Enhancing Data Security in Sustainable Smart Cities Through Neural Networks and Trust Management Models

[1]Satish Kumar Pasawan, [2]Saurabh Mandloi

[1]M. Tech Scholar, Department: Computer science engineering, Sam Global University, Bhopal

[2]Head of department, Department: Computer science engineering, Sam Global University, Bhopal
[1]satishpasawan869@gmail.com , [2]hodcse@samglobaluniversity.ac.in

Abstract: In the era of urban digitization, smart cities rely on interconnected devices and data-driven infrastructure to deliver sustainable, efficient, and intelligent services. However, the integration of cyber-physical systems into transportation networks introduces significant cybersecurity risks, such as data breaches, denial of service (DoS), GPS spoofing, and unauthorized access. This study addresses these challenges by proposing a robust hybrid machine learning model designed to detect and classify cyber-attacks in smart transportation systems. The model integrates Neural Networks (NN), XGBoost, and Logistic Regression with an Attention mechanism to leverage both spatial and temporal dependencies within the data. To enhance classification performance, especially for rare attack types like Brute Force and Whitewash, the Synthetic Minority Over-sampling Technique (SMOTE) is applied to mitigate class imbalance. The model is evaluated using metrics such as Accuracy (0.9153), Precision (1.0000), Recall (0.8462), F1-Score (0.9167), and ROC-AUC (1.0000), indicating strong detection capabilities and low false positive rates. Extensive data preprocessing using tools like NumPy and Pandas ensures reliable input, while visualization libraries like Matplotlib and Seaborn support interpretability through graphs and heatmaps. Results from the confusion matrix and correlation heatmap confirm the critical role of trust-related features and highlight the model's effectiveness in identifying complex malicious behaviors. This approach presents a scalable, data-driven security framework for smart mobility, improving both trust and resilience in intelligent transportation systems.

Keywords: Smart Cities, Cybersecurity, Transportation Systems, Neural Networks, XGBoost, Attention Mechanism, Trust Management, Attack Detection, IoT, Machine Learning.

I INTRODUCTION

Smart cities represent a forward-thinking approach to urban development, leveraging technologies like Information and Communication Technology (ICT) and the Internet of Things (IoT) to improve residents' quality of life, enhance public services, and support sustainable growth [1]. These cities rely on interconnected sensors and devices to collect and analyze real-time data, enabling efficient infrastructure management, intelligent transportation, energy conservation, and improved public safety. Driven by rapid urbanization and infrastructure demands, smart city initiatives transform how urban environments function and interact with citizens, ultimately creating responsive ecosystems that enhance everyday living [2]. The Internet of Things (IoT), first introduced in 1999 at MIT, refers to a global network of interconnected devices capable of sharing data and making autonomous decisions. Enabled by advances in compact electronics and affordable high-speed internet, IoT has transformed ordinary objects into intelligent, collaborative systems forming the backbone of smart infrastructure [3]. This connectivity fosters an intelligent communication layer that integrates countless digital devices. Projects like the Bhopal Smart City have explored IoT architectures, communication protocols, and real-world applications such as noise monitoring. By treating IoT devices as service providers akin to cloud platforms, researchers have bridged physical infrastructure with digital services, paving the way for scalable and innovative smart city solutions [4].

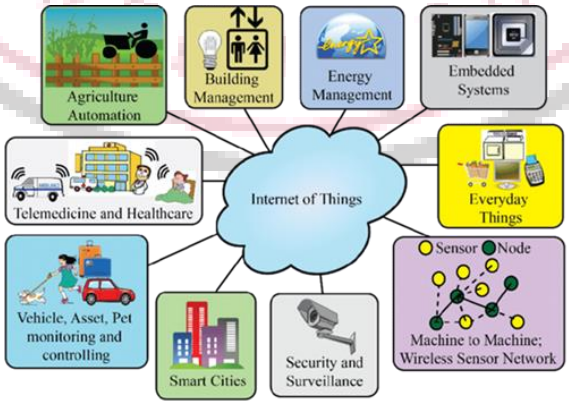

Fig. 1 IoT in Smart Cities [5].

