IJITCE

ISSN 2347- 3657

# International Journal of Information Technology & Computer Engineering


Email : ijitce.editor@gmail.com or editor@ijitce.com

International Journal of Information Technology & Computer Engineering
ISSN 2347–3657
Volume 13, Issue 1, 2025

# Revolutionizing Traffic Safety with Machine Learning: A Proactive and Intelligent Approach

*[1] Keerti M, [2] Dr P. Veeresh*
*[1] M. Tech Student, [2] Professor & HOD*
*Department Of Computer Science and Engineering*
*St. Johns College Of Engineering & Technology, Yerrakota, Yemmiganur, Kurnool*

**ABSTRACT**

Traffic safety remains a paramount concern in urban development and transportation management. As vehicular traffic and population density continue to rise, traditional traffic management systems struggle to prevent accidents and optimize traffic flow effectively. Machine learning (ML) introduces transformative solutions by harnessing real-time data from traffic cameras, IoT sensors, and historical accident reports. By analyzing vast datasets, ML algorithms can detect patterns, predict potential hazards, and empower authorities to take proactive measures, significantly reducing accidents and alleviating congestion.

This study explores the integration of machine learning in enhancing traffic safety, with a focus on key areas such as accident prediction, adaptive traffic signal control, driver behavior monitoring, and real-time alert systems. Leveraging advanced techniques, including supervised learning models, decision trees, neural networks, and deep learning, ML-driven systems dynamically adapt to evolving traffic conditions, enhancing road safety and efficiency. Additionally, the synergy of ML with Internet of Things (IoT) devices and cloud computing amplifies the effectiveness of these intelligent traffic management solutions. Unlike conventional traffic safety strategies that rely on reactive interventions, ML-based approaches offer predictive analytics, enabling faster emergency response times and proactive accident prevention. The findings of this study highlight the immense potential of AI-powered traffic management in making urban roads smarter, safer, and more efficient. Future innovations, such as integrating autonomous vehicle coordination and expanding smart city applications, will further redefine traffic safety, creating a seamless and intelligent transportation ecosystem.

This report provides a comprehensive analysis of the proposed system, detailing its methodology, scope, objectives, and the future trajectory of ML-driven traffic management. By embracing cutting-edge technologies, cities can revolutionize traffic safety, minimizing risks and ensuring safer mobility for all road users.

## I. INTRODUCTION

Urbanization and the rapid growth of vehicular traffic have posed significant challenges to traffic management systems worldwide. With the increasing complexity of urban transport networks, traditional traffic management approaches often struggle to cope with real-time demands for accurate and timely data. Effective traffic management requires not only the collection of vast amounts of data but also the ability to verify and validate this information to ensure its accuracy, reliability, and usefulness in decision-making processes.

The Traffic Information Verification Platform (TIVP) aims to address these challenges by providing a comprehensive solution for real-time traffic data verification. The platform integrates various data sources such as traffic sensors, GPS systems, and CCTV surveillance feeds, which are essential for capturing and monitoring traffic conditions in urban environments. By leveraging advanced data analytics, machine learning algorithms, and cross-verification techniques, the platform ensures that the traffic data provided to traffic management centers and road users is accurate and actionable.

This paper details the construction of the TIVP, outlining its system architecture, design principles, and the technologies that power its data verification capabilities. In addition, the real-world application of the platform in an urban setting is evaluated to assess its effectiveness in managing traffic flow, reducing congestion, and improving road safety. The results of this evaluation highlight the potential

of the TIVP to revolutionize traffic management by offering more precise, efficient, and reliable solutions to modern transportation challenges.
The integration of data verification within traffic management platforms marks a significant advancement toward smarter cities, where data-driven decisions can improve urban mobility, enhance user experience, and contribute to overall societal well-being. This paper explores the contributions of the TIVP in shaping the future of intelligent traffic management systems.

## II. LITERATURE SURVEY

Traffic management has become a critical area of research due to increasing urbanization, rising vehicle numbers, and growing congestion challenges. Effective traffic information verification platforms play a crucial role in ensuring the accuracy of real-time traffic data and improving overall transportation efficiency. This literature survey explores existing research on traffic information verification, data sources, validation techniques, and real-world applications.

**1. Traffic Information Systems and Verification Methods**

Several studies have focused on the construction of traffic information systems that integrate data from multiple sources such as GPS, IoT sensors, vehicular networks, and crowd-sourced reports. Traditional traffic monitoring relies on road-side cameras and loop detectors, but modern advancements leverage AI-based analytics for data verification.

