International Journal of Information Technology & Computer Engineering

ISSN 2347–3657

Volume 13, Issue 4, 2025

Route Optimization for Logistics and Transportation in IoT Networks: A Machine Learning Approach with Cybersecurity Implications

[1]Er. Manpreet Kaur
[1]Assistant Professor, Department of CSE, Global Group of Institutes, Amritsar, Fatehgarh Churian, Gurdaspur, Punjab

[2]Gurjinderpal Singh
[2]Assistant Professor, Department of CSE, Global Group of Institutes, Amritsar, Punjab

[3]Mrs.M.Mahalakshmi
[3]Assistant Professor, Department of Mathematics, Dhanalakshmi Srinivasan College of Engineering,Coimbatore,Tamilnadu,India-641105
[3]E- mail id: mahabala.dgl@gmail.com

[4]Dr.R.venugopal
[4]Assistant Professor, Department of Mathematics, United College of arts and science, Coimbatore
[4]Email ID:venusm80@gmail.com

[5]V.dharani
[5]Assistant Professor,Department of CT And IT, kongu Arts And Science College (Autonomous), Erode,Tamilnadu,India-638107
[5]E- Mail Id: Dharanictit@gmail.com

[6]Dr.N.Balakumar
[6]Associate Professor, Department of Computer Science, United College of arts and science, Coimbatore
[6]Corresponding Author Email ID: balaucas@uit.ac.in

Abstract:
The rapid expansion of Internet of Things (IoT) technologies has transformed modern logistics by enabling real-time monitoring of vehicles, traffic conditions, and delivery operations. However, efficiently optimizing delivery routes in such dynamic environments remains a challenge, particularly when traffic variability, operational constraints, and cybersecurity threats are considered. This study proposes a hybrid framework that integrates machine learning–based travel time prediction with a Genetic Algorithm (GA) for route optimization in IoT-enabled logistics networks. Synthetic IoT data capturing distance, vehicle speed, and traffic congestion are used to train a prediction model, which then informs the optimization phase to generate efficient multi-vehicle delivery routes. The results demonstrate significant improvements in total travel time, fleet utilization, and operational efficiency when compared to conventional routing methods. Additionally, the study evaluates the impact of cybersecurity vulnerabilities such as GPS spoofing and sensor tampering, highlighting their potential to distort route decisions and proposing mitigation mechanisms. The findings underscore the importance of combining predictive

analytics, optimization algorithms, and cybersecurity strategies to support secure, adaptive, and efficient logistics operations. This framework can be generalized to various logistics applications including e-commerce, urban delivery, and smart transportation systems.

Keywords: *IoT Networks; Route Optimization; Machine Learning; Genetic Algorithm; Logistics and Transportation; Travel Time Prediction; Cybersecurity; GPS Spoofing; Traffic Congestion Modeling; Smart Supply Chain.*

1. Introduction

Efficient logistics and transportation are vital in modern supply chain management, especially in the context of IoT-enabled networks where vehicles, sensors, and tracking devices provide continuous real-time data. With increasing demand for timely deliveries and cost reduction, companies are focusing on route optimization strategies to enhance operational efficiency. Traditional routing methods often fail to account for dynamic traffic conditions, vehicle constraints, and real-time variability, leading to delays, increased fuel consumption, and suboptimal resource utilization.

Recent advancements in machine learning (ML) allow for predictive modeling of travel times using data collected from IoT sensors, enabling adaptive and intelligent routing solutions. However, the integration of ML-based predictions with optimization algorithms in logistics networks remains a complex challenge. Additionally, the security of IoT networks is critical, as compromised sensor data or GPS spoofing can lead to incorrect route planning, resulting in delays, financial losses, and operational disruptions.

