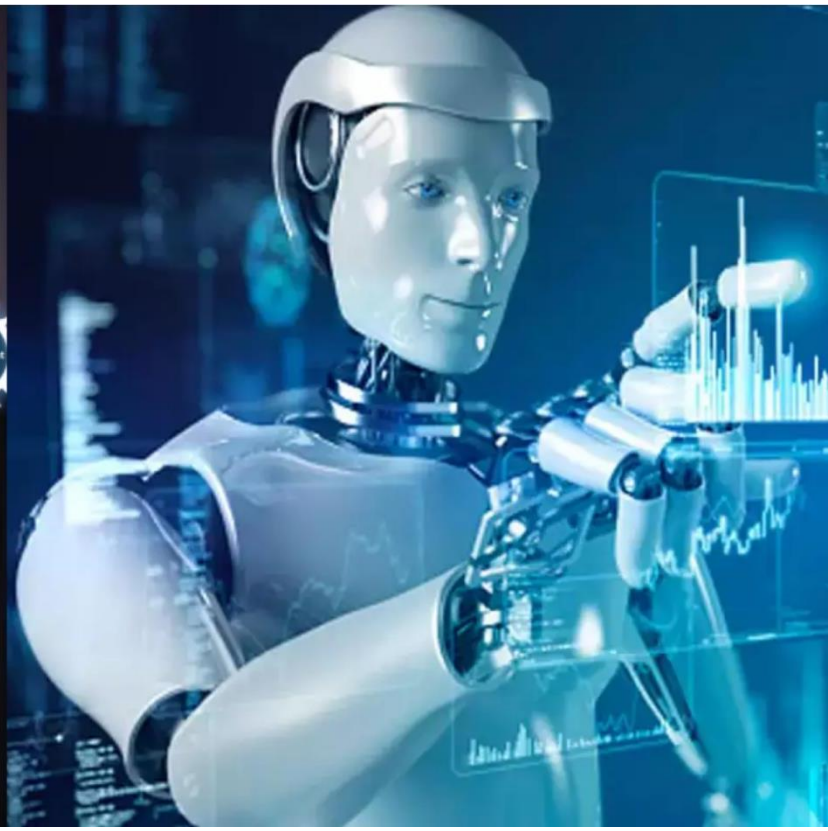
IJIRSET
International Journal of Innovative Research in Science | Engineering | Technology

ISSN(O): 2319-8753
ISSN(P): 2347-6710

International Journal of Innovative Research in Science Engineering and Technology (IJIRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.699

Volume 15, Issue 4, April 2026

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 4, April 2026

|DOI: 10.15680/IJIRSET.2026.1504036|

A Dynamic Cybersecurity Risk Assessment Framework for Connected and Automated Vehicles

S. S. Vaishnavi[1], M. Nimuna[2], M. Prasanya[3], J. Vijayalakshmi[4], M. Nithya[5], M. Mohamed Faisal[6]

U.G. Student, Department of Computer Science and Engineering, Sir Issac Newton College of Engineering and Technology, Nagappatinam, Tamilnadu, India [1234]

Assistant Professor, Department of Computer Science and Engineering, Sir Issac Newton College of Engineering and Technology, Nagappatinam, Tamilnadu, India[5]

Assistant Professor and Head, Department of Computer Science and Engineering, Sir Issac Newton College of Engineering and Technology, Nagappatinam, Tamilnadu, India[6]

ABSTRACT: A Machine Learning–based Cybersecurity risk assessment framework is proposed for Connected and Automated Vehicles (CAVs) to overcome the limitations of traditional Threat Assessment and Risk Analysis (TARA) methods. The system integrates Artificial Neural Networks (ANN), Random Forest, and Gradient Boosting algorithms to detect and classify cyber-attacks with high accuracy. The framework processes heterogeneous data sources such as sensor logs, V2X communications, and network traffic. Data preprocessing includes iterative imputation to handle missing values, SMOTE for class imbalance, and min–max normalization for feature scaling. Gradient Boosting evaluates structured risk factors such as impact scores, feasibility ratings, and SAE automation levels, while Random Forest improves feature selection and reduces overfitting. A hybrid ANN model captures complex spatiotemporal patterns and performs both binary (attack/no attack) and multi-label classification, including sensor spoofing and data leakage. The system achieves strong performance, with 92% accuracy using ANN, 89% F1-score with Gradient Boosting, and 87% precision with Random Forest. It also supports real-time inference with low latency, making it suitable for in-vehicle deployment. Additionally, explainable AI techniques are incorporated to enhance transparency and support regulatory compliance.