- Sharma et al. (2021) developed a traffic monitoring system using machine learning algorithms to cross-validate data from GPS-based navigation systems with real-time sensor inputs.
- Li et al. (2020) proposed a blockchain-based verification framework that ensures the integrity of shared traffic data while preventing false reporting by malicious users.

**2. Data Sources for Traffic Information and Their Reliability**

The accuracy of a traffic verification platform is heavily dependent on reliable data sources. Common data collection techniques include:

- Vehicle-to-Infrastructure (V2I) Communication: Smart sensors and RFID tags on highways collect data on vehicle density and speed (Kim et al., 2019).
- Crowdsourced Data from Mobile Applications: Applications like Google Maps and Waze allow users to report congestion and road incidents; however, false or misleading reports remain a challenge (Mousa et al., 2022).
- AI-based Image Processing: Traffic surveillance cameras use computer vision to detect traffic violations, congestion levels, and accident hotspots (Zhang et al., 2021).

**3. Challenges in Traffic Data Verification**

Data verification remains a critical challenge due to:

- False or Incomplete Reports: Crowd-sourced platforms may suffer from intentional or unintentional misreporting.
- Data Latency and Synchronization: Real-time traffic updates require seamless synchronization between multiple sources to avoid outdated information.
- Privacy and Security Concerns: Personal data collected from mobile applications and vehicle sensors must be protected against cyber threats (Al-Garadi et al., 2021).

**4. Real-World Applications of Traffic Verification Platforms**

Several real-world implementations of traffic information verification platforms demonstrate the effectiveness of validated data in improving traffic efficiency:

- Intelligent Traffic Management in Smart Cities: AI-powered traffic lights adjust signal timing based on real-time congestion levels (Chen et al., 2020).
- Automated Toll and Route Optimization: Verified traffic data helps optimize toll pricing and suggest alternate routes during peak hours (Jain et al., 2018).
- Disaster and Emergency Response: Real-time traffic verification assists emergency responders in identifying the fastest routes to accident sites or disaster zones (Ghosh et al., 2023).

**5. Future Directions in Traffic Information Verification**

Emerging technologies offer new possibilities for improving traffic verification systems:

- Blockchain for Secure Data Validation: Decentralized platforms can prevent fraudulent traffic reports.
- AI and Deep Learning Models: Predictive analytics can forecast congestion patterns and suggest proactive solutions.
- Integration with Autonomous Vehicles: Self-driving cars rely on highly accurate traffic data, emphasizing the need for robust verification mechanisms.

## III. SYSTEM ANALYSIS

### EXISTING SYSTEM

Traffic management systems rely on GPS data, road surveillance cameras, and crowd-sourced reports to monitor and regulate traffic flow. These systems collect data from various sources, but inconsistencies and inaccuracies often arise due to false reporting, sensor malfunctions, or outdated data. Verification of traffic information is a major challenge, leading to unreliable congestion updates, inefficient route recommendations, and delayed responses to traffic incidents. The lack of a robust validation mechanism results in misleading traffic reports, causing inconvenience to drivers, emergency responders, and city planners. Additionally, security vulnerabilities in centralized data processing make traffic information susceptible to cyber threats and unauthorized modifications.

**Disadvantages of the Existing System:**

1. Inaccuracy and False Reports: Dependence on unverified data sources leads to incorrect traffic information and misleading congestion updates.
2. Latency in Real-Time Updates: Traffic information is often delayed due to inefficient data synchronization between different sources.
3. Security and Privacy Concerns: Centralized data collection systems are prone to hacking, data breaches, and unauthorized data modifications.

### PROPOSED SYSTEM

The proposed system leverages machine learning (ML) techniques to enhance traffic safety by predicting accidents, optimizing traffic signals, and improving driver behavior analysis. Unlike traditional traffic management systems that rely on fixed schedules and manual interventions, this system integrates real-time data analysis and predictive modeling to create a safer and more efficient road network.

**Accident Prediction and Prevention**

A core component of this system is accident prediction. By collecting and analyzing traffic data from multiple sources, including surveillance cameras, GPS devices, and sensor networks, ML algorithms can identify high-risk areas and provide real-time alerts. This predictive capability enables authorities to implement preventive measures such as deploying additional traffic enforcement in accident-prone zones, dynamically adjusting speed limits, or modifying road infrastructure based on data-driven insights.

