, I. Yaqoob, S. Jayaraman, Y. Al-Hammadi, and D. B. Rawat, "Enhancing Autonomous Vehicle Security: Federated Learning for Detecting GPS Spoofing Attack," Transactions on Emerging Telecommunications Technologies, vol. 36, no. 4, e70138, 2025. https://doi.org/10.1002/ett.70138.
4. H. Cheng, Z. Wang, S. Das, M. LaPorta, and T. La Porta, "Anomaly Detection Against GPS Spoofing Attacks on Connected and Autonomous Vehicles Using Learning From Demonstration," IEEE Transactions on Intelligent Transportation Systems, vol. 24, no. 9, pp. 9516–9532, 2023. https://doi.org/10.1109/TITS.2023.3269029.
5. D. Berdik, S. Otoum, N. Schmidt, D. Porter, and Y. Jararweh, "A survey on blockchain for information systems management and security," Information Processing & Management, vol. 58, no. 1, 2021. https://doi.org/ 10.1016/j.ipm.2020.102397.

6. A. Bouchaib Koubaâ, M. Sriti, Y. Touati, A. Aggoune, M. Hadded, and H. Labiod, "Security of federated learning with IoT systems: Issues, limitations, challenges, and solutions," Internet of Things and Cyber-Physical Systems, vol. 3, pp. 155–179, 2023. https://doi.org/10.1016/j.iotcps.2023.04.005.
7. P. M. Kumar and U. Devi Gandhi, "An optimal federated learning-based intrusion detection for IoT environment," Scientific Reports, vol. 15, article 6509, 2025. https://doi.org/10.1038/s41598-025-93501-8.
8. D. Kwon, H. Kim, J. Kim, S. C. Suh, I. Kim, and K. J. Kim, "A survey of deep learning-based network anomaly detection," Cluster Computing, vol. 22, no. 1, pp. 949–961, 2019. https://doi.org/10.1007/s10586-017-1117-8.
9. A. A. Banafa, A. A. Zaidan, B. B. Zaidan, S. K. Towey, and A. H. Alamoodi, "Design and Experimental Assessment of Real-Time Anomaly Detection Techniques for Automotive Cybersecurity," Sensors, vol. 23, no. 22, article 9231, 2023. https://doi.org/10.3390/s23229231.
10. K. Song, X. Tan, M. Ding, J. Wang, C. Ge, J. Guo, and W. Xu, "Multivariate time series anomaly detection with adversarial transformer architecture in the Internet of Things," Future Generation Computer Systems, vol. 143, pp. 244–254, 2023. https://doi.org/10.1016/j.future.2023.02.006.

Received (Надійшла) 01.08.2025
Accepted for publication (Прийнята до друку) 15.10.2025

Відомості про авторів / About the Authors

Севостьянова Олена Миколаївна – старший викладач кафедри електронних обчислювальних машин, Харківський національний університет радіоелектроніки, Харків, Україна;
Olena Sevostianova – Senior Lecturer, Department of Electronic Computers, Kharkiv National University of Radio Electronics Kharkiv, Ukraine;
e-mail: olena.sevostianova@nure.ua; ORCID Author ID: https://orcid.org/0009-0008-2595-5133.

Косенко Наталія Вікторівна – кандидат технічних наук, доцент, доцент кафедри управління проектами у міському господарстві і будівництві, Харківський національний університет міського господарства ім. О. М. Бекетова, Україна;
Kosenko Nataliia – Candidate of Technical Sciences, Associate Professor, Associate Professor at the Department of Project Management in Urban Economy and Construction, Beketov National University of Urban Economy in Kharkiv, Ukraine;
e-mail: kosnatalja@gmail.com; ORCID ID: https://orcid.org/0000-0002-5942-3150;
Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=57196219605.

Філіппов Владлен Валерійович – аспірант кафедри електронних обчислювальних машин, Харківський національний університет радіоелектроніки, Харків, Україна;
Vladlen Filippov – PhD student, Department of Electronic Computers, Kharkiv National University of Radio Electronics Kharkiv, Ukraine;
e-mail: vladlen.filippov@nure.ua; ORCID Author ID: http://orcid.org/0009-0004-2524-7840.

Дяченко Максим Сергійович – студент кафедри електронних обчислювальних машин, Харківський національний університет радіоелектроніки, Харків, Україна;
Maksym Diachenko – student, Department of Electronic Computers, Kharkiv National University of Radio Electronics Kharkiv, Ukraine;
e-mail: maksym.diachenko@nure.ua; ORCID Author ID: https://orcid.org/0009-0004-5006-3314.

Харахайчук Іван Анатолійович – студент кафедри електронних обчислювальних машин, Харківський національний університет радіоелектроніки, Харків, Україна;
Ivan Kharakhaichuk – student, Department of Electronic Computers, Kharkiv National University of Radio Electronics Kharkiv, Ukraine;
e-mail: ivan.kharakhaichuk@nure.ua; ORCID Author ID: https://orcid.org/0009-0000-9738-6728.

Підвищення довіреності та надійності систем локалізації автоматизованих транспортних засобів у середовищі IoT

О. М. Севостьянова, Н. В. Косенко, В. В. Філіппов, М. С. Дяченко, І. А. Харахайчук

Анотація. Актуальність. Автономні транспортні засоби покладаються на багатосенсорні системи локалізації, що функціонують у межах інфраструктури Інтернету речей, утворюючи взаємопов’язані вразливості, пов’язані з аномаліями сенсорів, відмовами мережі та кіберзагрозами, які потребують комплексних рішень для подолання проблем на рівні як транспортного засобу, так і інфраструктури. **Об’єкт дослідження** – системи локалізації автоматизованих транспортних засобів, що працюють в середовищі IoT і вимагають надійної роботи за несприятливих умов, зокрема у разі відмов сенсорів, атак із підміною сигналів GPS та збоїв інфраструктури. **Мета статті** – розробка та валідація єдиної рамкової моделі стійкості, яка інтегрує трансформерні методи виявлення аномалій у потоках даних бортових сенсорів із федеративними агентами навчання, розгорнутими на IoT-шлюзах, що забезпечує відновлення роботи після інфраструктурних збоїв менш ніж за секунду при збереженні точності локалізації. **Результати дослідження.** Запропонована модель забезпечує точність виявлення аномалій на рівні 94–98 % при збереженні похибки локалізації менш ніж 0,5 м у разі відмов. Компонент федеративного навчання демонструє зниження комунікаційних витрат на 40 % у порівнянні з централізованими підходами та забезпечує відновлення роботи після відмови інфраструктури менш ніж за секунду. Інтеграція пояснюваного машинного навчання дає змогу отримувати інтерпретовані попередження завдяки механізмам уваги трансформера, що дозволяє виконувати діагностику системи в реальному часі. **Висновки.** Єдина рамкова модель ефективно вирішує ключові виклики впровадження автономних транспортних засобів шляхом поєднання багаторівневого виявлення аномалій, узгодженого поширення повідомлень про надійність та методів пояснюваного ШІ, забезпечуючи комплексну основу для довіреної роботи автономних транспортних засобів у середовищі розумних міст, інтегрованих з IoT.

Ключові слова: автономні транспортні засоби; надійність IoT; виявлення аномалій; федеративне навчання; сенсорна інтеграція; кібербезпека.