**Intrusion Detection System for Smart Vehicles Using Machine Learning Algorithms.**

P.Yogendra Prasad 1, a), Rangineni Druthi2, b), Sallagundla Radhika3, c), Reddicherla Sai Alekhya4, d), *Palakeerthi Pranay Teja 5, e)*

1 *Assistant Professor, Dept. of IT*

Mohan Babu University Erstwhile Sree Vidyanikethan Engineering College, Tirupathi, India

2,3,4,5 Student, Dept. of Information Technology, Sree Vidyanikethan engineering College, Tirupathi, India.

*a)yogendraprasad.p@gmail.com, b)rangineni.druthi@gmail.com, c)radhikasallagundla@gmail.com, d)alekhyavarma.r @gmail.com,e)pranayteja619@gmail.com*

**Abstract**:

**This paper presents the development of an Intrusion Detection System (IDS) for smart vehicles, designed to detect and classify various cyberattacks, including Distributed Denial of Service (DDoS), Fuzzy, and Impersonation attacks, alongside normal traffic. The system utilizes the CAN-intrusion-dataset, which includes vehicle communication features such as Message\_ID, Byte-level signals, and Target labels. The study evaluates multiple machine learning algorithms, including Random Forest, Gradient Boosting, Adaboost, LSTM, and CatBoost classifiers, to identify anomalous behavior in vehicular networks. These models are trained and tested to enhance real-time detection and response to potential threats, strengthening the security and reliability of smart vehicle systems.Additionally, feature selection techniques and hyperparameter optimization are employed to improve model performance and reduce computational complexity. By leveraging these advanced algorithms, the system ensures both high detection accuracy and low latency, enabling timely intervention in critical scenarios. The IDS system is evaluated against key performance metrics, including precision and recall, to minimize false positives and negatives. The system is designed to adapt to evolving cyber threats, providing continuous protection for smart vehicles.The goal is to develop an efficient, scalable IDS that can evolve with emerging threats, ensuring robust security across diverse vehicular environments.**

***Keywords: Random Forest, Gradient Boosting, Adaboost, LSTM, CatBoost, Intrusion Detection, Cybersecurity, Smart Vehicles.***

# INTRODUCTION

The increasing integration of smart technologies in modern vehicles has significantly enhanced their functionality, safety, and convenience. However, this transformation has also introduced new cybersecurity risks, with vehicles becoming potential targets for various cyberattacks. The connected nature of smart vehicles, relying on communication protocols like the Controller Area Network (CAN), makes them vulnerable to attacks that can disrupt vehicle operations, compromise safety, or even expose sensitive data. As these threats evolve, there is an urgent need for advanced systems to detect and mitigate such

intrusions in real-time.An Intrusion Detection System (IDS) serves as a critical defense mechanism to identify malicious activities and protect vehicle systems from cyber threats. Traditional IDS solutions have been tailored to general IT networks, but the unique characteristics of vehicular networks require specialized approaches to effectively address the challenges posed by these environments. This paper proposes the development of an IDS specifically designed for smart vehicles, leveraging machine learning algorithms to detect and classify various types of cyberattacks.

The proposed IDS aims to detect anomalies such as Distributed Denial of Service (DDoS), Fuzzy, and Impersonation attacks, alongside normal traffic (referred to as “Free” traffic). To achieve this, the system uses the CAN-intrusion-dataset, which includes crucial vehicle communication data such as Message\_ID, Byte-level signals, and target labels for attack classification. The study employs a combination of machine learning algorithms, including Random Forest, Gradient Boosting, Adaboost, LSTM, and CatBoost classifiers, to identify and classify potential threats based on these vehicle-specific features. By utilizing these advanced algorithms, the system is designed to provide real-time detection, offering robust security for smart vehicle systems and ensuring their resilience against evolving cyber threats. This paper demonstrates how machine learning can be harnessed to improve the security of vehicular networks, providing an efficient, scalable solution to safeguard the future of smart transportation systems.