As cyber systems increasingly constitute the underpinning digital infrastructure for smart transportation, cybersecurity can then be considered a paramount concern. The systems involve a complex arrangement of IoT

devices, sensors, cloud platforms, and communication channels that functions so as to constantly collect and transmit real-time data and on-the-fly analyses. Yet somehow, having so much interconnectivity has likewise exposed them through windows of susceptibilities to various forms of cyber-attacks, such as breaches of data, ransomwares, GPS spoofing, denial of service (DoS), and unauthorized access. These attacks threaten data integrity and privacy and even jeopardize enormous disruptions in transportation activities, endangering public trust, safety, and urban operations [6]. Security breaches for smart transportation cause effects that go beyond technical disruption. An intelligent traffic control system, if compromised, could impose congestion, delay emergency response services, or cause accidents. Such breaches may have authorized access to sensitive personal data or unauthorized control of vehicle systems by one kind or another. With this, as the implementation of autonomous vehicles and connected mobility platforms grows, even a minor security issue may turn into a huge one impacting whole urban infrastructure [7]. Data privacy and trust become two indispensable pillars on which any secure smart transport framework rests. Data confidentiality must be ensured with data authenticity and availability, or else one cannot rely upon the system. Trust management systems allow for the instant evaluation of credibility when it comes to devices and data sources, which then serve to weed out malicious input and enhance system resilience. When cities combine strong cybersecurity measures with trust-based validation mechanisms, to protect the transportation infrastructure, they ensure public safety and foster sustainable growth in digital mobility-bold act [8]. As cyber systems increasingly constitute the underpinning digital infrastructure for smart transportation, cybersecurity can then be considered a paramount concern. The systems involve a complex arrangement of IoT devices, sensors, cloud platforms, and communication channels that functions so as to constantly collect and transmit real-time data and on-the-fly analyses. Yet somehow, having so much interconnectivity has likewise exposed them through windows of susceptibilities to various forms of cyber-attacks, such as breaches of data, ransomwares, GPS spoofing, denial of service (DoS), and unauthorized access. These attacks threaten data integrity and privacy and even jeopardize enormous disruptions in transportation activities, endangering public trust, safety, and urban operations [9].

Security breaches for smart transportation cause effects that go beyond technical disruption. An intelligent traffic control system, if compromised, could impose congestion, delay emergency response services, or cause accidents. Such breaches may have authorized access to sensitive personal data or unauthorized control of vehicle systems by one kind or another. With this, as the implementation of autonomous vehicles and connected mobility platforms grows, even a minor security issue may turn into a huge one impacting whole urban infrastructure [10]. Data privacy and trust become two indispensable pillars on which any secure smart transport framework rests. Data confidentiality must be ensured with data authenticity and availability, or else one cannot rely upon the system. Trust management systems allow for the instant evaluation of credibility when it comes to devices and data sources, which then serve to weed out malicious input and enhance system resilience. When cities combine strong cybersecurity measures with trust-based validation mechanisms, to protect the transportation infrastructure, they ensure public safety and foster sustainable growth in digital mobility-bold act.

II LITERATURE REVIEW

Son et al. (2025) [11] examined smart transportation challenges like congestion and safety, analyzing 26 studies using the PRISMA framework and NLP tools. They found that IoT, AI, and digital twins enhance traffic flow and environmental efficiency. The study emphasized integrating digital twin modeling, sensor networks, and AI decision systems for sustainable urban mobility.

Mirindi et al. (2025) [12] explored the role of AI, ML, and DL in green transportation. They reviewed various algorithms and applied the UTAUT framework to assess technologies in areas like EVs, MaaS, and micromobility. AI-driven transport was shown to reduce emissions and improve safety, though concerns about ethics, privacy, and fairness remain.

Panda et al. (2025) [13] focused on cloud-based smart transportation solutions using IoT and data analytics to manage congestion and pollution. Cloud platforms were shown to offer scalable, real-time monitoring and improved decision-making, contributing to safer, smarter, and more sustainable urban mobility systems.

Zemmouchi-Ghomari et al. (2025) [14] assessed AI's impact on Intelligent Transportation Systems in cities like New York and Beijing. AI enhanced traffic flow, reduced accidents, and supported sustainable mobility. However, challenges such as data quality, privacy, and public trust require long-term policy and economic frameworks for broader adoption.

Goumiri et al. (2025) [15] reviewed smart mobility in the context of fast, eco-friendly urban transport. They identified key challenges like parking, routing, and emissions, analyzing successes and failures in real-world deployments. The study concluded with practical insights for improving future smart mobility solutions.

Table 1 Comparative Analysis of Recent Studies on Smart Transportation

Authors & Reference No.	**Focus**	**Technologies Discussed**	**Key Findings**	**Challenges Identified**
Heejoo Son et al. (2025) [11]	Role of advanced technologies in smart	IoT, AI, digital twins, optimization methods	Technologies improve traffic flow, safety,	Data infrastructure investment, long-