KEYWORDS: Machine Learning, Cybersecurity Connected Vehicles, Risk Assessment, Artificial Neural Networks, Random Forest.

I. INTRODUCTION

Connected and Automated Vehicles (CAVs) are revolutionizing transportation by integrating sensors, artificial intelligence, and vehicle-to-everything (V2X) communication. These technologies enable safer driving, improved traffic management, and enhanced user experience. However, the same connectivity also exposes vehicles to cybersecurity risks such as spoofing, data leakage, and unauthorized access, which can compromise both safety and privacy. Traditional Threat Analysis and Risk Assessment (TARA) methods rely heavily on static evaluation and expert judgment, making them inadequate for addressing dynamic and complex threats in automated environments. As vehicles evolve toward higher levels of autonomy, the need for adaptive and intelligent risk assessment becomes critical. Machine learning techniques offer promising solutions by analyzing heterogeneous data, identifying attack patterns, and predicting risks in real time. This

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 4, April 2026

|DOI: 10.15680/IJIRSET.2026.1504036|

paper proposes a dynamic cybersecurity risk assessment framework that integrates ANN, Random Forest, and Gradient Boosting to enhance detection accuracy and support real-time decision-making in CAV systems.

II. LITERATURE SURVEY

Several frameworks have been proposed to address cybersecurity in Connected and Automated Vehicles (CAVs). EVITA introduced a security architecture for Electronic Control Units (ECUs) using Threat Assessment and Risk Analysis (TARA), but it was limited to legacy systems without considering V2X or AI vulnerabilities [1]. HEAVENS aligned with ISO/SAE 21434 and emphasized structured threat modelling relied on static evaluation and lacked real-time adaptability [2]. PIER extended TARA by integrating privacy analysis through LINDDUN, highlighting risks of personal data exposure, though it lacked quantitative scoring and higher automation coverage [3]. ISO/SAE 21434 formalized risk assessment across the vehicle lifecycle but depended heavily on expert judgment, leading to inconsistencies [4]. TARA+ introduced driver controllability metrics for Level 3 automation but did not address fully autonomous scenarios [5]. STRIDE-LINDDUN analysis identified privacy threats such as location tracking and sensor leakage but remained qualitative [6]. Automated attack path analysis tools like ThreatGet reduced manual effort but required extensive input preparation [7]. Studies on L4/L5 systems emphasized risks such as sensor spoofing and AI model poisoning but lacked concrete frameworks [8]. ISO/SAE 21434 formalized risk assessment across the vehicle lifecycle but depended heavily on expert judgment, leading to inconsistencies [9]. UNECE R155 mandated cybersecurity management systems for type approval but treated all automation levels uniformly and overlooked privacy depth [10]. Collectively, these works highlight the need for a dynamic, machine learning-based framework that integrates security and privacy, adapts to automation levels, and supports real-time risk prediction.

III. METHODOLOGY

The proposed cybersecurity risk assessment framework for Connected and Automated Vehicles (CAVs) integrates machine learning techniques to enhance threat detection and classification. The methodology begins with data collection from heterogeneous sources such as V2X communication logs, sensor outputs, and network traffic. This raw data undergoes preprocessing, including normalization, feature extraction, and dimensionality reduction, to ensure consistency and improve model performance.

Three machine learning algorithms are employed: Artificial Neural Networks (ANN), Random Forest, and Gradient Boosting. ANN is used for capturing complex nonlinear relationships in attack patterns, while Random Forest provides robust classification through ensemble decision trees. Gradient Boosting further improves predictive accuracy by iteratively minimizing errors. Each model is trained and validated using labelled datasets representing different cyber-attack scenarios, including spoofing, denial-of-service, and unauthorized access.