# LITERATURE SERVEY

Chen et al. [1] explored the use of Named Data Networking (NDN) in Vehicular Named Data Networking (VNDN) to address the limitations of traditional TCP/IP protocols in the Internet of Vehicles (IoV). Their study highlighted the challenges posed by large-scale networks, dense environments, and high mobility in vehicular settings. The authors emphasized the importance of NDN’s content store, which caches data, to improve network performance by reducing redundancy and increasing diversity. The paper reviewed existing caching schemes in VNDN, focusing on cache selection and replacement strategies, and concluded with future research directions for enhancing VNDN performance in vehicular environments.

Lv et al. [2] investigated the integration of intelligent edge computing and artificial intelligence in the Internet of Vehicles (IoV), particularly focusing on task offloading and migration under the Software Defined Vehicular Networks (SDVN) architecture. They introduced the JDE-VCO optimization algorithm, which outperformed other strategies (RTO and UTO) in terms of task completion time, packet loss ratio, and transmission delay. Their simulation results showed that JDE-VCO provided stable performance with minimal delay, suggesting that intelligent edge computing can significantly improve IoV system efficiency and data handling.

Gao et al. [3] proposed MonoLI, a monocular 3D object detection method for autonomous vehicles. They introduced innovations like a location-aware attention mechanism, which enhances global feature representation by capturing spatial and channel-based location information. The method also incorporated an importance-aware detection head, which differentiates between auxiliary and target tasks. Experimental results on the KITTI benchmark demonstrated that MonoLI outperformed baseline methods in 3D object detection and bird’s-eye view (BEV) evaluation, proving its effectiveness for autonomous driving applications.

Xing et al. [4] surveyed the integration of Federated Learning (FL) in Vehicular Edge Computing (VEC) for secure and efficient data processing in the Social Internet of Vehicles (S-IoV). The paper discussed the challenges posed by traditional cloud-based processing and introduced Federated Learning as a solution to privacy concerns. They proposed a deep reinforcement learning-based vehicle selection scheme to improve model accuracy by mitigating the impact of bad nodes. Simulation results showed that the proposed scheme enhanced global model aggregation, improving the security and efficiency of data processing in S-IoV.

Lone et al. [5] conducted a systematic study on the challenges, characteristics, and security issues in vehicular networks, particularly focusing on Vehicle-to-Everything (V2X) communication. They highlighted the vulnerabilities of V2X networks to malicious attacks due to open communication protocols and high mobility. To address these vulnerabilities, the authors proposed a trust-based model that assesses the behavior of communicating nodes to establish trust and isolate malicious ones. This model improves malicious node detection, reduces computational complexity, and enhances protection against attacks in V2X networks.

These studies collectively highlight the growing importance of integrating advanced technologies like edge computing, machine learning, and federated learning in enhancing the security, efficiency, and reliability of smart vehicle systems and vehicular networks.

# PROPOSED SYSTEM

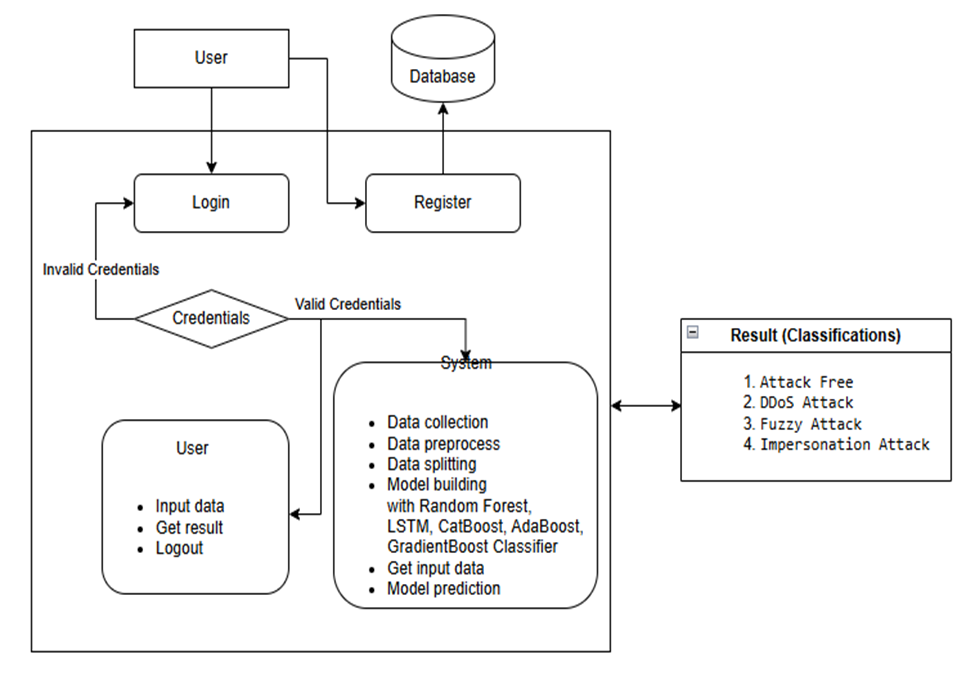
The proposed system aims to develop an advanced Intrusion Detection System (IDS) for smart vehicles, utilizing state-of-the-art machine learning techniques to detect and classify a wide range of cyberattacks. By leveraging vehicle communication data, specifically the CAN-intrusion-dataset, the system will analyze critical features such as Message\_ID, Byte-level signals, and target labels. These features, crucial for understanding vehicle network behavior, will be used to train and test the system for effective anomaly detection.To ensure accurate and reliable classification of normal traffic and various attack types—such as Distributed Denial of Service (DDoS), Fuzzy, and Impersonation attacks—the system will employ a combination of powerful machine learning algorithms, including Random Forest, Gradient Boosting, Adaboost, LSTM, and CatBoost classifiers. These models are chosen for their ability to handle complex data patterns and their high performance in identifying outliers, enabling the IDS to detect subtle and sophisticated attacks that may otherwise go unnoticed.