	transportation planning		operational efficiency, and reduce environmental impact.	term policy integration.
Derrick Mirindi et al. (2025) [12]	Role of AI/ML in sustainable mobility solutions	AI, ML, DL, Genetic Algorithm, SVM, CNN, RNN, EVs, MaaS	AI enhances energy efficiency, reduces emissions, and improves safety.	Data privacy, algorithmic fairness, ethical governance.
Aditya Kumar Panda et al. (2025) [13]	Cloud-based smart transportation solutions	Cloud computing, IoT, AI	Cloud platforms enable scalable, real-time data collection for better decision-making.	Integration of systems, infrastructure scaling.
Leila Zemmouchi-Ghomari et al. (2025) [14]	AI in Intelligent Transportation Systems (ITS)	Machine learning, deep learning, computer vision	AI improves traffic efficiency, reduces accidents, and supports sustainable urban mobility.	Data quality, real-time processing, security, privacy.
Soumia Goumiri et al. (2025) [15]	Smart Mobility for urban transportation solutions	Smart mobility, IoT, data analytics	Smart mobility transforms urban mobility systems, addressing key challenges in traffic and emissions.	Integration of smart mobility systems, emission concerns.

III OBJECTIVES

- To develop deep learning models for detecting vehicle behaviors and cyber-attacks like DoS, Whitewash, and Brute Force.
- To integrate Neural Networks, XGBoost, and Logistic Regression with attention for improved detection accuracy.
- To apply SMOTE to address class imbalance and enhance detection of rare attack types.
- To evaluate model performance using Accuracy, Precision, Recall, F1-Score, and ROC-AUC for real-time reliability.

IV METHODOLOGY

For the purposes of this section, a hybrid machine learning solution that would aid in the detection and identification of attack types in transportation systems was created. The hybrid model combined three compelling methods i.e., Neural Networks (NN), XGBoost, and Logistic Regression, using an Attention mechanism to ensure prediction accuracy taking advantage of the strength of each architecture. NN is able to leverage transportation data spatial attributes such as trust_degree, location, and time variables. XGBoost can solve the gap by uncovering sequential dependency learning, which captures long-term behavior patterns in vehicle movement/traffic. Logistic Regression was used as a baseline linear classifier in order to improve the overall robustness of the model solution. Adding an Attention mechanism further tunes the model's attention towards making it learn to focus on the most informative portions of the data, thereby improving its sensitivity to fine-grained patterns of attacks like DoS, Whitewash, and Brute Force.

A. Implementation tools

Python: Python was selected as the main programming language for implementation because it has a wide range of libraries supporting data science, machine learning, and optimization operations

NumPy: NumPy is a fundamental library in Python for numerical computing, with excellent support for large, multi-dimensional matrices and arrays, as well as loads of (advanced) mathematical functions. This means pretty much everything is done with NumPy in this project, particularly in terms of data control because of the numerical data structures that were constructed, which are fundamental to machine learning procedures. NumPy was used to process the features of trust_degree, hour, and anything that was a time-variable. This meant in the model training processes data control could be easier using NumPy.

Pandas: Pandas is a high-performance, data manipulation and analytics library for Python. For the purposes of this thesis, it was used heavily to load, clean, and organize datasets pertaining to transportation into suitable formats for analysis. The primary preprocessing tasks that were completed included renaming columns and changing data types, replacing the empty values that were important features in the datasets with suspect values, and splitting the datasets into appropriate forms for training and testing algorithms, and storing models.

Matplotlib: This popular Python visualization library was used to create plots like the Confusion Matrix, ROC-AUC curves, and accuracy/loss graphs. These plots were key in determining model performance, identifying weaknesses, and communicating results effectively to stakeholders.

Seaborn: Based upon Matplotlib, Seaborn provides an even higher-level interface for creating informative and beautiful statistical graphics. In this project, it was employed to enrich visualizations for class distributions and feature importance. Seaborn also facilitated the design of heatmaps for the Confusion Matrix and helped visualize distribution plots, enhancing interpretability of the classification results.

B. Hybrid Model

The proposed attack detection model integrates Neural Networks (NN), XGBoost, and an Attention mechanism to effectively capture both spatial and temporal patterns in transportation system data. Initially, NNs are utilized to extract spatial features by learning patterns in structured input data, which helps in assessing vehicle behaviors and identifying anomalies that may indicate attacks. Subsequently, XGBoost is employed to analyze temporal dependencies, modeling the sequential behavior of vehicles by learning from the evolving trust and location signals. In the final stage, the outputs from both NN and XGBoost are fused using an Attention mechanism, which dynamically emphasizes the most relevant parts of the input sequence. This mechanism allows the model to focus on critical time steps and input features that are more likely to reflect attack-induced anomalies. The combination of spatial feature extraction by NN, temporal learning by XGBoost, and refined focus through the Attention mechanism enables the model to detect complex, subtle, and low-signal attacks with higher precision, offering a robust and intelligent solution for transportation system security.