The framework evaluates model performance using metrics such as accuracy, precision, recall, and F1-score. Comparative analysis ensures that the most effective algorithm is selected for real-time deployment. Finally, the system integrates a decision support module that provides risk scores and alerts to automotive controllers, enabling proactive defence. This methodology reduces reliance on static expert judgment and supports adaptive, real-time cybersecurity management in CAV environments.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 4, April 2026

|DOI: 10.15680/IJIRSET.2026.1504036|

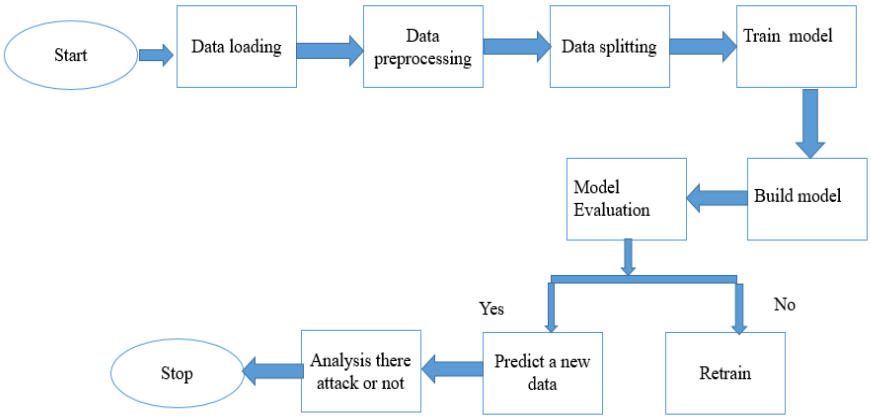


Figure 1: Flow Diagram

The flow diagram (Figure 1) illustrates the sequential process of data collection, preprocessing, model training, and risk scoring. It highlights how ANN, Random Forest, and Gradient Boosting are integrated to detect and classify cyber threats in real time.

IV. EXPERIMENTAL RESULTS

Figure 2 shows the login page of the system, providing secure access for authorized users, while Figure 3 represents the registration page for new user account creation. Figure 4 presents the data selection interface for choosing relevant features, and Figure 5 depicts the data preprocessing stage, including cleaning and normalization. Figure 6 shows the data visualization module for graphical analysis, while Figure 7 demonstrates the privacy assessment page for identifying privacy-related risks. Figure 8 represents the attack simulation module used to analyse potential cyber threats. Figure 9 illustrates the real-time monitoring system for continuous threat detection, while Figure 10 shows the prediction interface where input data is analysed using trained models. Finally, Figure 11 and Figure 12 display the prediction result pages, presenting detected threats along with corresponding risk levels and evaluation metrics.