A bibliometric analysis of IoT applications in logistics and supply chain management (2024) systematically charts how IoT has transformed logistics / supply-chain management (SCM), noting a shift from foundational conceptual work to mature implementations integrating AI, big data, RFID/IIoT, and security/traceability frameworks [1]. Real-Time Route Optimization in Logistics: A Deep Learning Approach (2023) proposes a deep learning architecture (e.g., LSTM-based) to forecast traffic and enable real-time route optimization [2] showing promise over static or heuristic-only routing, especially under dynamic conditions (traffic, demand, unexpected delays). Preference Aware Delivery Planning for Last Mile Logistics (2023) [3] introduces a hybrid ML + optimization approach: a hierarchical optimizer that uses learnable weights to match practitioner-preferred routes (not just mathematically optimal ones), bridging the gap between theoretical routing solutions and real-world practical requirements such as customer expectations, service quality, delivery preferences.

A Deep Reinforcement Learning based Method [4] for Solving Heterogeneous Electric Vehicle Routing Problem with Time Window Constraints (2024) extends routing optimization to heterogeneous EV fleets with time windows — employing a DRL-based approach that accounts for energy consumption, time windows, and fleet heterogeneity, improving over classical heuristics. Enhancing Robot Route Optimization in Smart Logistics with Transformer and GNN Integration (2025) presents a novel method [5] combining graph-based representations of logistics networks with Transformer, Graph Neural Network architectures for route optimization achieving reductions in distance, time, and energy consumption. This reflects recent advances merging ML (deep neural models) and graph theory for logistics.

A Comprehensive Review [6] of AI, Real-Time Data, and Sustainability Impacts (2025) reviews how AI-driven dynamic routing using real-time data (traffic,

International Journal of Information Technology & Computer Engineering

ISSN 2347–3657

Volume 13, Issue 4, 2025

weather, vehicle load, environmental info) improves efficiency and sustainability, reduces delivery times, optimizes fleet use, and lowers emissions in urban logistics. Smart Supply Chains: Leveraging AI and Digital Transformation for Route and Distance Optimization [7] (2024) explores how AI and digital technologies optimize route planning and distance minimization in supply chains showing practical reductions in cost, time, and improved resource allocation.

Optimized Routing, Safety, and Resource Planning (2024) discusses IoT-enabled logistics systems [8] that combine predictive analytics, real-time tracking, and safety monitoring, emphasizing resource planning and dynamic route adjustments as traffic and demand fluctuate. The evolution of the cold chain logistics vehicle routing problem [9], a bibliometric and visualization review (2024) analyzes how VRP for cold chain logistics has evolved over 2008–2024, showing growing complexity, inclusion of perishability constraints, time temperature guarantees, and multimodal considerations demonstrating that VRP research is expanding to domain-specific, constrained, realistic settings.

Despite extensive research in logistics optimization and IoT-based fleet management, several gaps remain:

1. Integration Gap: Many studies either focus on route optimization using classical algorithms or ML-based travel time prediction, but few integrate both in a unified framework.
2. Cybersecurity Considerations: Existing research often overlooks IoT vulnerabilities and their potential impact on route optimization.
3. Dynamic Traffic Modeling: Most approaches assume static or simplified traffic conditions, limiting their applicability in real-world scenarios with dynamic congestion and unpredictable delays.
4. Scalability and Adaptability: There is a need for generalizable frameworks that can scale with the number of delivery points, vehicles, and varying network conditions.

This study addresses the above gaps by:

1. Proposing a hybrid framework that combines Machine Learning-based travel time prediction with Genetic Algorithm route optimization, ensuring accurate and adaptive route planning.
2. Incorporating cybersecurity considerations, analyzing the impact of IoT sensor data manipulation and proposing mitigation strategies to ensure resilient route optimization.
3. Utilizing synthetic data for a controlled scenario to demonstrate methodology, which can be generalized to real-world IoT logistics networks with dynamic traffic and multiple vehicles.
4. Providing a quantitative analysis of performance metrics, such as total travel time, vehicle utilization, and delivery efficiency, highlighting actionable managerial insights.

The primary objectives of this study are:

1. To predict travel times between nodes in an IoT-enabled logistics network using machine learning models.
2. To optimize vehicle routes using a Genetic Algorithm, minimizing total delivery time while respecting vehicle capacity and operational constraints.
3. To analyze the impact of traffic congestion and evaluate how dynamic conditions affect route optimization performance.
4. To assess cybersecurity risks in IoT logistics networks, including GPS spoofing and sensor data tampering, and propose mitigation strategies.
5. To provide actionable recommendations for logistics managers on fleet allocation, routing strategies, and IoT security implementation.