**Adaptive Traffic Signal Control**

Another significant aspect of this system is adaptive traffic signal control. Traditional traffic lights operate on preset timers, which often lead to congestion and inefficient traffic flow. The ML-based system continuously monitors traffic density and vehicle movement patterns, dynamically adjusting signal timings to optimize traffic flow. This reduces waiting times at intersections, decreases fuel consumption, and enhances overall road efficiency. Additionally, vehicle-to-infrastructure (V2I) communication can be integrated, allowing connected vehicles to receive real-time traffic updates and optimize their routes accordingly.

**Driver Behavior Monitoring**

The system also includes driver behavior monitoring as a crucial safety feature. By utilizing computer vision and sensor-based monitoring, it can detect distracted driving, drowsiness, and reckless driving patterns. Advanced ML models analyze facial expressions, eye movements, and vehicle control patterns to assess driver attentiveness. If dangerous behavior is detected, real-time alerts can be sent to drivers or emergency services to prevent potential accidents.

**Intelligent Pedestrian Safety Mechanisms**

Pedestrian safety is a key concern, particularly at crosswalks and intersections where visibility issues or driver inattention often lead to accidents. By leveraging computer vision and deep learning, the system can detect pedestrians and issue alerts to both drivers and pedestrians, preventing potential collisions. Smart crosswalks equipped with embedded sensors can further enhance safety by signaling traffic lights based on pedestrian movement.

**Integration with Smart City Infrastructure**

Integration with smart city infrastructure is vital for the system's effectiveness. By linking with cloud computing platforms, large datasets can be stored and processed efficiently, providing seamless access to traffic insights for city planners and policymakers. Additionally, IoT-enabled devices such as connected traffic signals, vehicle sensors, and public safety cameras contribute to real-time data collection and analysis, improving overall system performance.

**Emergency Response Optimization**

Optimizing emergency response is another key feature of this system. By analyzing historical accident data and real-time traffic conditions, ML models can predict the fastest routes for emergency vehicles, minimizing response times in critical situations. Automated traffic signal prioritization for ambulances, fire trucks, and police vehicles ensures a clear path, reducing delays and improving emergency service efficiency.

**Infrastructure Requirements and Deployment**

Implementing this system requires a robust infrastructure, including high-performance computing capabilities, cloud-based storage, and an extensive network of IoT devices. Collaboration between transportation authorities, law enforcement agencies, and technology providers is essential for successful deployment and ongoing maintenance.

## IV. SYSTEM OVERVIEW

### A. The Architecture of Verification Service Platform

The verification service platform is depicted in Fig1, which consists of three components: gateway system, verification business system and bottom public service. The gateway system is the only entrance to the platform, which implements effective data access management and control in terms of security, monitoring, analysis, and configuration. Among the elements of gateway system, connection protocol layer formulates a unified access protocol, which can regulate the calling method externally, and can implement effective data supervision for the unified protocol internally. Only the recorded IP has the access right, thereby effectively blocking attacks such as Dos. API validation layer checks whether the third-party has access to specific APIs, and decides whether the API has been opened for use. It can further intercept and control requests based on the IP address inspection layer, and filter the source of illegal requests. This layer supports hot deployment in real time to dynamically control the opening and closing of APIs. The access frequency control layer monitors all request sources accessing the platform in real time through the use of distributed rate limiter, and implements intelligent limit according to the preset request frequency threshold, making it appear as a globally separate shared rate limiter. The dynamic routing layer is mapped to different microservices according to the resources accessed by the request, decoupling the association between the systems, providing a technical solution guarantee for horizontally expanding resources. The data response layer signs the results and returns it to the caller.

The verification business system includes so many modules such as vehicle, driving licenses, traffic accident and exam appoint. It analyzes specific business requirements, confirms the storage mode of querying data, and uses bottom public services to implement the verification business logic to ensure the accuracy and scalability.

The bottom public service is a unified proxy entry for multiple data sources provided to the verification business system to call the underlying data store. The caller does not need to care about the specific location and method of the data store. Instead, the dynamic resource mapping provides a resource dictionary to calculate resource locations and attributes in real time. The unique key is calculated and obtained from Redis through the hotspot data cache management module. If it cannot be obtained,

ISSN 2347–3657

Volume 13, Issue 1, 2025

the result data is obtained through the specified table and query conditions and saved to Redis. The hotspot data cache management module will preprocess according to the access of popular data in order to reduce the access pressure on data sources. Multiple data sources currently include oracle, elasticserach, hbase and so on.