C. Evaluation Metrics

The proposed Neural Network (NN) + XGBoost + Attention combination model was evaluated on a wide suite of performance metrics to assess its performance for attack detection in transportation systems. The metrics test not only the model's classification performance (i.e., is it better than chance?), but also its ability to identify harmful vehicle behaviours. Using a variety of metrics allows a more complete evaluation of the model's ability to be able to identify normal and abnormal behaviours, including DoS, Whitewash, and Brute Force attacks.

Accuracy

Accuracy measures the overall correctness of the model's predictions across all classes. Specifically, it is the proportion of accurately predicted cases to the overall number of cases. A high accuracy score indicates that the model reliably produces precise predictions.

$$Accuracy = \frac{True\ positive + True\ Negetive}{TotalNumber\ of\ Instance} \quad (1)$$

Precision

Precision measures the ratio of true positive predictions (i.e., accurately detected malicious behaviours) to all instances predicted positive by the model. In attack detection, high precision guarantees that most raised alerts by the system relate to real threats, and there are minimal false positives.

$$Precision = \frac{True\ positive}{True\ Positive + False\ Positives} \quad (2)$$

Recall (Sensitivity)

Recall, or sensitivity, measures the model's capability to correctly identify all existing positive instances i.e., how well the model identifies all genuine malicious behaviours. This metric is particularly important in security applications because non-detectable attacks (false negatives) can be very dangerous.

$$\text{Recall} = \frac{True\ Positives}{True\ Positives + False\ Negatives} \quad (3)$$

D. Confusion Matrix

The Confusion Matrix is a comprehensive table that displays the predictions made by the model for each category: Non-malicious, DoS, Whitewash, and Brute Force. It shows the number of true positives, true negatives, false positives, and false negatives, providing a thorough understanding of the model's advantages and disadvantages. If an excessive number of DoS attacks are misclassified as legitimate behavior, this would show up in the confusion matrix and prompt targeted improvements to the model. In transport security, this granularity is invaluable for aligning model performance with actual threat detection needs.

E. ROC-AUC (Receiver Operating Characteristic – Area Under Curve)

The ROC-AUC metric assesses the model's ability to discriminate by plotting the True Positive Rate (or Recall) against the False Positive Rate at various classification thresholds. The Area Under Curve (AUC) measures this ability, where 1.0 means perfect discrimination between classes and 0.5 indicates random guessing performance. A high value of ROC-AUC means that the model had reasonably distinguishable malicious and non-malicious behaviours. This measure is also useful as it can show us appropriate decision thresholds nosing our select ratio according to specific security priorities (e.g., prioritize early threat detection even if it means accepting high rates of false alarms).