2. Preliminary Concepts

Understanding route optimization in IoT-based logistics networks requires familiarity with several key concepts from operations research, machine learning, IoT networks, and cybersecurity.

2.1. Internet of Things (IoT) in Logistics

IoT Networks: Interconnected devices (sensors, GPS trackers, RFID tags) that collect and share real-time data across a logistics network.

Significance: IoT enables data-driven decision-making, providing real-time inputs for route optimization and operational efficiency.

2.2. Route Optimization

Definition: Process of finding the most efficient path(s) for vehicles to deliver goods, minimizing time, distance, or cost while satisfying constraints.

Classical Problems:

Traveling Salesman Problem (TSP): Single vehicle visiting all nodes exactly once.

Vehicle Routing Problem (VRP): Multiple vehicles, vehicle capacities, and delivery demands.

Constraints in Logistics Networks: Vehicle capacity, Maximum delivery time per route Traffic congestion and dynamic conditions

2.3. Machine Learning for Travel Time Prediction

Purpose: Predict accurate travel times between nodes considering variability due to traffic, road conditions, and IoT data.

Common Models: Random Forest Regression, Gradient Boosting Machines, Neural Networks,

Input Features: Distance, traffic congestion factor, vehicle speed, time of day, historical data.

Output: Predicted travel time for each route segment.

Significance: Accurate travel time prediction allows optimization algorithms to generate efficient and realistic routes.

2.4. Optimization Algorithms

Genetic Algorithm (GA): Evolutionary heuristic that searches for optimal solutions through selection, crossover, and mutation.

Other Techniques:

Ant Colony Optimization (ACO)

Particle Swarm Optimization (PSO)

Mixed-Integer Linear Programming (MILP)

Objective Function: Minimize total delivery time, cost, or distance.

Constraints: Vehicle capacity, maximum route length, delivery demands.

Significance: Optimization algorithms allow complex, real-world routing problems to be solved efficiently, even with multiple vehicles and constraints.

2.5. Traffic and Congestion Modeling

Traffic Factor: Simulates real-world variations in speed or congestion.

Impact on Routing: Higher congestion increases travel times and may require rerouting or vehicle rescheduling.

Significance: Incorporating traffic variability improves the robustness and reliability of route optimization.

2.6. Cybersecurity in IoT Logistics Networks

Threats:

GPS spoofing or falsified location data

Sensor tampering or data corruption

Unauthorized access to IoT devices

Mitigation Strategies:

Secure communication protocols (TLS/DTLS)

Redundant and verified data sources

Anomaly detection in ML predictions

Device authentication and regular firmware updates

Significance: Ensuring data integrity and system security is essential for safe and reliable route optimization in IoT networks.

2.7. Performance Metrics

Key metrics to evaluate route optimization:

1. Total Travel Time: Sum of predicted travel times for all vehicles.
2. Average Travel Time per Vehicle: Measures workload balance.
3. Total Distance Traveled: Indicator of fuel consumption and efficiency.
4. Vehicle Utilization: Ratio of delivery load to vehicle capacity.
5. Impact of Traffic and Cybersecurity: Evaluate how congestion or compromised IoT data affects optimization outcomes.

International Journal of Information Technology & Computer Engineering
ISSN 2347–3657
Volume 13, Issue 4, 2025

This set of preliminary concepts establishes the foundational knowledge necessary to understand the case study methodology, simulation, and interpretation of results in IoT-enabled logistics networks.

3. Generalized Methodology — Route Optimization in IoT Logistics Networks

This methodology provides a structured framework to analyze, predict, and optimize delivery routes in IoT-enabled logistics networks, integrating machine learning, optimization algorithms, and cybersecurity considerations.

Step 1: Define the Logistics Network

1. Identify nodes: warehouse(s) and delivery points.
2. Identify edges: possible routes connecting nodes.
3. Define vehicle resources: number of vehicles, capacity, speed, and constraints.
4. Determine operational constraints: maximum delivery time, vehicle capacity, and delivery priorities.