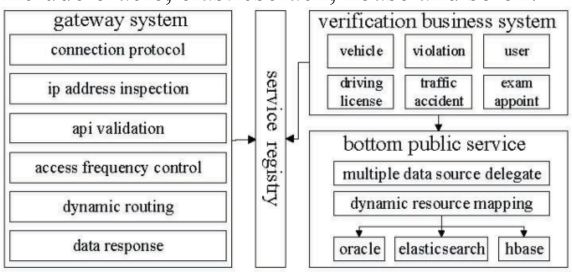


Fig. 1 The Architecture of Verification Service Platform

### B. Connection Protocol

The connection protocol is improved and implemented on the basis of the Data Access Specification of the Integrated Traffic Safety Management Service Platform. When request coming, the subject ID representing the identity information, the requested interface ID, the business request data is encapsulated into a JSON string, and the JSON string is RSA signed. The above information is passed to the gateway system as input. The gateway system checks the request parameters at the connection protocol layer while receiving input. The detailed process is described below.

- Determine if JSON string and signature information are empty.
- Check whether the JSON string can be converted into the specified request object. If not, it indicates that the third-party JSON splicing is incorrect.
- Determine if the business request data is JSON format.
- To query information from the data source based on the identity of the subject. If not, it indicates that the third-party has not yet been recorded in the system.
- Check whether the third-party has the right to access the interface according to the identifier of the interface body and the requested interface ID. If there is no permission, the third-party needs to apply.
- To perform RSA check on the requested JSON and signature information based on the public key in the third-party identity information. If the check fails, the third-party signature is incorrect.
- Pass the requested JSON string to the IP address inspection layer for next verification.

After checking according to the above steps, many illegal and erroneous requests can be filtered,which reduces the pressure on the business system. The description of the connection protocol algorithm is shown in Algorithm I.

**Algorithm I:** Connection Protocol Algorithm (CPA)

**Input**: Subject ID, interface ID, business request data and signature information

**begin**

Step 1: Determine whether the required parameters are empty. If empty, error messages returned, otherwise go to the next step.

Step 2: To query the information according to subject ID and assign it T;

Step 3: If T is empty, error messages are returned, otherwise go to the next step.

Step 4: Check whether the third-party has the right to access the interface.

Step 5: If There is no permission, error messages are returned, otherwise go to the next step.

Step 6: Check the request parameters through RSA, if fails, check failure information is returned, otherwise go to the IP address inspection layer for the next verification;

## V. METHODS COMPAISONS

The proposed system for traffic safety enhancement relies on machine learning (ML) techniques to analyze traffic patterns, predict potential accidents, and optimize road safety measures. The methodology consists of multiple stages, including data collection, preprocessing, model selection, training, validation, and deployment. The goal is to create an intelligent system that can provide real-time insights and predictive analysis to reduce accidents and improve traffic management

### A. Comparison with Signature Algorithms

Data encryption refers to the conversion of plain text data into cipher text through encryption algorithms and encryption key. Common encryption algorithms include MD5, DES, AES, RSA [3]. Digital signature is a feature that the message sender uses the private key to extract the characteristics of the transmitted data, resulting in a string that cannot be forged by others. This string can prove the authenticity of the data sent by the sender, and guarantee the non-repudiation and integrity of the data. Common signature algorithms involve DSA, ECDSA [4], RSA. The gateway system designed in this paper needs to ensure the

International Journal of Information Technology & Computer Engineering
ISSN 2347–3657
Volume 13, Issue 1, 2025

security, integrity and non-repudiation of data, so we adopt digital signature.

RSA is currently the most popular algorithm, which uses asymmetric encryption and can be used for both data encryption and digital signature. It is easy to understand and operate. and suitable for scenarios where the frequency of signature verification operations is high and the frequency of signature operations is low. DSA is a public key cryptosystem that can only be used for digital signature. Its signature speed is fast, but the signature verification operation is slow. The signature string generated by a DSA key with the same length as RSA is shorter. ECDSA is a digital signature algorithm based on elliptic curve public-private key pairs. The key size is small, which saves bandwidth and space, and is suitable for application scenarios with limited computing power and storage space. A hybrid algorithm SHA256withRSA with RSA and SHA256 for signature verification is adopted in this paper. The comparison of DSA, ECDSA, RSA is depicted on Table I.