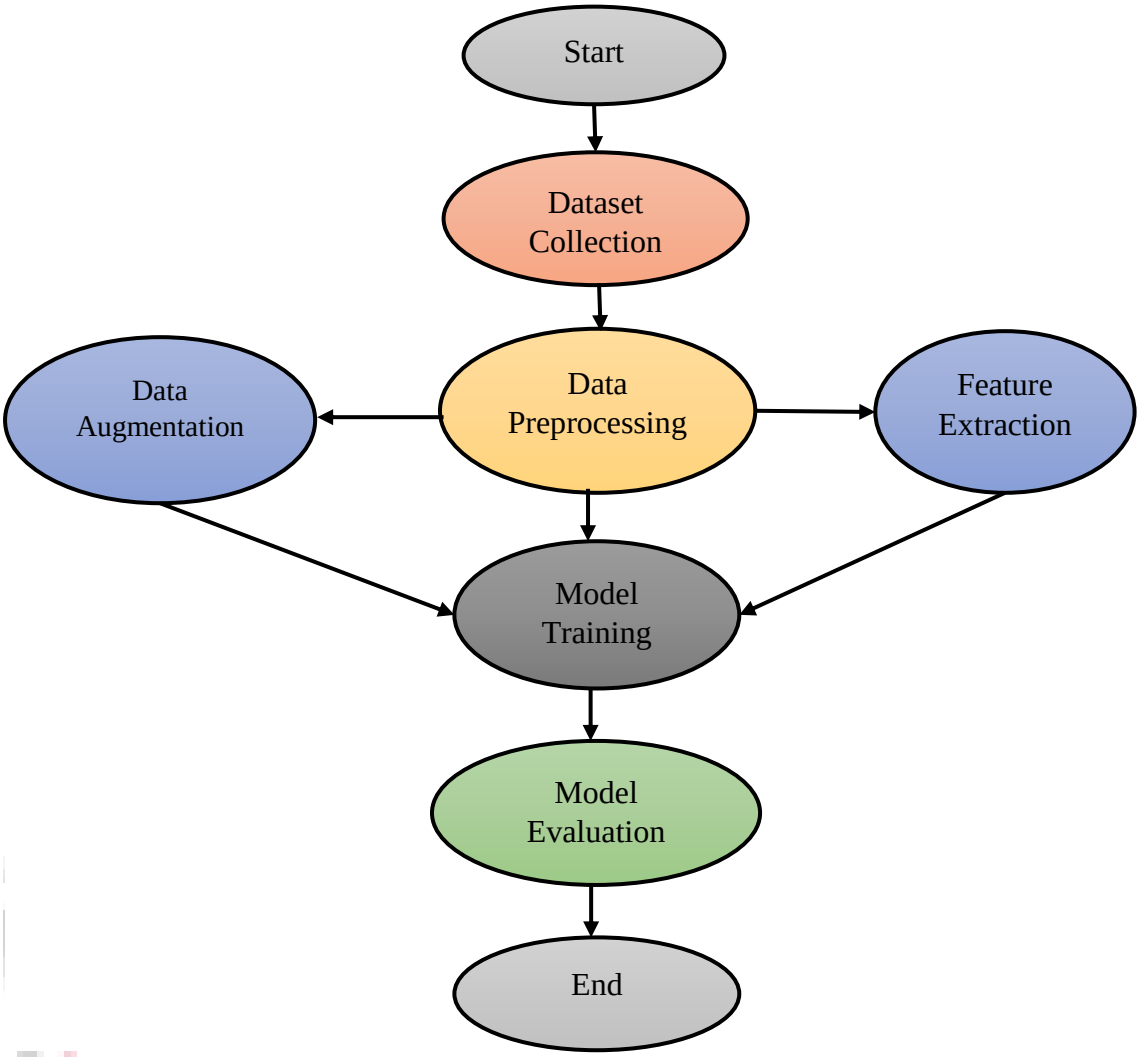

Fig. 2 Flow Chart of Methodology

V RESULTS AND DISCUSSION

This segment showcases a complete performance evaluation of the hybrid machine learning model that consists of a Neural Network (NN), XGBoost, and an Attention Mechanism used for attack detection in transportation systems. The assessment aims to explore classification metrics like Accuracy, Precision, Recall, F1-Score, Confusion Matrix, and ROC-AUC for an in-depth analysis of a model's performance in identifying and categorizing corrupted vehicular behaviors, which may include DoS, Whitewash, or Brute Force attacks.

A. Hybrid ML-Based Detection of Attacks and Behavioural Anomalies in Transportation Networks

In earlier works, there has been a structured and systematic framework that was useful to enhance security and provide anomaly detection in smart transport systems. This framework primarily focused on various aspects of data improvement, class imbalance, and metrics as needed for classifying the unique types of attacks. This framework starts with the extraction of transport system data as the raw input resource for analysis. A key first step is data pre-processing in regards to managing missing values, as well as ensuring the dataset is as balanced as possible for proper classification. The Simple Imputer method is a model that was used for imputing missing values, along with SMOTE (Synthetic Minority Over-sampling Technique) for overcoming class imbalance problems. This is done to ensure the training dataset contains both malicious and non-malicious behaviour instances in sufficient quantity.

Table 2 Model Performance Metrics

Metric	**Score**
Accuracy	0.9153
Precision	1
Recall	0.8462
F1-Score	0.9167
ROC-AUC	1

Table 2 showcases the model's strong classification performance. With an accuracy of 0.9153, it correctly identifies over 91% of instances. A precision of 1.0000 means all predicted Malicious cases were truly malicious, with no false positives. The recall of 0.8462 shows it detects most malicious instances, though a small portion is missed. The F1-score of 0.9167 reflects a balanced performance between precision and recall. Finally, the ROC-AUC of 1.0000 indicates perfect distinction between Malicious and Non-Malicious cases, confirming the model's high reliability.

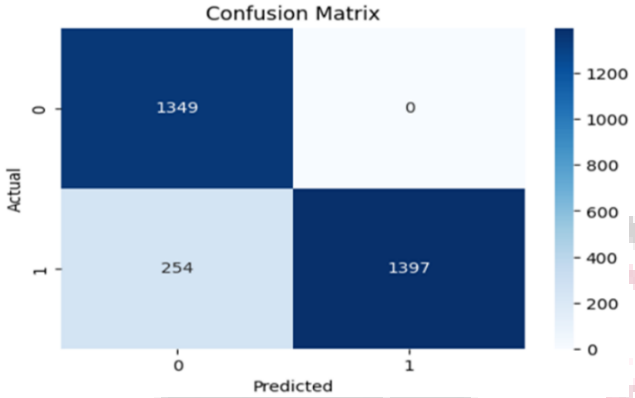

Fig. 3 Confusion Matrix.