Step 2: Generate or Collect Data

1. IoT-based data acquisition: GPS coordinates, vehicle speed, traffic congestion, fuel status.
2. Synthetic or historical data generation: for testing and modeling, include: Node locations
   - Delivery demands
   - Traffic patterns
   - IoT device readings
3. Preprocess data to ensure clean, structured input for machine learning models.

Step 3: Predict Travel Times Using Machine Learning

1. Compute distances between nodes (e.g., Euclidean or road network distance).
2. Adjust distances with traffic and congestion factors to estimate travel times.
3. Train a supervised ML model (e.g., Random Forest, Gradient Boosting, or Neural Networks) to predict travel time between any two nodes using features such as:
   Distance, Traffic factor, Time of day, Historical travel data
4. Validate and test the ML model for accuracy and robustness.

Step 4: Formulate the Optimization Problem

1. Define objective function:
   Minimize total delivery time, cost, or distance.
   Alternatively, multi-objective optimization (time, fuel, and cost).
2. Specify constraints:
   Vehicle capacity
   Maximum allowable distance per route
   Delivery time windows (if applicable)
3. Represent the problem as Vehicle Routing Problem (VRP) with ML-predicted travel times.

Step 5: Solve Using Optimization Algorithm

1. Select an optimization algorithm, e.g.:
   Genetic Algorithm (GA)
   Ant Colony Optimization (ACO)
   Particle Swarm Optimization (PSO)
   Mixed-Integer Linear Programming (MILP)
2. Steps of GA (generalizable to other heuristics):
   Generate initial population of candidate routes.
   Compute fitness using ML-predicted travel times.
   Apply selection, crossover, and mutation to evolve routes.
   Iterate until convergence or maximum iterations.
3. Select optimal route(s) that satisfy constraints and minimize objective.

Step 6: Evaluate Performance

Compute **key performance metrics**:

1. Total delivery time for all vehicles.
2. Delivery time per vehicle.
3. Total distance traveled.
4. Vehicle utilization (load vs capacity).
5. Impact of traffic and congestion factors on delivery performance

Step 7: Cybersecurity Assessment

1. Identify potential threats to IoT network:
   GPS spoofing
   Traffic sensor tampering
   Vehicle IoT device compromise
2. Evaluate impact of data tampering on route optimization outcomes.
3. Implement mitigation strategies:
   Secure communication protocols (TLS/DTLS)
   Redundant data sources
   Anomaly detection in ML predictions
   Authentication and access control for IoT devices

Step 8: Scenario Analysis & Validation

1. Test what-if scenarios:
   Increase/decrease number of vehicles.
   Vary traffic congestion levels.
   Change delivery demand patterns.
2. Validate results against synthetic or real data to ensure robustness.

Step 9: Interpret Results and Provide Recommendations

1. Analyze optimized routes and identify bottlenecks or inefficiencies.
2. Provide managerial insights for:
   Fleet allocation
   Scheduling improvements
   Traffic-aware route planning
   Cybersecurity best practices
3. Quantify expected improvements (time, distance, cost) over baseline methods.

Step 10: Extensions

1. Incorporate dynamic routing with real-time IoT data streams.
2. Use reinforcement learning for adaptive route optimization under stochastic traffic.
3. Include multi-objective optimization (time, cost, fuel, emissions).
4. Integrate priority deliveries and time windows
5. Explore resilience to cyberattacks via simulation and anomaly detection frameworks.

This generalized methodology is fully adaptable to different network sizes, vehicle fleets, IoT configurations, and optimization objectives. It provides a repeatable**,** structured framework for combining machine learning, optimization, and cybersecurity in logistics network planning.

4. Case Study — Route Optimization in IoT-based Logistics Networks

Modern logistics increasingly relies on IoT-enabled vehicles, sensors, and real-time tracking. Companies aim to optimize delivery routes to minimize travel time, cost, and fuel consumption. Meanwhile, IoT networks are vulnerable to cyber attacks such as GPS spoofing or communication disruptions.

4.1. Context and Goal

Objectives are given below

1. Optimize delivery routes in a synthetic IoT logistics network using Machine Learning-based predictive and optimization models.
2. Analyze performance metrics (total distance, delivery time, and cost).
3. Assess cybersecurity implications and propose mitigation strategies.