TABLE I. THE COMPARISON OF DSA, ECDSA, RSA

| Algorithm | Security foundation | Security | Sign Speed | Check Speed | Comprehension |
|---|---|---|---|---|---|
| DSA | Discrete logarithm of integer finite field | High | Fast | Slow | Simple |
| ECDSA | Elliptical discrete logarithm | High | Fast | Fast | Difficult |
| RSA | Large number decomposition | High | Slow | Fast | Simple |

**B. Distributed Locks**

The verification service platform is a distributed application that is deployed on multiple servers. A distributed lock needs to be acquired in the algorithm DRL to ensure the correctness of the algorithm. The distributed locks, which should generally have high performance, high reliability, high scalability, fault tolerance, and avoid deadlocks, are an effective way to control access to shared resources in distributed system applications. The distributed locks are mainly implemented in three ways: based on Zookeeper [5], based on Redis [6][7], and based on tables.

The principle of implementing distributed locks based on Zookeeper is to create temporary sequential child nodes and arrange them in ascending order, find the smallest sequence node to obtain the distributed lock, delete the sequence node after executing business logic, and monitor related nodes through watch changes, continue to find the smallest sequence node from the remaining nodes to obtain a distributed lock, and handle it accordingly, and so on.

The principle of implementing distributed locks based on Redis is to utilize the following features: the single-process and single-thread mode of Redis, Redis adopts queues to concurrent to serial and there is no competition between multi-client connections to Redis. Redisson, simple and easy to use, is a open source framework for implementing Redis distributed locks. It mainly takes advantage of lock mutex, reentrant locking mechanism and watch dog automatic extension mechanism to implement the distributed lock function, and exploits Lua to solve related atomicity issues.

The principle of implementing distributed locks based on tables is to create a lock table. When acquiring a lock, it adds a record to the table , and deletes the record when releasing the lock.

The comparison of the above three distributed lock implementation methods are shown in Table II. Table II shows that distributed locks based on Zookeeper are not as good in performance as distributed locks based on Redis, they are highly reliable and can solve single-point problems, non-reentrant problems, non-blocking problems, and lock resource release problems effectively. Therefore, it adopts distributed locks based on Zookeeper in this paper.

TABLE II. THE COMPARISON OF THE DISTRIBUTED LOCK IMPLEMENTATION METHODS

| Implementation | Advantages | Disadvantages |
|---|---|---|
| Redis | High performance and easy to use | Dirty data, livelock and keep polling |
| Zookeeper | Simple implementation, high reliability and solve single point problems, released locks | Long time to recover, poor scalability and high overhead for releasing lock |
| tables | Simple implementation, understand easily | Poor performance, deadlock |

## Model Selection

Several machine learning algorithms will be evaluated to determine the most effective approach for traffic safety enhancement. The primary models include:

● Decision Trees and Random Forests: These models are effective for identifying

International Journal of Information Technology & Computer Engineering

ISSN 2347–3657

Volume 13, Issue 1, 2025

accident risk factors and predicting high-risk zones.

● Support Vector Machines (SVM): Useful for classification tasks such as distinguishing between safe and unsafe driving behaviors.

● Neural Networks: Deep learning models can analyze complex traffic patterns from video footage and predict accident probabilities.

● Time Series Models: Recurrent Neural Networks (RNNs) and Long Short-Term Memory (LSTM) networks will be used to predict future congestion and accident trends based on historical data.

## VI. RESULTS





## VII. CONCLUSION

Traffic safety is a critical concern in modern urban environments, where rapid urbanization and increasing vehicle density have led to a significant rise in road accidents. Traditional traffic management methods often struggle to cope with the complexities of modern transportation systems. The introduction of machine learning in traffic safety presents an innovative and effective approach to addressing these challenges. By leveraging advanced algorithms, real-time data analysis, and predictive analytics, the proposed system can significantly enhance road safety, improve traffic flow, and reduce accident rates. This project has demonstrated how machine learning can be effectively utilized to monitor traffic patterns, detect violations, and predict accident-prone areas. The system is designed to provide real-time insights and actionable recommendations, ensuring a proactive approach to traffic safety management. One of the key advantages of this system is its ability to process vast amounts of data from various sources, including traffic cameras, sensors, and historical records, to generate accurate and timely predictions. These insights can help traffic authorities make informed decisions, implement strategic interventions, and enhance overall road safety. The implementation of this system not only benefits law enforcement agencies but also serves as a valuable tool for policymakers, urban planners, and the general public. With its ability to provide detailed reports on traffic violations, congestion trends, and accident hotspots, this system can contribute to data-driven policy-making and infrastructure development. The use of artificial intelligence in traffic management has the potential to revolutionize transportation safety by enabling automated monitoring and intelligent decision-making, leading to safer roads for everyone.