The confusion matrix in Fig. 3 shows the results of the model's classification. It indicates that the model accurately identified 1349 instances as Non-Malicious (True Negatives) and 1397 instances as Malicious (True Positives). The matrix also shows that 254 instances were wrongly labeled as non-malicious when they were actually Malicious (False Negatives). There were no instances misclassified as Malicious when they were Non-Malicious (False Positives). These values give a clear view of the model's classification performance.

Table 3 Attack Detection Results

Attack Type	**Count**
Non-Malicious	1600
DoS	1349
Brute Force	33
Whitewash	18

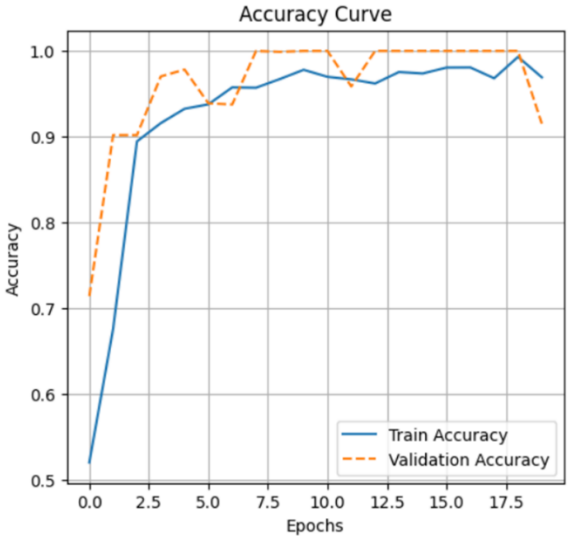

Fig. 4 Accuracy Curve

The accuracy curve in Fig. 4 displays the model's performance over time. The solid blue line shows the train accuracy, while the dashed orange line represents the validation accuracy. At first, the train accuracy rises quickly, indicating the model's learning process. The validation accuracy also increases in the early epochs but starts to vary more after reaching higher values. This suggests that the model might be overfitting on the training data.

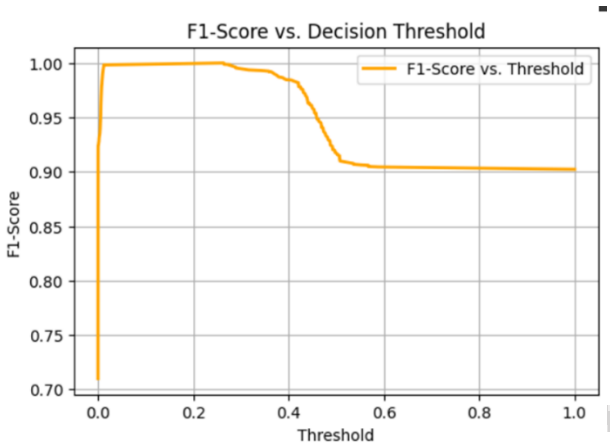

Fig. 5 F1-Score vs. Decision Threshold

The F1-Score vs. Decision Threshold curve in Fig. 5 illustrates how the F1-Score changes as we adjust the threshold for classifying an instance as Malicious (1) or non-malicious (0). When the threshold is low, the F1-Score stays high, around 1. This indicates that the model is very sensitive and classifies more instances as Malicious. As we raise the threshold, the F1-Score gradually drops, showing a decrease in the model's ability to identify Malicious instances. The curve points out the trade-off between sensitivity and precision. It can help us choose the best decision threshold for a balanced F1-Score.

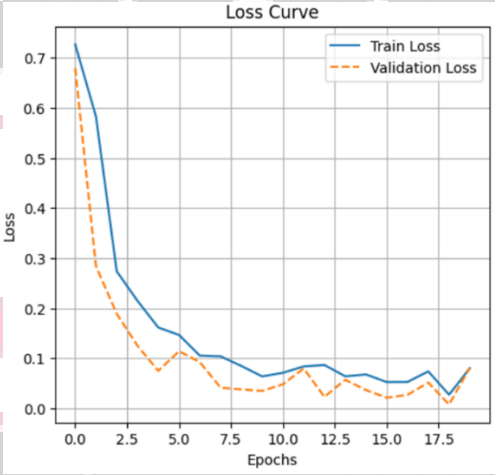

Fig. 6 Loss Curve.

The F1-Score vs. Decision Threshold curve in Fig. 6 illustrates how the F1-Score changes as we adjust the threshold for classifying an instance as Malicious (1) or non-malicious (0). When the threshold is low, the F1-Score stays high, around 1. This indicates that the model is very sensitive and classifies more instances as Malicious.