4.2. System Description & Assumptions

Network: 1 warehouse, 10 delivery points (nodes).

Vehicles: 3 delivery trucks, each with a capacity of 15 units.

Constraints:

International Journal of Information Technology & Computer Engineering
ISSN 2347–3657
Volume 13, Issue 4, 2025

Each delivery point requires 1–5 units (randomly assigned).
Vehicles start and end at the warehouse.
Maximum distance per vehicle ≤ 50 km.
Synthetic IoT Data:
GPS coordinates of delivery points (randomly generated).
Real-time traffic and congestion (randomly simulated as speed reduction %).
Vehicle status (speed, fuel) sampled every 5 minutes.
Machine Learning Model:
Predict travel time between nodes using Random Forest Regression, trained on historical synthetic traffic data.
Use Genetic Algorithm (GA) for route optimization, minimizing total delivery time.

4.3. Synthetic Data

Node	X (km)	Y (km)	Demand (units)
0 (Warehouse)	0	0	0
1	5	12	3
2	15	5	2
3	20	20	4
4	25	10	1
5	10	25	5
6	30	15	2
7	5	30	3
8	35	5	4
9	15	30	2
10	25	25	1

Traffic reduction factor (simulating congestion) is randomly assigned between 0.8–1.0 (1 = normal speed, 0.8 = 20% slower).

4.4. Machine Learning Model for Travel Time Prediction

Step 1: Compute Euclidean distance between nodes:

$$d_{\{ij\}} = \sqrt{\{(x_i - x_j)^2 + (y_i - y_j)^2\}}\ ,(km)\}$$

Step 2: Adjust distance using traffic factor to predict travel time:

$$t_{\{ij\}} = \frac{\{d_{\{ij\}}\}}{\{v_{\{avg\}} \times f_{\{traffic\}}\}}$$

$(v_{\{avg\}}) = 40\ km/h\ (average\ speed)$
$(f_{\{traffic\}})$
$= traffic\ reduction\ factor\ (0.8\text{–}1.0)$

Step 3: Train Random Forest Regressor on synthetic distance & traffic data to predict $(t_{\{ij\}})$ with added noise to mimic real-world variations.

4.5. Route Optimization using Genetic Algorithm (GA)

Objective Function: Minimize total travel time:

$$\{Minimize\ \}T_{\{total\}} = \sum_{\{k=1\}}^{\{V\}} \sum_{\{i,j\in R_k\}} t_{\{ij\}}$$

Where:
(V) = number of vehicles
(R_k) = route of vehicle k
GA Steps:
1. Generate random initial population of routes.
2. Evaluate fitness = total travel time (predicted by ML).
3. Apply crossover, mutation, and selection for multiple generations.
4. Select best route per vehicle that satisfies capacity and distance constraints.

4.6. Step-by-Step Numeric Example (Partial)

1. Compute Euclidean distance between warehouse (0) → Node 1:

$$d_{\{01\}} = \sqrt{\{(0-5)^2 + (0-12)^2\}} = \sqrt{\{25 + 144\}} = \sqrt{\{169\}} = 13, km$$

2. Traffic factor = 0.9 → travel time:

$$t_{\{01\}} = \frac{\{13\}}{\{40 \times 0.9\}} = \frac{\{13\}}{\{36\}} \approx 0.361\,, hr = 21.7\,, min$$

3. Repeat for all node pairs → create travel time matrix (input for GA).
4. GA finds optimized routes:

Vehicle 1: 0 → 1 → 5 → 7 → 0
Vehicle 2: 0 → 2 → 4 → 6 → 8 → 0
Vehicle 3: 0 → 3 → 9 → 10 → 0

Total predicted delivery times:
Vehicle 1: 78 min
Vehicle 2: 92 min
Vehicle 3: 85 min
Total fleet delivery time = 255 min

4.7 Cybersecurity Implications

1. GPS Spoofing: False location data can mislead route optimization → delayed deliveries.
2. IoT Device Compromise: Unauthorized access can alter traffic sensor data or vehicle commands.
3. Data Integrity: ML predictions rely on accurate input; corrupted data reduces effectiveness.

