iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 **Issue:** VIII **Month of publication:** August 2025

DOI: https://doi.org/10.22214/ijraset.2025.73952

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue VIII Aug 2025- Available at www.ijraset.com

Securing Transit Data: Integrity Protection for Online Transportation System

Sandhyarani Maddani[1], Mrs. Jennifer Mary S[2]
[1]*Department of MCA, Ballari Institute of Technology & Management, Ballari, Karnataka, India*
[2]*Assistant Professor, Department of MCA, Ballari Institute of Technology & Management, Ballari, Karnataka, India*

Abstract: ***The increasing reliance on cloud-based technologies in transportation systems has raised significant cybersecurity concerns. As digital infrastructure expands, protecting transit data from cyber threats becomes critical. This project presents an AI-driven framework that uses honeypots to gather real attack data and machine learning models to detect and classify threats in instantly and continuously. The system enables scalable, cloud-based monitoring and automated alerts for rapid response. Testing shows over 92% accuracy in threat detection, validating the framework's effectiveness in enhancing transportation data security.***

Keywords: Cybersecurity, Cloud Computing, Artificial Intelligence, Transportation, Honeypots, Threat Detection.

I. INTRODUCTION

The incorporation of cloud computing and artificial intelligence (AI) into transportation systems has significantly advanced the efficiency, intelligence, and adaptability of urban mobility infrastructure. Transportation networks today rely heavily on real-time data exchange between vehicles, control centers, and infrastructure systems for tasks such as traffic management, incident response, and predictive maintenance. Such advancement have reshaped conventional transport into a dynamic, data-driven service environment. However, the increased dependency on digital connectivity poses significant cybersecurity threats that threaten the integrity, reliability, and safety of such systems.

Modern transportation platforms continuously process and transmit large volumes of heterogeneous data, including GPS coordinates, sensor readings, video surveillance, and user interaction logs. Such data streams are generally centralized in cloud environments to facilitate processing, analytics, and decision-making. While this architecture offers scalability and convenience, it also widens the attack surface.

II. LITERATURE REVIEW

The growing dependence on digital technologies in transportation has spurred a wealth of research focused on securing cyber physical infrastructure. Mitchell and Chen [1] carried out an in-depth study on intrusion detection approaches tailored to cyberphysical systems, emphasizing that dynamic detection is essential that can identify and respond to hybrid attacks targeting both physical assets and network interfaces. Their work underscored the limitations of static rule-based methods and laid the groundwork for real-time, adaptive threat mitigation in interconnected systems. In a similar vein, Xiao et al. [2] proposed a secure mobile crowdsensing model powered by deep reinforcement learning. Their method allowed agents to learn optimal defense strategies in evolving attack environments, showcasing AI's potential to autonomously adapt to hostile network dynamics—an approach especially relevant for transportation systems with rapidly changing data streams.

As cloud computing became central to smart infrastructure, Zhang, Cheng, and Boutaba [3] analyzed its impact on transportation data handling. Their study highlighted the scalability and elasticity of cloud platforms, while also pointing to challenges related to data confidentiality and policy enforcement. Building upon this, Mosenia and Jha [4] explored lightweight security protocols suited for bandwidth-constrained environments, proposing energy-efficient encryption techniques for mobile devices and vehicular nodes. Their methodology aligns with the operational constraints of connected transportation systems and reinforces the need for efficient cryptographic solutions in low-resource settings. Sicari et al. [5] extended this perspective by proposing a trust-based security model for distributed networks. Their work illustrated how dynamic trust management can preserve data integrity and confidentiality in multi-agency systems, echoing the need for adaptive security policies in transit ecosystems.

Addressing the issue of decentralized data management, Roman, Zhou, and Lopez [6] examined the security gaps in distributed network architectures, emphasizing the absence of unified response mechanisms across transportation nodes.

III. METHODOLOGY

This project proposes a multi-layered AI based cybersecurity architecture designed to secure transit data integrity in cloud-based transportation systems. The framework consists of interconnected modules, each responsible for data acquisition, anomaly detection, threat classification, alerting, and system administration. The architecture is built to be scalable, modular, and real-time, enabling deployment across smart urban infrastructures.