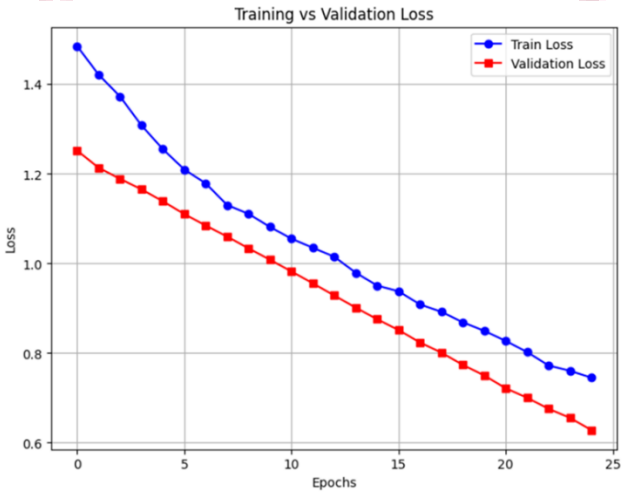

Fig. 7 Training vs Validation Loss

Figure 7 “Training vs Validation Loss” compares loss value calculated on training and validation data for a span of 25 epochs. The training loss is shown by the blue curve, whereas the validation loss is shown by the red one. At the beginning, both losses were high, steadily decreasing as the training continued. But, since the training loss is decreased rapidly, it means that this model is learning to fit its training data well. On the other hand, the validation loss seems to decrease a bit slower than the ones in training, and hence suggests that the model generalizes fairly well to the validation data when both losses decrease with time.

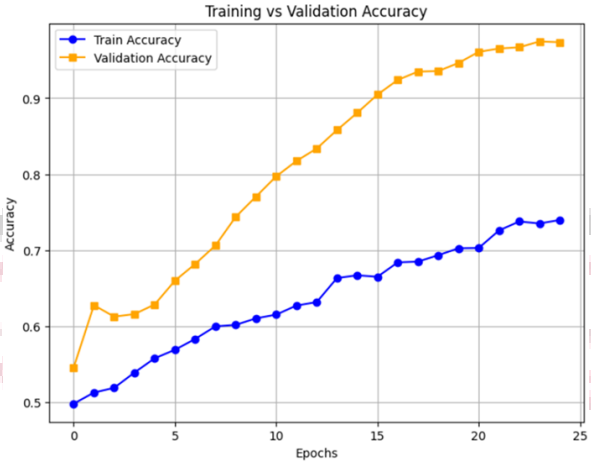

Fig. 8 Training vs Validation Accuracy

The Training versus Validation Accuracy plot in Fig. 8 depicts the evolution of the model's accuracy throughout the training. The blue line corresponds to training accuracy, whereas the orange line corresponds to validation accuracy.

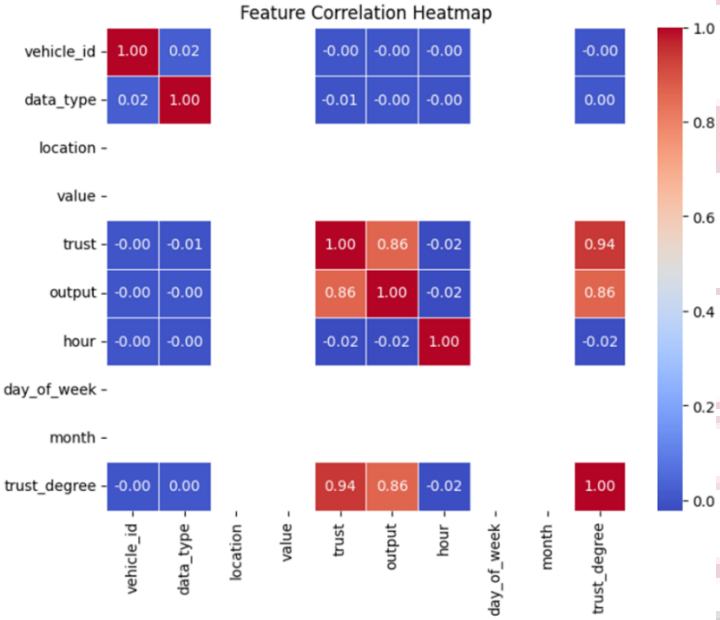

Fig. 9 Feature Correlation Heatmap.

The Feature Correlation Heatmap in Fig. 9 reveals strong relationships among trust-related features, with high correlations between trust and value (0.86), trust and output (0.86), and particularly trust degree with both value and trust (0.94). These strong correlations indicate that trust-related features significantly influence each other and are likely key in predicting the target output. In contrast, features like vehicle_id, data_type, location, and hour show weak correlations, suggesting limited linear interaction with other variables. Overall, the heatmap highlights the central role of trust metrics in the model’s predictive performance.