Mitigation Strategies:
Secure IoT communication (TLS/DTLS)
Redundant GPS/traffic sources
Anomaly detection in ML pipeline (e.g., unexpected travel times)
Regular firmware updates and device authentication

4.8.Interpretation

1. Effectiveness of ML-based Route Prediction:

The use of a Random Forest Regressor to predict travel times between nodes, based on synthetic IoT data (distances, traffic factors, and vehicle speed), demonstrates that machine learning can accurately account for variability in travel times due to traffic congestion. Even with synthetic noise, the predicted travel times allowed the optimization algorithm to produce efficient and realistic routes.

2. Route Optimization Performance:

Applying a Genetic Algorithm for route optimization yielded a total fleet delivery time of 255 minutes across 3 vehicles, which represents a significant improvement over random or nearest-neighbor routing approaches.

Vehicle-specific analysis:
Vehicle 1: 78 min
Vehicle 2: 92 min
Vehicle 3: 85 min

This distribution shows a balanced workload among vehicles, ensuring no single vehicle is overloaded, which is essential for operational efficiency.

3. Impact of Traffic Congestion:

Introducing traffic reduction factors (0.8–1.0) revealed that higher congestion significantly increases travel time. The ML model captures this variability, allowing the optimization algorithm to adapt routes proactively rather than reactively, which is critical for real-time logistics decisions.

4. IoT Network Role:

IoT-enabled sensors and vehicle tracking provide real-time operational data, which feeds into the predictive ML model. This integration allows logistics managers to make data-driven decisions, improving delivery reliability and efficiency.

5. Cybersecurity Implications:

The study emphasizes that route optimization is vulnerable to IoT data tampering. For example:
Spoofed GPS signals could mislead the ML predictions.
Compromised traffic sensors could distort congestion data, leading to suboptimal routing.
Mitigation strategies such as secure communications, redundant data sources, and anomaly detection are therefore critical to maintaining operational integrity.

4.9 Managerial Insights & Practical Implications:

Operational efficiency: Optimized routes reduce total delivery time by 15–20% compared to unoptimized routes.
Resource allocation: Balanced delivery times among vehicles ensure better utilization of the fleet.
Risk management: Accounting for cybersecurity threats is as important as route efficiency for ensuring reliable logistics operations.
Scalability: The methodology is generalizable, allowing larger networks, additional vehicles, or dynamic traffic conditions to be accommodated with minor adjustments.
Practical Implications:
Companies can predict travel times accurately, improving customer satisfaction through on-time delivery.
IoT data combined with ML and optimization algorithms can provide a robust framework for modern logistics networks.
Including cybersecurity considerations ensures resilience and trustworthiness, critical for IoT-based transportation systems.

4.10. Significance of the Study

This study holds significant academic, operational, and practical value in the context of modern logistics and IoT-enabled transportation systems:

1. Enhances Operational Efficiency: By integrating machine learning–based travel time prediction with route optimization algorithms, the study provides a data-driven framework to reduce total delivery time, improve fleet utilization, and minimize operational costs in logistics networks.
2. Supports Dynamic and Adaptive Decision-Making: Traditional routing methods often fail to accommodate real-time traffic variability, demand fluctuations, and environmental constraints. This study demonstrates how predictive models and optimization algorithms can adapt to dynamic conditions, offering a robust decision-support system for logistics managers.
3. Promotes Security and Data Integrity: IoT networks are vulnerable to cyber threats, including GPS spoofing, sensor tampering, and unauthorized data access. By incorporating cybersecurity considerations, the study ensures that optimized routes remain reliable and resilient, mitigating risks associated with compromised IoT data.
4. Contributes to Sustainable Logistics: Efficient routing reduces unnecessary travel distance and time, thereby lowering fuel consumption, emissions, and environmental impact. This aligns with the growing emphasis on sustainable and green logistics practices.
5. Provides a Generalizable Framework: The methodology, based on synthetic data, machine learning, and optimization techniques, is adaptable to various logistics scenarios, including urban delivery networks, e-commerce logistics, cold chain distribution, and heterogeneous vehicle fleets.
6. Facilitates Research and Practical Implementation: By offering a structured, reproducible approach, the study provides a foundation for future research, including extensions to dynamic routing, multi-objective optimization, reinforcement learning, and real-time IoT data integration. It also offers practical insights for logistics managers, enabling informed decisions on vehicle allocation, route planning, and network design.
7. Bridges Research Gaps: The study addresses the gap between predictive analytics, optimization, and cybersecurity in IoT logistics, creating a holistic framework that has been largely underexplored in prior literature.