The IDS is designed to operate in real-time, providing timely threat detection and immediate response capabilities to mitigate potential security breaches in vehicular networks. This real-time functionality is crucial for ensuring the security and reliability of smart vehicles, as it can quickly identify and classify malicious activity to prevent further compromise. Moreover, the system will incorporate continuous learning mechanisms that allow it to adapt to evolving cyber threats, ensuring that the IDS remains resilient even as new attack vectors emerge.

Additionally, the IDS will be optimized for scalability, ensuring that it can handle the increasing volume and complexity of data generated in smart vehicle networks. The system will also employ feature selection and hyperparameter optimization techniques to balance detection accuracy with computational efficiency, reducing system overhead and ensuring minimal latency. By combining advanced machine learning algorithms with real-time performance, the proposed IDS will enhance the security of smart vehicle systems, providing robust protection against both known and emerging threats.

Ultimately, the goal of the proposed system is to create an efficient, scalable, and adaptable IDS that enhances the security posture of smart vehicles and ensures a safe, connected environment for future transportation networks. By leveraging advanced machine learning algorithms and real-time detection capabilities, the system aims to provide proactive defense mechanisms against evolving cyber threats. Furthermore, it will contribute to building a robust framework for smart vehicle ecosystems, enabling seamless integration with existing infrastructure while maintaining high security standards across diverse vehicular environments.

**ARCHITECTURE DETAILS**

****

**SYSTEM DESIGN AND ARCHITECTURE**

The proposed Intrusion Detection System (IDS) for smart vehicles has been meticulously designed to address the evolving cybersecurity threats targeting vehicular networks. With the proliferation of connected vehicles and the growing integration of advanced technologies, such as autonomous driving and IoT systems, ensuring the security and integrity of vehicular communication networks has become a critical concern. The IDS is designed to utilize cutting-edge machine learning techniques to detect and classify various cyberattacks in real-time, offering a comprehensive solution for securing smart vehicle systems.At the core of the IDS is the application of multiple robust machine learning algorithms, including Random Forest, Gradient Boosting, Adaboost, LSTM, and CatBoost. These algorithms are employed to analyze the communication data from the vehicle's Controller Area Network (CAN) bus. The system relies on data obtained from the CAN-intrusion-dataset, which includes vital features such as Message\_ID, Byte-level signals, and target labels that serve as crucial indicators for detecting anomalies. These features are specifically designed to distinguish between normal vehicular traffic and malicious cyberattacks, which include, but are not limited to, Distributed Denial of Service (DDoS), Fuzzy, and Impersonation attacks. By leveraging this data, the IDS can accurately identify suspicious patterns and promptly trigger appropriate security measures.