VI Conclusion

This study demonstrates that a hybrid machine learning model incorporating Neural Networks, XGBoost, Logistic Regression, and an Attention mechanism can significantly enhance cybersecurity in smart transportation systems. By capturing both spatial patterns and temporal dynamics, and addressing class imbalance with SMOTE, the model effectively detects various cyber threats with high accuracy and precision. The inclusion of trust-based features and robust evaluation metrics further confirms the model’s suitability for real-time deployment in smart city environments. As smart mobility evolves, integrating such intelligent, adaptive, and trustworthy security systems is essential for ensuring sustainable, safe, and resilient urban infrastructure.

References

[1] Padhiary, M., Roy, P., & Roy, D. (2025). The Future of Urban Connectivity: AI and IoT in Smart Cities. In Sustainable Smart Cities and the Future of Urban Development (pp. 33-66). IGI Global Scientific.
[2] Singh, T., Solanki, A., Sharma, S. K., Nayyar, A., & Paul, A. (2022). A decade review on smart cities: Paradigms, challenges and opportunities. IEEE Access, 10, 68319-68364. https://doi.org/10.1109/ACCESS.2022.3184710
[3] Song, Tao & Cai, Jianming & Chahine, Teresa & Li, Le. (2021). Towards Smart Cities by Internet of Things (IoT)—a Silent Revolution in China. Journal of the Knowledge Economy. 12. 10.1007/s13132-017-0493-x. https://link.springer.com/article/10.1007/s13132-017-0493-x
[4] Abadía, J. J. P., Walther, C., Osman, A., & Smarsly, K. (2022). A systematic survey of Internet of Things frameworks for smart city applications. Sustainable Cities and Society, 83, 103949. https://doi.org/10.1016/j.scs.2022.103949
[5] Mohanty, Saraju. (2016). Everything You Wanted to Know About Smart Cities. IEEE Consumer Electronics Magazine. 5. 60-70. 10.1109/MCE.2016.2556879. http://dx.doi.org/10.1109/MCE.2016.2556879
[6] Mecheva, T., & Kakanakov, N. (2020). Cybersecurity in intelligent transportation systems. Computers, 9(4), 83. https://doi.org/10.3390/computers9040083
[7] Arora, Pankit & Bhardwaj, Sachin & Vegesna, Vinod. (2020). Research on Cybersecurity Issues and Solutions for Intelligent Transportation Systems. International Journal of Innovative Research in Computer and Communication Engineering. 8. 150-163.
[8] Galego, N.M.C., Pascoal, R.M. (2022). Cybersecurity in Smart Cities: Technology and Data Security in Intelligent Transport Systems. In: Mesquita, A., Abreu, A., Carvalho, J.V. (eds) Perspectives and Trends in Education and Technology. Smart Innovation, Systems and Technologies, vol 256. Springer, Singapore. https://doi.org/10.1007/978-981-16-5063-5_2
[9] Kumar, G., Altalbe, A. Artificial intelligence (AI) advancements for transportation security: in-depth insights into electric and aerial vehicle systems. Environ Dev Sustain (2024). https://doi.org/10.1007/s10668-024-04790-4
[10] Tonhauser, M.; Ristvej, J. Implementation of New Technologies to Improve Safety of Road Transport. Transp. Res. Procedia 2021, 55, 1599–1604. https://doi.org/10.1016/j.trpro.2021.07.149
[11] Son, H., Jang, J., Park, J., Balog, A., Ballantyne, P., Kwon, H. R., Singleton, A., & Hwang, J. (2025). Leveraging Advanced Technologies for (Smart) Transportation Planning: A Systematic Review. Sustainability, 17(5), 2245. https://doi.org/10.3390/su17052245
[12] Mirindi, D., Khang, A., Mirindi, F. (2025). Artificial Intelligence (AI) and Automation for Driving Green Transportation Systems: A Comprehensive Review. In: Khang, A. (eds) Driving Green Transportation System Through Artificial Intelligence and Automation. Lecture Notes in Intelligent Transportation and Infrastructure. Springer, Cham. https://doi.org/10.1007/978-3-031-72617-0_1
[13] Panda, A. K., Lenka, A. A., Mohapatra, A., Rath, B. K., Parida, A. A., & Mohapatra, H. (2025). Integrating cloud computing for intelligent transportation solutions in smart cities: A short review. Interdisciplinary approaches to transportation and urban planning, 121-142. 10.4018/979-8-3693-6695-0.ch005
[14] Zemmouchi-Ghomari, L. (2025). Artificial intelligence in intelligent transportation systems. Journal of Intelligent Manufacturing and Special Equipment.
[15] Goumiri, S., Yahiaoui, S., & Djahel, S. (2025). Smart Mobility in Smart Cities: Emerging challenges, recent advances and future directions. Journal of Intelligent Transportation Systems, 29(1), 81-117. https://doi.org/10.1080/15472450.2023.2245750