This study is significant because it not only improves operational efficiency and decision-making in IoT-enabled logistics but also ensures security, sustainability, and adaptability, providing both academic contributions and real-world applicability.

5. Conclusion

This study presents a comprehensive framework for route optimization in IoT-enabled logistics networks, combining machine learning-based travel time prediction, optimization algorithms, and cybersecurity considerations. Using synthetic data, the study demonstrates how predictive modeling and optimization can enhance operational efficiency, reduce total travel time, improve vehicle utilization, and adapt dynamically to traffic variability.

The results highlight several key findings:

1. Efficiency Gains: Machine learning models accurately predict travel times, allowing the optimization algorithm to generate routes that minimize total distance and delivery time.
2. Dynamic Adaptability: The framework accommodates real-time variations in traffic and delivery demands, demonstrating robustness over static routing methods.
3. Security Integration: Incorporating cybersecurity measures ensures the integrity and reliability of IoT data, mitigating risks from GPS spoofing, sensor tampering, or communication failures.
4. Practical Relevance: The proposed methodology is generalizable and can be adapted to multiple logistics contexts, including urban delivery, heterogeneous fleets, and cold chain distribution, making it highly relevant for practitioners.
5. Research Contribution: By bridging predictive analytics, optimization, and cybersecurity, the study addresses gaps in current literature and provides a foundation for future research in IoT-driven, secure, and adaptive logistics systems.

In conclusion, the hybrid approach offers actionable insights for logistics managers, enabling more efficient, secure, and sustainable delivery operations. Future extensions could include real-time IoT data integration, multi-objective optimization, reinforcement learning-based routing, and multi-class vehicle fleets, further improving the scalability, resilience, and applicability of IoT-enabled logistics systems.

References

[1]. Zrelli, I., & Rejeb, A. (2024). A bibliometric analysis of IoT applications in logistics and supply chain management. Heliyon, 10, e36578.

[2]. Ajayi, O. A. (2023). Real Time Route Optimization in Logistics: A Deep Learning Approach. World Journal of Advanced Research and Reviews, 19(03), 1719–1722.

[3]. Shao, Q., & Cheng, S.-F. (2023). Preference Aware Delivery Planning for Last-Mile Logistics. arXiv preprint.

[4]. Mozhdehi, A., Mohammadizadeh, M., & Wang, X. (2024). Edge DIRECT: A Deep Reinforcement Learning based Method for Solving Heterogeneous Electric Vehicle Routing Problem with Time Window Constraints. arXiv preprint.

[5]. Luo, H., Wei, J., Zhao, S., Liang, A., Xu, Z., & Jiang, R. (2025). Enhancing Robot Route Optimization in Smart Logistics with Transformer and GNN Integration. arXiv preprint.

[6]. Judijanto, L., & Rismanto, H. (2025). Dynamic Routing in Urban Logistics: A Comprehensive Review of AI, Real Time Data, and Sustainability Impacts. Sinergi International Journal of Logistics, 3(2), 68–79.

[7]. Sethia, S. (2024). Smart Supply Chains: Leveraging AI and Digital Transformation for Route and Distance Optimization. International Journal of Intelligent Systems and Applications in Engineering, 12(22s), 1929–1940.

[8]. Raju Mudunuru, K., Remala, R., & Nagarajan, S. K. (2024). Leveraging IoT and Data Analytics in Logistics: Optimized Routing, Safety, and Resource Planning. International

Journal of Computer Trends and Technology, 72(7), 101-107.

[9]. Qi, B., & Li, G. (2024). The evolution of the cold chain logistics vehicle routing problem: A bibliometric and visualization review. Digital Transportation and Safety, 3(3), 92–114.