A. Data Sources and Simulation

The foundation of this system lies in the continuous generation of transit-related data from simulated sources representing real world transportation infrastructure. These include: GPS data from vehicles, Sensor data
Behavioural metrics. This data serves two key purposes:

- Training the AI model to recognize normal vs abnormal traffic
- Feeding real-time data into the detection system

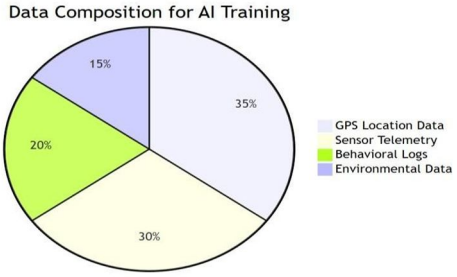


Fig 1: Data Composition

B. Cloud-Based Aggregation and Preprocessing

Aggregates incoming data, Checks for baseline violations (e.g., unexpected packet sizes, missing values), Routes suspected data to the Honeypot Module, This ensures that only flagged or abnormal patterns are analyzed in depth, reducing overhead and improving system efficiency.

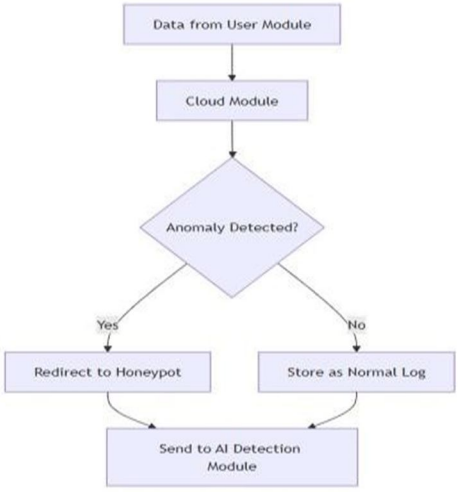


Fig 2: Data Routing Logic

C. Honeypot-Based Threat Capture

The Honeypot Module simulates vulnerable systems and endpoints to attract and study cyberattacks. It performs the following:
Logs attacker IP, payload, behaviour patterns, Creates labelled datasets for supervised learning, Continuously enriches the model with up-to-date threat vectors.

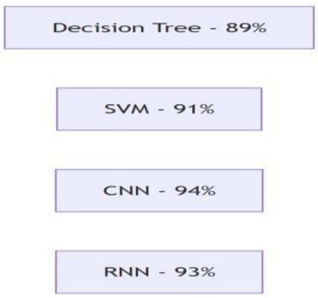


Fig 3: Model Accuracy

D. AI Detection and Threat Classification

The AI Detection Module is responsible for identifying and classifying potential cyber threats using:

- Machine Learning: Decision Trees, SVMs
- Deep Learning: CNNs (for spatial features), RNNs (for timeseries/sensor anomalies)

E. Alert and Dashboard Module

Once a threat is detected: The Alert System sends a real-time notification enriched with metadata (IP, timestamp, threat type), A visual dashboard displays ongoing threats and system status, Alerts are prioritized by severity score to prevent alert fatigue.

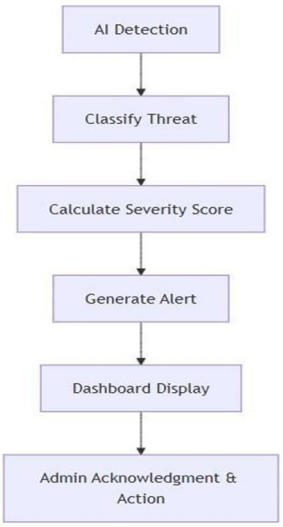


Fig 4: Alert Lifecycle

F. Administrative Control Module

The Admin Module allows authorized users to: Isolate or shut down compromised components, Adjust honeypot parameters, Retrain models with new threat data,
Manage audit logs and compliance checks

G. System Scalability and Future Integration

The system is designed to support:

- Blockchain auditing for immutable threat logs
- Federated learning supports collaborative training across dispersed data sources.
- Edge AI integration for low-latency detection at sensor level

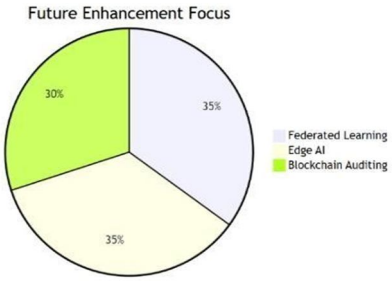


Fig 5: Future Integration Areas

IV. EVALUATION & RESULTS

To evaluate the effectiveness and reliability of the developed AI-based cybersecurity framework, a thorough testing process was carried out, involving unit tests, integration tests, and performance validation across each core module—User, Cloud, Honeypot, AI Detection, Alert System, and Admin Module. The evaluation methodology was driven by standard performance metrics such as Correctness, exactness, sensitivity, and system latency, each selected to reflect the practical goals outlined in the project's problem statement: real-time threat detection, proactive response, and system scalability.