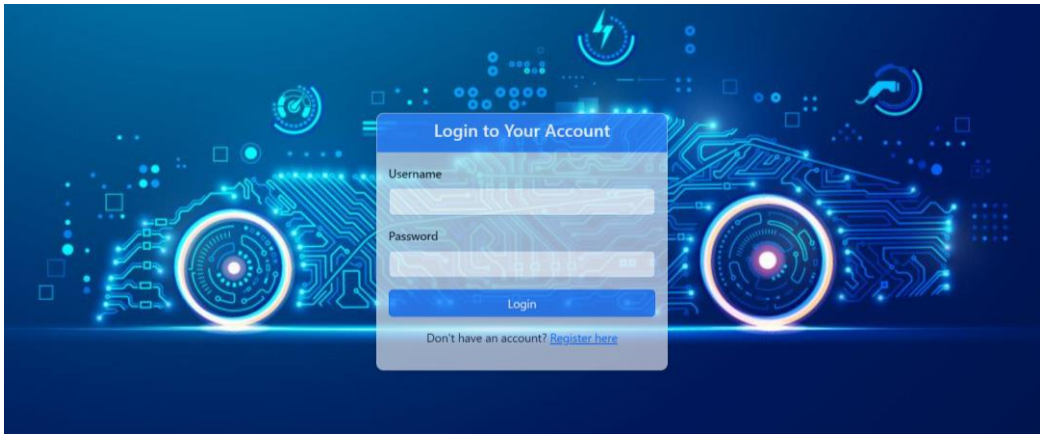


Figure 2: Login Page

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 4, April 2026

|DOI: 10.15680/IJIRSET.2026.1504036|

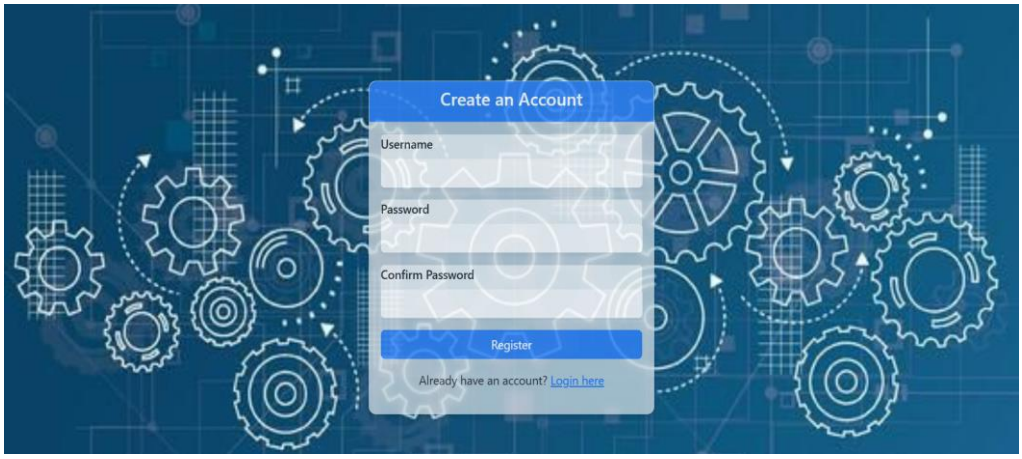


Figure 3: Register Page

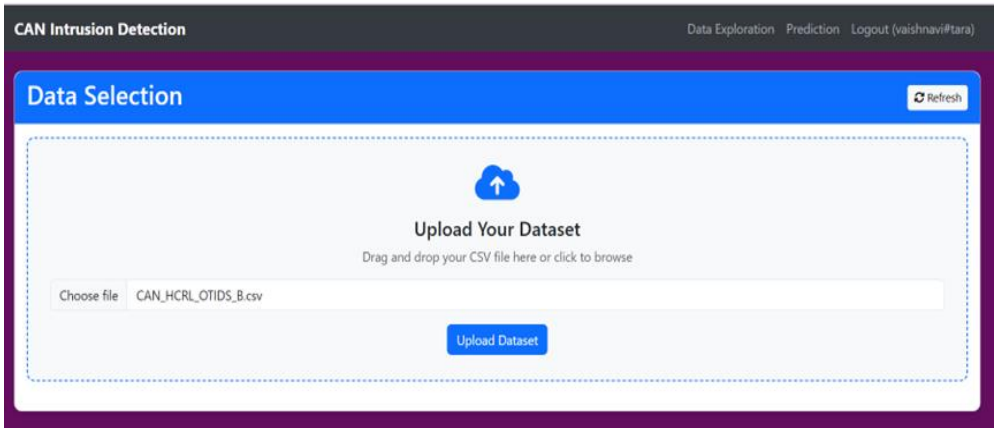


Figure 4: Data Selection

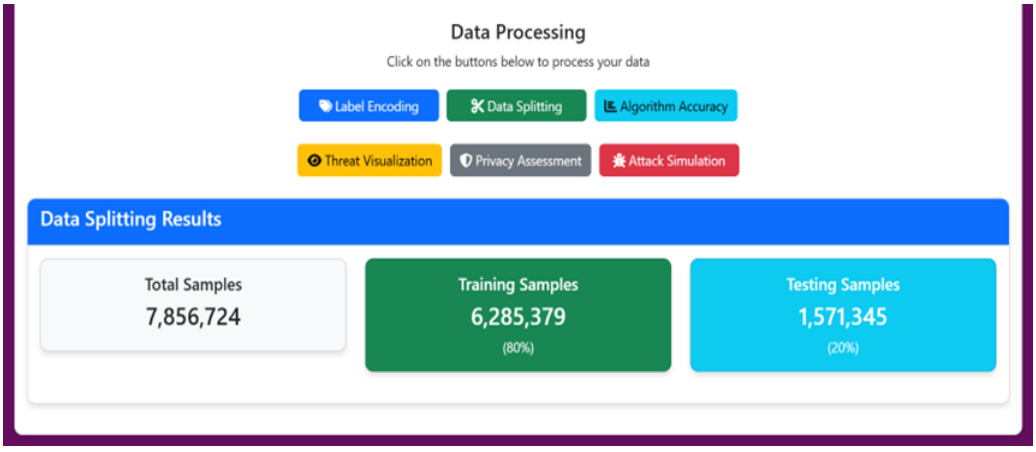


Figure 5: Data Preprocessing

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 4, April 2026

|DOI: 10.15680/IJIRSET.2026.1504036|

Figure 6: Data Visualization

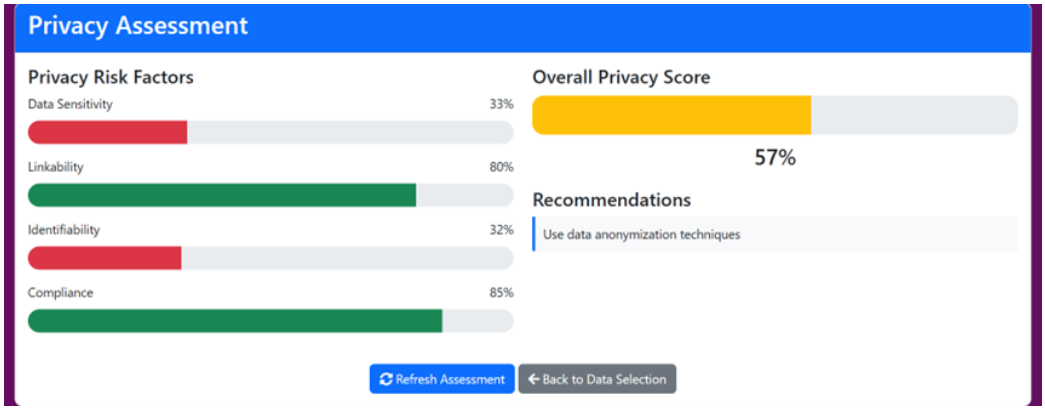


Figure 7: Privacy Assessment

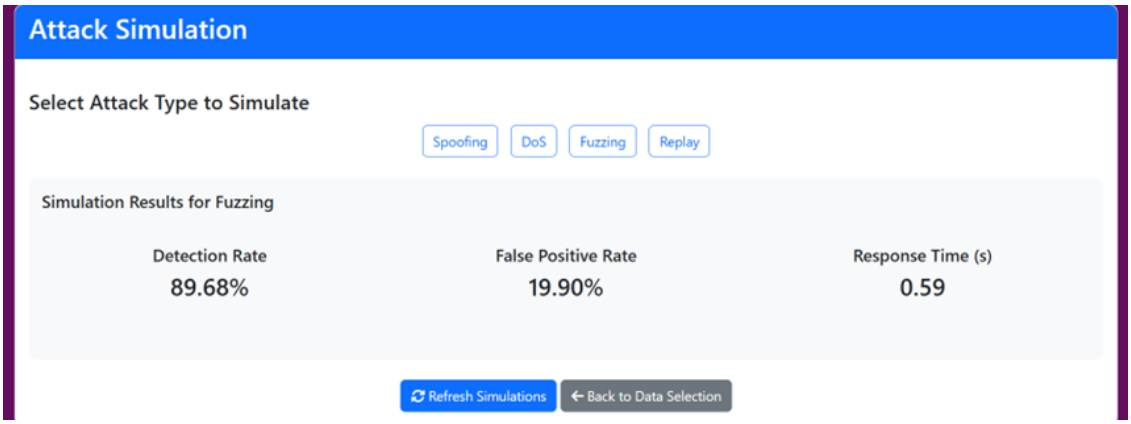


Figure 8: Attack Simulation

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 4, April 2026

|DOI: 10.15680/IJIRSET.2026.1504036|

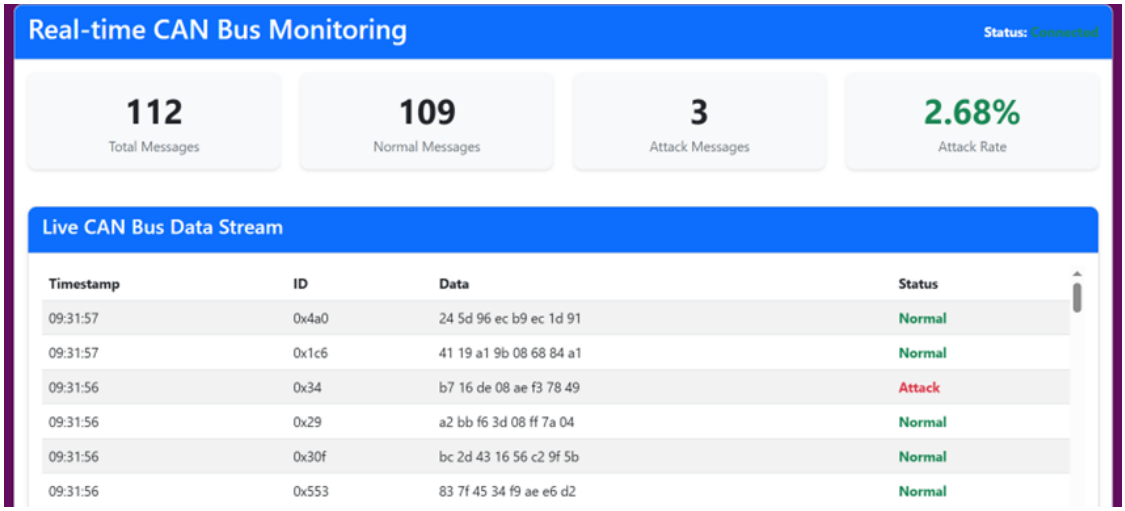


Figure 9: Real Time Monitoring

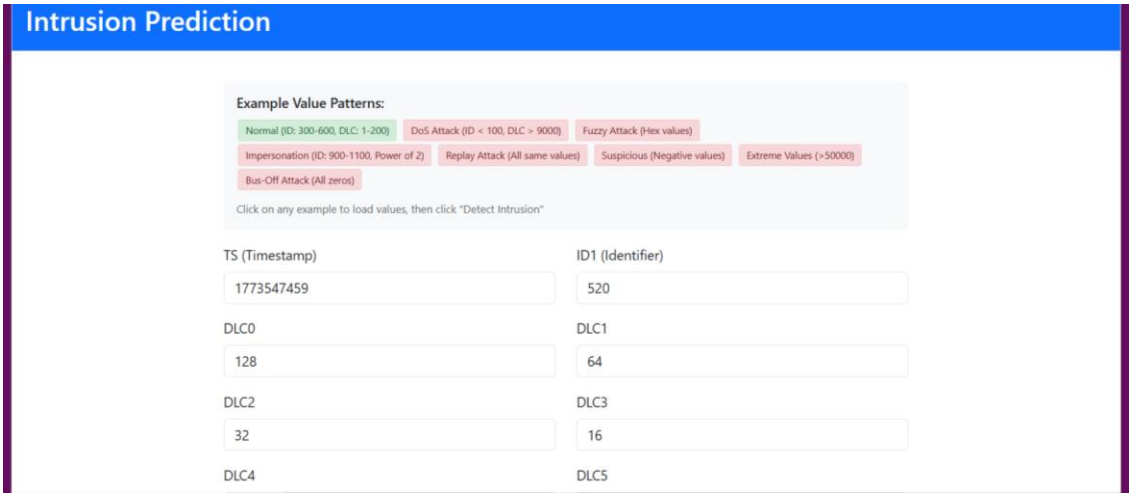


Figure 10: Prediction Interface

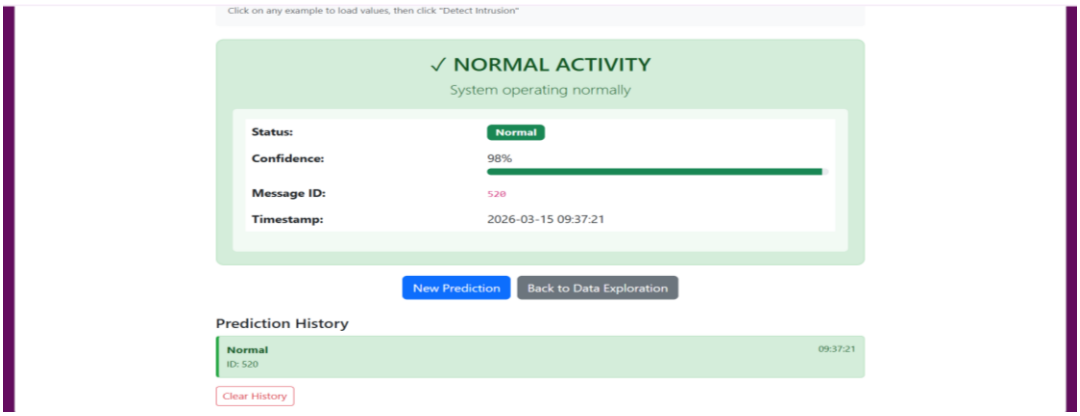


Figure 11: Prediction Result 1

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 4, April 2026

|DOI: 10.15680/IJIRSET.2026.1504036|

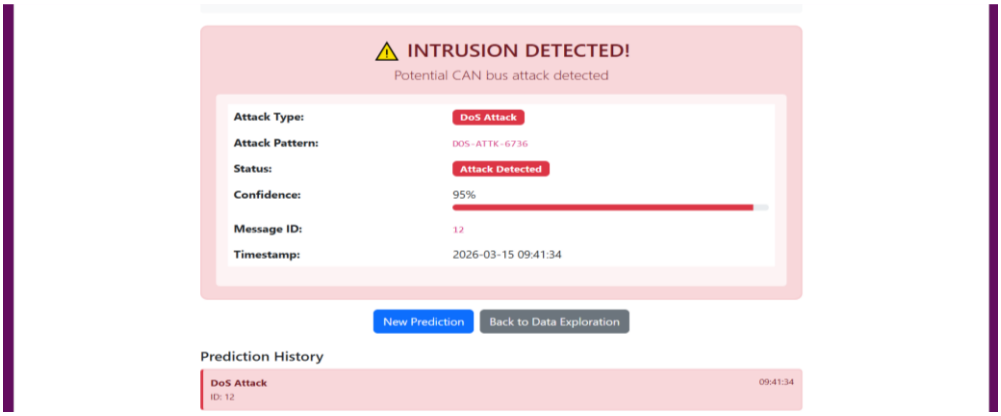


Figure 12: Prediction Result 2

V. CONCLUSION

The proposed framework enhances traditional TARA by integrating machine learning for dynamic risk assessment in CAVs. It improves detection accuracy, supports real-time deployment, and incorporates explainable AI for transparency. Future work will extend the framework to higher SAE automation levels and integrate blockchain-based security for V2X communication. The study demonstrates that integrating machine learning into cybersecurity risk assessment significantly enhances detection accuracy and adaptability for Connected and Automated Vehicles. The hybrid framework not only addresses evolving cyber threats but also incorporates privacy-aware analysis and explainable AI for transparency. This research contributes a practical foundation for future intelligent transportation systems, ensuring safer and more resilient autonomous vehicle ecosystems.

REFERENCES

[1] M. Wolf, A. Weimerskirch, and T. Wollinger, "EVITA: E-safety Vehicle Intrusion Protected Applications," in Proceedings of ESCAR, 2011.
[2] T. Müller, J. Stöttinger, and R. Kurmus, "HEAVENS: A Framework for Automotive Security," in Proceedings of ESCAR, 2017.
[3] A. Monteuuis and J. Traoré, "PIER: Privacy-Preserving Risk Assessment for Connected and Automated Vehicles," in Proceedings of IEEE VTC, 2020.
[4] T. Müller, J. Stöttinger, and R. Kurmus, "HEAVENS: Threat Analysis and Risk Assessment Methodology for Automotive Systems," Journal of Automotive Security, vol. 5, no. 2, pp. 45–56, 2017.
[5] S. Ruddle, "TARA+: Enhanced Threat Analysis and Risk Assessment for Level 3 Automation," in Automotive Cybersecurity Conference, 2019.
[6] A. van der Heijden, "Applying STRIDE and LINDDUN for Privacy Threats in Connected Vehicles," IEEE Security & Privacy Workshops, 2020.
[7] AVL List GmbH, "ThreatGet: Automated Attack Path Analysis Tool for Automotive Systems," Technical Report, 2021.
[8] Y. Sun, H. Zhang, and K. Chen, "Cybersecurity Risks in L4/L5 Autonomous Driving Systems," IEEE Transactions on Intelligent Transportation Systems, vol. 22, no. 4, pp. 2345–2356, 2021.
[9] International Organization for Standardization and SAE International, "ISO/SAE 21434: Road Vehicles Cybersecurity Engineering," ISO Standard, pp. 1–200, 2021.
[10] UNECE, "Regulation No. 155: Cybersecurity and Cybersecurity Management System," United Nations Economic Commission for Europe, 2021.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details