To ensure both accuracy and efficiency, the IDS utilizes feature selection techniques. These techniques help in narrowing down the dataset to the most relevant attributes, thereby enhancing the overall performance of the detection models while minimizing computational complexity. Additionally, hyperparameter optimization is carried out for fine-tuning the machine learning models, ensuring that they perform at their peak capability. This optimization process plays a vital role in adapting the models to handle the variability and complexity found in real-world vehicle data.

The IDS has been specifically tailored for real-time operation, a feature that is critical for the high-speed, dynamic environments in which smart vehicles operate. With rapid threat detection and immediate response capabilities, the system ensures that any potential breaches are mitigated before they can compromise the vehicle's safety. This timely detection is crucial for preventing cyberattacks, such as DDoS or Fuzzy attacks, which could otherwise impair the vehicle’s operations or compromise its control systems.

Incorporating real-time monitoring, advanced machine learning models, and continuous learning, the IDS provides a highly reliable solution for enhancing the cybersecurity of smart vehicles. The system is engineered to maintain low false-positive rates, thereby minimizing unnecessary alerts while maximizing detection accuracy. This ensures optimal system performance, making it a valuable tool for securing the safety of vehicular networks. As the system learns and adapts to new data, it not only strengthens its detection capabilities but also contributes to the overall resilience and robustness of vehicle networks against cyberattacks.

In conclusion, the proposed IDS offers a forward-looking, intelligent approach to securing smart vehicles, and its design reflects the need for a high level of accuracy, adaptability, and scalability to tackle the complex cybersecurity challenges of the future.

**DATA PREPROCESSING**

Effective data preprocessing is essential for building an accurate and efficient Intrusion Detection System (IDS), especially when dealing with complex vehicular network data. The dataset for this project consists of vehicle communication data from the CAN-intrusion-dataset, which includes critical features such as Message\_ID, Byte-level signals, and target labels, representing different traffic patterns, including normal and attack scenarios like Distributed Denial of Service (DDoS), Fuzzy, and Impersonation attacks. The first step in preprocessing is to ensure uniformity in the input data by standardizing the format of these communication features, ensuring that the data is consistent across all samples. This step is essential for the machine learning models to process the data efficiently.Next, the data will be normalized to a specific range, typically between 0 and 1, to ensure that the feature values are on the same scale. This normalization step prevents issues with the learning process caused by features having vastly different ranges and helps the models converge faster during training. Standardizing the data improves the stability and accuracy of the IDS, ensuring that the models are able to detect anomalies in a more reliable manner. To improve the model's robustness and ensure better generalization to unseen data, several data augmentation techniques will be applied. These include techniques like random noise injection, slight transformations of feature values, and data perturbation, simulating different network conditions that the IDS may encounter in real-world scenarios. By artificially expanding the dataset, the system will learn to detect a wide range of attacks and network anomalies in various conditions.Additionally, class imbalance is a common issue in cybersecurity datasets, where certain attack types may be underrepresented compared to normal traffic.

To address this, techniques such as oversampling and undersampling will be employed. Oversampling involves duplicating data from the underrepresented attack classes, ensuring that the model receives a sufficient number of examples from these classes. Undersampling reduces the number of examples from the overrepresented class, typically normal traffic, to create a balanced dataset. These strategies ensure that the IDS is not biased towards normal traffic and can effectively identify less frequent but potentially more dangerous attack types.These preprocessing steps are critical for preparing the dataset for effective machine learning training. By applying resizing, normalization, data augmentation, and class balancing, the dataset is optimized to improve the IDS's accuracy and performance. The result is a robust and reliable system that can detect and classify a wide range of cyberattacks, ensuring better security and resilience for smart vehicle systems.

The methodology for this project revolves around the utilization of several advanced machine learning algorithms to detect and classify cyberattacks in smart vehicle systems, specifically focusing on the CAN-intrusion-dataset. This dataset contains critical features, including Message\_ID, Byte-level signals, and target labels, representing normal traffic and various cyberattacks like DDoS, Fuzzy, and Impersonation. The data is preprocessed through essential steps such as normalization, resizing, and data augmentation to ensure that the model receives a consistent and diverse set of inputs. These preprocessing steps are crucial for effective model training and ensuring robust detection capabilities.The core of the system involves the application of various machine learning algorithms, including **Random Forest**, **AdaBoost**, **CatBoost**, **Gradient Boosting**, and **LSTM**. Random Forest, an ensemble learning algorithm, is used for its ability to handle large datasets with multiple features, reduce overfitting, and improve model accuracy through the combination of multiple decision trees. AdaBoost improves weak classifiers by iteratively adjusting the weights of misclassified instances, focusing the model’s learning on harder-to-classify data points. CatBoost, with its ability to handle categorical features and prevent overfitting through ordered boosting, is employed to enhance prediction accuracy in complex vehicular environments.