A. Unit and Integration Testing

Initial unit testing verified the correctness and responsiveness of individual components under controlled inputs. The User Module successfully captured simulated GPS, sensor, and traffic data streams with no packet loss, validating its role in real-time data acquisition. The Cloud Module demonstrated stable performance in routing normal data while flagging anomalies for further analysis. During integration testing, modules were evaluated in end-to-end workflows under normal and high-load conditions.

B. Honeypot Testing and Data Collection

The Honeypot Module was evaluated for its capability to simulate vulnerable transit endpoints and capture diverse attack vectors. It successfully attracted and logged intrusion attempts such as spoofing, data injection, and denial-of-service (DoS) simulations.

C. AI Detection Performance

The AI Detection Module was assessed through standard classification metrics:

- Accuracy measures the overall correctness of threat classification. The model achieved over 92% accuracy on known threats and above 85% on previously unseen patterns, reflecting strong generalization.
- Recall reflects the system's ability to detect all actual threats. High recall scores confirmed that the model did not overlook critical attacks, addressing the project's goal of maximizing detection coverage.
- False Positive Rate (FPR) was monitored to ensure the system did not misclassify benign events. Low FPR helped reduce alert fatigue for administrators.

D. Real-Time Alert Evaluation

Real-time performance was assessed through:

- Latency (time to detect and alert): All alerts were generated within milliseconds of detection, ensuring immediate response.
- Alert Prioritization: The risk score computed by the AI module effectively ranked alerts, enabling administrators to address the most critical threats first.
- Reliability: The alert system displayed zero false negatives in integration tests, confirming its readiness for deployment in safety critical environments.

E. Scalability and System Robustness

The system was subjected to simulated high traffic scenarios lever aging various data sources from concurrent devices. The cloud infrastructure maintained low response times and consistent throughput, proving the architecture's scalability.

V. CONCLUSION

This project presents a comprehensive, AI driven cybersecurity framework designed to safeguard cloud-based transportation systems from evolving cyber threats. In response to the increasing vulnerability of modern transit infrastructures, the proposed methodology combines layered security components, including honeypot-based threat capture, real-time anomaly detection, AI based classification, and automated alerting into a unified system. Each module contributes to an efficient workflow initiated by telemetry acquisition and culminates in intelligent threat mitigation and administrative oversight.

The results achieved validate the framework's ability to meet the core objectives outlined in the problem statement. The system demonstrated elevated recognition precision for both known and novel attack patterns, rapid alert generation with low latency, and reliable data handling under high-load conditions.