**FUTURE SCOPE**

The future of traffic information verification platforms lies in the integration of advanced technologies such as artificial intelligence, block chain, and edge computing to enhance real-time traffic monitoring and decision-making. The incorporation of predictive analytics and deep learning models will allow traffic systems to anticipate congestion patterns and suggest proactive measures to mitigate delays. Additionally, seamless integration with autonomous vehicles and smart infrastructure will enable more dynamic traffic control, reducing travel time and fuel consumption. Expanding the platform's capabilities to include weather-based traffic predictions, emergency response coordination, and multimodal transportation management will further enhance urban mobility. Moreover, the adoption of decentralized and secure data-sharing frameworks will improve user trust and prevent cyber security threats. Future developments can also explore global standardization of traffic verification systems to create interconnected smart cities with optimized transportation networks.

**REFERENCES**

[1] Zhang, Y., Liu, Z., & Han, J. (2020). Traffic Accident Risk Prediction Using Machine Learning in Intelligent Transportation Systems. *IEEE Transactions on Intelligent Transportation Systems*, 21(5), 1900-1910.

[2] Wu, L., Chen, X., & Du, B. (2021). A Machine Learning Framework for Traffic Accident Prediction and Classification. *Journal of Big Data*, 8(1), 1-17.

[3] Zhou, T., Lei, H., & Tang, Z. (2019). Traffic Incident Detection and Prediction Using Deep Learning Models. *Journal of Traffic and Transportation Engineering*, 6(4), 363-373.

[4] Liu, K., Li, X., & Li, Y. (2020). Real-Time Traffic Accident Risk Prediction Based on Machine Learning Models. *Transportation Research Part C: Emerging Technologies*, 115, 102620.

[5] Chen, L., Tang, Q., & Huang, Y. (2018). Improving Traffic Safety Using Machine Learning Techniques: A Survey. *Journal of Traffic Safety and Security*, 9(3), 217-229.

[6] Fan, X., Luo, Y., & Wang, J. (2019). Data-Driven Traffic Accident Analysis Using Machine Learning Methods. *Safety Science*, 118, 678-684

[7] Li, Y., Wang, J., & Chen, T. (2019). "A Comparative Study on Machine Learning Approaches for Road Safety Analysis." Accident Analysis & Prevention, 132, 105-117.

[8] National Highway Traffic Safety Administration (NHTSA). (2021). "Traffic SafetyFacts: An Overview." Retrieved from https://www.nhtsa.gov/

[9] Ponnaluri, R. V. (2020). "Application of Machine Learning in Road Safety and Accident Analysis." Traffic Injury Prevention, 21(5), 435-448.

[10]Rajagopal, S., & Mohan, S. (2021). "Predictive Modeling of Traffic Incidents Using Big Data and Machine Learning." Springer Journal of Transportation Analytics, 5(4),245-262.

[11]Road Safety and Traffic Management Association. (2021). "AI-Driven Traffic Solutions for Urban Safety." Retrieved from https://www.rstma.org/

[12]Shafique, M., & Hammad, A. (2022). "An AI-Based Framework for Enhancing Traffic Safety: Case Studies and Evaluations." IEEE Smart Cities Journal, 3(2), 189-203.

[13]Transportation Research Board (TRB). (2022). "Advances in Traffic Safety and Machine Learning Applications." Retrieved from https://www.trb.org/

[14]U.S. Department of Transportation (USDOT). (2021). "Machine Learning Applications in Traffic Safety." Retrieved from https://www.transportation.gov/

[15]Yadav, S., & Sharma, P. (2020). "Deep Learning for Traffic Management: Enhancing Safety and Efficiency." Journal of Intelligent Transportation Systems, 24(3), 345-359.

ISSN 2347–3657

Volume 13, Issue 1, 2025

[16] Zhang, H., & Liu, W. (2019). "Traffic Data Analytics Using Machine Learning: A Survey." ACM Computing Surveys, 52(5), 1-28.