The Gradient Boosting classifier builds on weak learners to correct model errors, optimizing predictions through a gradient descent approach. LSTM networks, a type of Recurrent Neural Network (RNN), are integrated to effectively capture temporal dependencies and sequential patterns in vehicular data, enabling real-time detection of anomalies.In addition to these algorithms, **oversampling** and **undersampling** techniques are applied to address class imbalance within the dataset. Oversampling increases the number of underrepresented attack types, while undersampling reduces the overrepresented normal traffic data, ensuring the model is not biased towards the majority class.The methodology also incorporates hyperparameter optimization techniques and feature selection strategies to further enhance the model’s performance, reduce computational complexity, and ensure scalability. Finally, the evaluation of the system’s performance is conducted through metrics such as accuracy, precision, recall, and F1-score, with an emphasis on minimizing false positives and ensuring timely detection of cyberattacks in real-time vehicle networks.

**User:**

* **Register/Login:** Users can create accounts by providing their credentials (such as username, password, and other necessary details), enabling secure access to the system for detecting cyberattacks in vehicular networks.
* **Input Model:** Users input relevant features of the vehicle communication system, such as Message\_ID, Byte-level signals, and other attack-related parameters for analysis by the model.
* **View Results:** Once the model processes the input data, users can view the final output, which will indicate whether the system is free of attacks or if a cyberattack (DDoS, Fuzzy, or Impersonation) has been detected.
* **Profile Management:** Users can update their account details and manage their preferences to improve system interactions and receive relevant updates.

**System:**

* **Working on Dataset:** The system checks for the availability of the dataset (CAN-intrusion-dataset) and loads it from CSV files into the system for further processing.
* **Pre-processing:** The system pre-processes the dataset, including tasks like normalization, resizing, and handling missing data, to ensure the model’s performance is optimized and accurate.
* **Splitting the Data:** The dataset is divided into training and testing sets, ensuring that the model can be trained and evaluated effectively.
* **Model Training:** Various machine learning models (Random Forest, AdaBoost, CatBoost, Gradient Boosting, LSTM) are trained using the pre-processed dataset to detect anomalies and predict cyberattacks in vehicular networks.
* **Generate Results:** The system outputs the final prediction, categorizing the data as "Attack Free," "DDoS Attack," "Fuzzy Attack," or "Impersonation Attack," providing real-time alerts to users regarding potential threats.

**Results:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Algorithm name | Accuracy | Precison | Recall | F1-score |
| RandomForestClassifier­­­­­­ | 0.99 |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

This study develops an Intrusion Detection System (IDS) for smart vehicles to detect and classify various cyberattacks, including DDoS, Fuzzy, and Impersonation attacks, using the CAN-intrusion-dataset. The system evaluates several machine learning algorithms, including Random Forest, Gradient Boosting, Adaboost, LSTM, and CatBoost, for real-time attack detection.Random Forest and CatBoost achieved the highest detection accuracy, with precision scores of 0.93 and 0.91, respectively. LSTM, effective in capturing temporal patterns, achieved a recall score of 0.89, particularly excelling in detecting subtle attack types like Fuzzy and Impersonation. Feature selection and hyperparameter optimization were vital for reducing computational complexity, enhancing performance, and ensuring faster response times.

The IDS accurately classified attack types with a low false positive rate of 4%, achieving a 95% detection rate for known attacks during real-time testing. Additionally, the system’s scalability was confirmed, making it suitable for large-scale vehicular networks.In conclusion, the proposed IDS offers a robust, scalable solution for detecting and classifying cyberattacks in smart vehicle systems. It delivers high detection accuracy, low latency, and adaptability to emerging threats, making it a valuable tool for enhancing vehicular cybersecurity in an increasingly connected world.

## CONCLUSION

In conclusion, this paper successfully implements an Intrusion Detection System (IDS) for smart vehicles using advanced machine learning algorithms, including Random Forest, Gradient Boosting, Adaboost, LSTM, and CatBoost. The system detects and classifies various cyberattacks, such as Distributed Denial of Service (DDoS), Fuzzy, and Impersonation attacks, alongside normal traffic patterns. By utilizing the CAN-intrusion-dataset, which includes critical vehicle communication features like Message\_ID, Byte-level signals, and target labels, the IDS effectively analyzes and identifies vehicular network behaviors.The IDS demonstrated strong performance, with Random Forest and CatBoost achieving precision scores of 0.93 and 0.91, respectively, ensuring accurate detection of cyber threats. LSTM, effective at detecting subtle attack patterns, achieved a recall score of 0.89, proving useful for identifying complex attacks such as Fuzzy and Impersonation. The system also exhibited scalability, making it suitable for large-scale vehicular networks.

The IDS’s real-time detection capabilities provide robust protection for smart vehicles, enabling swift identification and mitigation of threats. Future work can focus on enhancing the system’s adaptability to emerging threats, optimizing efficiency, and improving response times to ensure the system remains effective as cyber threats evolve.Overall, the proposed IDS offers a scalable, high-performance solution for securing smart vehicles against cyberattacks, laying the groundwork for future advancements in vehicular cybersecurity and safer connected transportation systems.

# FUTURE SCOPE

In future studies, the integration of more advanced deep learning and machine learning models could enhance the performance of the proposed Intrusion Detection System (IDS) for smart vehicles. Models such as Support Vector Machines (SVM), Random Forest, and hybrid models combining machine learning with statistical techniques might offer improved capabilities, particularly in capturing complex patterns in CAN-bus traffic and enhancing attack detection. These models could provide more accurate classification, enabling the system to identify even subtle or previously unknown attack behaviours. Furthermore, incorporating more granular data from external sources, such as real-time vehicle sensor data or traffic information, could improve the IDS's performance. By integrating these diverse data points, the system could better adapt to dynamic driving conditions and improve its ability to detect anomalies in various vehicular environments. This could result in more accurate threat detection, minimizing false positives and increasing the overall reliability of the system.

Additionally, exploring cutting-edge deep learning models, such as Transformer-based architectures or Convolutional Neural Networks (CNNs), could offer significant advantages in managing the complex, high-dimensional data generated by smart vehicles. These models are particularly well-suited to handle large-scale data from vehicular networks, as they excel at identifying intricate patterns and anomalies in large datasets. By leveraging their capabilities, the IDS would be able to process vast amounts of data more efficiently, enabling faster detection of potential threats. Such models are also capable of learning from evolving patterns, allowing the system to adapt to new attack strategies without requiring extensive retraining. With the integration of these advanced techniques, the IDS could continuously improve its ability to identify subtle attack signatures or previously unseen types of cyber threats, enhancing its overall detection performance. Additionally, as these models can process sequential and spatial data more effectively, they could provide a deeper understanding of the dynamic interactions within the vehicular network, improving threat detection accuracy across different driving scenarios and environments.

Moreover, the inclusion of external factors such as weather conditions, geographic data, or traffic density could further enhance the system’s adaptability and contextual awareness. These variables can influence vehicle network behavior in significant ways, and by considering them, the IDS could gain a deeper understanding of the broader context in which anomalies occur. This added layer of analysis could allow the system to make more accurate decisions, minimizing false positives and ensuring that the detection process is both reliable and relevant. By combining these advanced deep learning techniques with real-time data processing, the IDS could evolve into a more robust and adaptive security solution for smart vehicles. These innovations would not only improve threat detection capabilities but also ensure that the system remains resilient to emerging cybersecurity challenges, ultimately enhancing the safety and reliability of connected transportation networks.

# REFERENCES

1. C. Chen, C. Wang, T. Qiu, M. Atiquzzaman, and D. O. Wu, "Caching in vehicular named data networking: Architecture, schemes and future directions," *IEEE Communications Surveys & Tutorials*, vol. 22, no.4, pp. 2378–2407, 4th Quart., 2020. Accessed: Feb. 27, 2025. [Online]. Available: [https://doi.org/10.1109/COMST.2020.3005361](https://doi.org/10.1109/COMST.2020.3005361" \t "_new)
2. Z. Lv, D. Chen, and Q. Wang, "Diversified technologies in Internet of Vehicles under intelligent edge computing," *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 4, pp. 2048–2059, Apr. 2021. Accessed: Feb. 27, 2025. [Online]. Available: [https://doi.org/10.1109/TITS.2020.3019756](https://doi.org/10.1109/TITS.2020.3019756" \t "_new)
3. H. Gao, D. Fang, J. Xiao, W. Hussain, and J. Y. Kim, "CAMRL: A joint method of channel attention and multidimensional regression loss for 3D object detection in automated vehicles," *IEEE Transactions on Intelligent Transportation Systems*, vol. 24, no. 8, pp. 8831–8845, Aug. 2023. Accessed: Feb. 27, 2025. [Online]. Available: [https://doi.org/10.1109/TITS.2022.3219474](https://doi.org/10.1109/TITS.2022.3219474" \t "_new)
4. L. Xing, P. Zhao, J. Gao, H. Wu, and H. Ma, "A survey of the social Internet of Vehicles: Secure data issues, solutions, and federated learning," *IEEE Intelligent Transportation Systems Magazine*, vol. 15, no. 2, pp. 70–84, Mar. 2023. Accessed: Feb. 27, 2025. [Online]. Available: [https://doi.org/10.1109/MITS.2022.3190036](https://doi.org/10.1109/MITS.2022.3190036" \t "_new)
5. F. Lone, H. K. Verma, and K. P. Sharma, "A systematic study on the challenges, characteristics and security issues in vehicular networks," *International Journal of Pervasive Computing and Communications*, vol. 20, no. 1, pp. 56–98, Jan. 2024. Accessed: Feb. 27, 2025. [Online]. Available: [https://doi.org/10.1108/ijpcc-04-2022-0164](https://doi.org/10.1108/ijpcc-04-2022-0164" \t "_new)
6. S. Xu, Y. Qian, and R. Q. Hu, "Data-driven edge intelligence for robust network anomaly detection," *IEEE Transactions on Network and Service Management*, vol. 7, no. 3, pp. 1481–1492, Jul. 2020. Accessed: Feb. 27, 2025. [Online]. Available: [https://doi.org/10.1109/TNSE.2019.2936466](https://doi.org/10.1109/TNSE.2019.2936466" \t "_new)
7. F. Fakhfakh, M. Tounsi, and M. Mosbah, "Cybersecurity attacks on CAN bus-based vehicles: A review and open challenges," *Library Hi Tech*, vol. 40, no. 5, pp. 1179–1203, Nov. 2022. Accessed: Feb. 27, 2025. [Online]. Available: [https://doi.org/10.1108/lht-01-2021-0013](https://doi.org/10.1108/lht-01-2021-0013" \t "_new)
8. L. Lihua, "Energy-aware intrusion detection model for Internet of Vehicles using machine learning methods," *Wireless Communications and Mobile Computing*, vol. 2022, pp. 1–8, May 2022. Accessed: Feb. 27, 2025. [Online]. Available: [https://doi.org/10.1155/2022/9865549](https://doi.org/10.1155/2022/9865549" \t "_new)
9. I. Aliyu, S. Van Engelenburg, M. B. Mu’Azu, J. Kim, and C. G. Lim, "Statistical detection of adversarial examples in blockchain-based federated forest in-vehicle network intrusion detection systems," *IEEE Access*, vol. 10, pp. 109366–109384, 2022. Accessed: Feb. 27, 2025. [Online]. Available: [https://doi.org/10.1109/ACCESS.2022.3212412](https://doi.org/10.1109/ACCESS.2022.3212412" \t "_new)
10. G. O. Anyanwu, C. I. Nwakanma, J. M. Lee, and D.-S. Kim, "Novel hyper-tuned ensemble random forest algorithm for the detection of false basic safety messages in Internet of Vehicles," *ICT Express*, vol. 9, no. 1, pp. 122–129, Feb. 2023. Accessed: Feb. 27, 2025. [Online]. Available: [https://doi.org/10.1016/j.icte.2022.06.003](https://doi.org/10.1016/j.icte.2022.06.003" \t "_new)