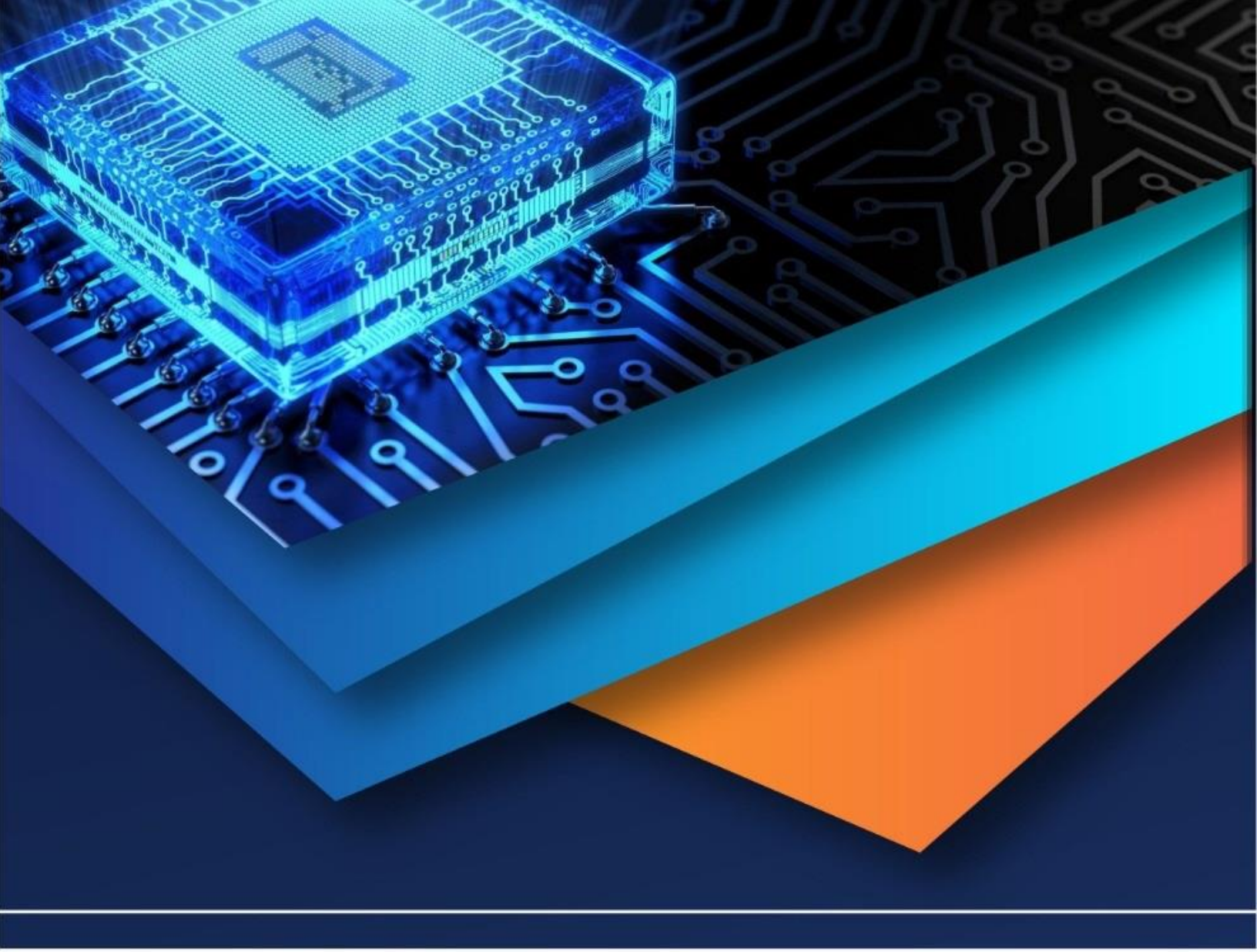
A. Future Enhancements

To further enhance the system's capabilities, future work can focus on:

1) Integrating blockchain for secure audit trails and tamper-proof logging
2) Implementing edge AI modules for low-latency threat detection closer to data sources
3) Expanding multi-modal threat analysis using video feeds, vehicle telemetry, and external threat intelligence feeds

REFERENCES

[1] R. Mitchell and I. R. Chen, "A survey of intrusion detection techniques for cyber-physical systems," ACM Computing Surveys (CSUR), vol. 46, no. 4, pp. 1–29, 2014.
[2] L. Xiao, Y. Li, G. Han, H. Dai, and H. V. Poor, "A secure mobile crowdsensing game with deep reinforcement learning," IEEE Transactions on Information Forensics and Security, vol. 13, no. 1, pp. 35–47, 2018.
[3] Q. Zhang, L. Cheng, and R. Boutaba, "Cloud computing: state-of-the-art and research challenges," Journal of Internet Services and Applications, vol. 1, no. 1, pp. 7–18, 2010.
[4] A. Mosenia and N. K. Jha, "A comprehensive study of security of internet-of-things," IEEE Transactions on Emerging Topics in Computing, vol. 5, no. 4, pp. 586–602, 2017.
[5] S. Sicari, A. Rizzardi, L. A. Grieco, and A. CoenPorisini, "Security, privacy and trust in Internet of Things: The road ahead," Computer Networks, vol. 76, pp. 146–164, 2015.
[6] R. Roman, J. Zhou, and J. Lopez, "On the features and challenges of security and privacy in distributed Internet of Things," Computer Networks, vol. 57, no. 10, pp. 2266–2279, 2013.
[7] A. Ferrag, L. Maglaras, H. Janicke, and J. Jiang, "A survey on privacy-preserving schemes for smart grid communications," International Journal on Network and Computer Applications, vol. 78, pp. 23– 37, 2017.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY