Grenze International Journal of Engineering and Technology, January Issue

Securing the Road Ahead: A Comprehensive Review of Hybrid Deep Learning and Optimization-based Intrusion Detection in Vehicular Networks

Sandeep G. Shukla[1] and Monika Bhatnagar[2]
[1]Research Scholar, Department of Computer Science and Engineering, Oriental University, Indore (M.P.), India
Email: sandeep.g.shukla@gmail.com
[2]Supervisor, Department of Computer Science and Engineering, Oriental University, Indore (M.P.), India
Email: monikabhatnagar@oriental.ac.in

***Abstract*— With the rapid evolution of intelligent transportation systems, the integration of Vehicular Ad Hoc Networks (VANETs), Internet of Vehicles (IoV), Industrial IoT (IIoT), and Unmanned Aerial Vehicles (UAVs) has introduced a new range of cybersecurity vulnerabilities. These networks are increasingly targeted by advanced threats such as Denial-of-Service (DoS), Sybil, spoofing, replay, and distributed attacks, which can disrupt real-time communication, compromise safety-critical functions, and breach driver privacy. To address these challenges, researchers have turned to advanced Intrusion Detection Systems (IDS) powered by hybrid DL and ML techniques. This review systematically evaluates recent developments in IDS for vehicular and IoT networks by analysing multiple cutting-edge studies. The models examined include hybrid CNN-LSTM, GRU with attention mechanisms, transfer learning-based IDS, federated learning architectures, and blockchain-enabled detection schemes to name a few. It was found that Several models achieved exceptionally high detection rates—often exceeding 97% to 99.9% accuracy—for both known and zero-day attacks. Feature selection and optimization techniques like PCA, mutual information, particle swarm optimization, and genetic algorithms were commonly used to reduce model complexity and improve performance. The review identifies several research gaps, including a lack of lightweight IDS deployment strategies for resource-constrained environments, limited generalizability across real-world vehicular topologies, and insufficient adaptability to evolving attack vectors. The paper concludes with recommendations for future research, such as incorporating distributed IDS architectures to enhance the robustness and applicability of IDS in next-generation vehicular networks.**

***Index Terms*— Intrusion Detection Systems (IDS), Vehicular Networks, Hybrid Deep Learning, Optimization Techniques, CNN-LSTM.**

I. INTRODUCTION

A. Overview of the Domain

The rapid advancement of Intelligent Transportation Systems (ITS) has revolutionized how modern vehicles interact with their environments, paving the way for more connected, autonomous, and efficient mobility solutions.

Grenze ID: 01.GIJET.12.1.518

At the heart of this transformation are advanced vehicular communication networks such as Vehicular Ad Hoc Networks (VANETs), the Internet of Vehicles (IoV), and Industrial Internet of Things (IIoT) systems. These networks form the digital nervous system of smart vehicles and urban mobility infrastructure, enabling seamless and real-time data exchange between vehicles, road-side units (RSUs), cloud platforms, and edge devices [1]– [3].

Applications built on these technologies support various real-time traffic and safety applications [4]– [6]. Core to their function are communication protocols such as - Controller Area Network (CAN) bus, which governs the interaction among various Electronic Control Units (ECUs) within a vehicle [7].

As vehicles become increasingly software-defined and interconnected, cyber threats such as Denial-of-Service (DoS), replay attacks, spoofing, blackhole routing, and zero-day exploits can compromise the integrity of vehicular operations, endanger human lives, and undermine public trust in intelligent transport technologies [8]– [10].

To address these challenges, researchers have turned to (Intrusion Detection Systems) IDSs, particularly those incorporating ML and Deep Learning (DL), have demonstrated significant potential in detecting both known and emerging attack vectors in real-time [11] - [13].

In recent years, hybrid models that fuse various AI techniques—such as Convolutional Neural Networks (CNNs), Long Short-Term Memory (LSTM) networks, Gated Recurrent Units (GRUs), ensemble classifiers, optimization algorithms (e.g., Particle Swarm Optimization, Genetic Algorithms), and federated learning—have gained traction for their ability to capture both spatial and temporal patterns in vehicular network data [14]. These models offer significant advantages in accuracy, adaptability, and scalability, especially in resource-constrained edge environments common to autonomous vehicles and IIoT systems.

This study provides a structured review of hybrid deep learning and optimization-based intrusion detection techniques for vehicular and IoT networks. We analyse their architectures, detection capabilities, datasets, and deployment challenges. Furthermore, we identify key research gaps and propose directions for developing lightweight, adaptive IDS frameworks for next-generation automotive ecosystems.

B. Problem Statement

Despite the significant advances in AI-based intrusion detection systems for vehicular networks, the research landscape remains fragmented. Most studies focus on specific IDS models or datasets without offering a holistic comparison of methodologies, performance metrics, real-time feasibility, or deployment challenges. A few systematic reviews exist, but they often lack integration of emerging hybrid models and optimization techniques across VANETs, IoV, and IIoT domains.

Therefore, a critical need exists for an in-depth, comparative review that not only categorizes the various IDS approaches but also identifies their strengths, limitations, and future research directions across emerging vehicular and IoT contexts.

C. Key Objectives and Contributions

This paper addresses the above gaps through a structured review and comparison of hybrid machine learning and deep learning approaches for intrusion detection in vehicular networks. The key objectives of this study are:

- To categorize and analyze the current state-of-the-art IDS approaches for VANETs, IoV, IIoT, and UAV networks based on their architecture (ML, DL, hybrid), feature engineering techniques, and optimization strategies.
- To compare model performance across key metrics such as accuracy, F1-score, recall, false positive rate (FPR), and computational cost using reported results from diverse studies.
- To identify research gaps and limitations, including dataset generalizability, real-time feasibility, adaptability to emerging threats, and resource constraints.
- To propose future research directions for adaptive IDS solutions capable of operating efficiently in resource-constrained vehicular environments.

This review integrates findings from multiple relevant studies and proposes a classification framework that aligns IDS approaches with their deployment scope and performance context.

D. Novelty of the Study

- Cross-Domain Integration of IDS Frameworks: This study uniquely compares and analyses intrusion detection systems across Vehicular Ad Hoc Networks (VANETs), Internet of Vehicles (IoV), Industrial IoT (IIoT), UAV networks, and Internet of Drones (IoD)—a scope rarely addressed collectively in existing reviews.

- Model-Centric Tabular Evaluation of multiple IDS Approaches: A comprehensive matrix-based analysis has been conducted that categorizes each study by model architecture, dataset used, detection performance metrics, and identified research gaps—enabling rapid benchmarking for future IDS development.
- Emphasis on Optimization Techniques within IDS Design: Unlike traditional IDS surveys, this study specifically highlights the role of optimization methods such as particle swarm optimization (PSO) and genetic algorithms (GA) in enhancing intrusion detection models for real-time vehicular deployment.
- Practical Deployment and Real-Time Feasibility Analysis: The research distinctly evaluates whether the reviewed IDS models are suitable for onboard ECU integration, RSU deployment, or cloud-edge hybrid architectures, focusing on latency, computational efficiency, and model scalability in vehicular environments.

II. Hybrid Deep Learning and Optimization-based Approaches for Intrusion Detection in Vehicular Networks

Several studies have explored the application of deep learning and hybrid models for vehicle network-based intrusion detection systems (IDSs), addressing challenges in detecting cyber threats in automotive networks.

A. Hybrid Deep Learning and Machine Learning Approaches for Intrusion Detection in Vehicular Networks

Modern vehicle connectivity brings an urgent need for improved security solutions within IVNs thus making it essential to pursue research efforts in this area. This research [15] explores 102 artificial intelligence-based intrusion detection system (IDS) proposals for IVNs specifically focusing on CAN bus security. This research evaluates self-learning algorithms which include autoencoders and one-class SVMs against security weaknesses that affect AI-based IDS systems. Current models struggle with two principal weaknesses which include inadequate generality between different datasets and weak capabilities against adversarial attacks. The research in [16] delivers HyDL-IDS as a hybrid system that integrates CNNs combined with LSTM networks to analyze spatial through temporal elements of IVN traffic behavior.

B. Optimized and Distributed IDS Models

The evolution of IDS becomes necessary due to rising vehicle network complexity to achieve accurate efficient security solutions. In [17], an IDS for Internet of Vehicles (IoV) operating through CNN analyses security threats using transfer learning and ensemble learning (fig 2.1) combined with hyperparameter optimization is proposed. The proposed detection model achieves superiority over 99.25% in both detection rates and F1-scores while successfully identifying both intra-vehicle and external network attacks on the Car-Hacking and CICIDS2017 datasets.

To further refine detection accuracy, the study leverages particle swarm optimization (PSO) for fine-tuning CNN parameters. However, the proposed approach does not consider essential trade-offs between computational costs and latency measurements especially concerning energy consumption that are required for real-time vehicle network operations.

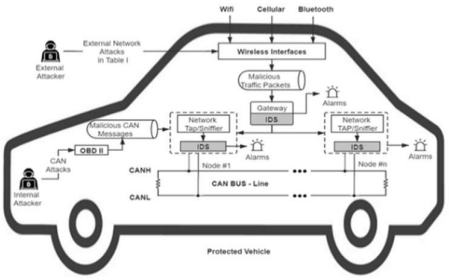

Fig 1: Proposed IDS system in [17]

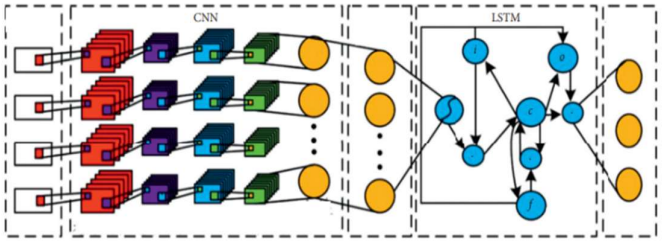

Fig 2: CNN-LSTM Architecture used in [18]

Proper management and processing of big vehicular traffic data represents a necessary requirement to detect system intrusions effectively. A distributed IDS based on deep learning described in [18] integrates Apache Spark framework to merge both CNN and LSTM algorithms (fig 2.2). This model operates with NSL-KDD and UNSW-NB15 datasets which produces 99.7% accuracy together with shortened detection times compared to single deep learning applications.

C. Comparative, Optimization-Based, and Adaptive IDS Techniques

Current assessments of different machine learning models aim to evaluate the effectiveness of securing vehicular networks because of their growing usage. 6G networks have advanced to the point where ensuring secure vehicular communication has become a challenging task. A many-objective optimization-based intelligent intrusion detection system (MaOEA-BCD) appears in [19] (fig 2.3) which focuses on increasing security in vehicular networks. The system combines WBELA with multi-objective optimization to implement a precision improvement while stopping false positives.

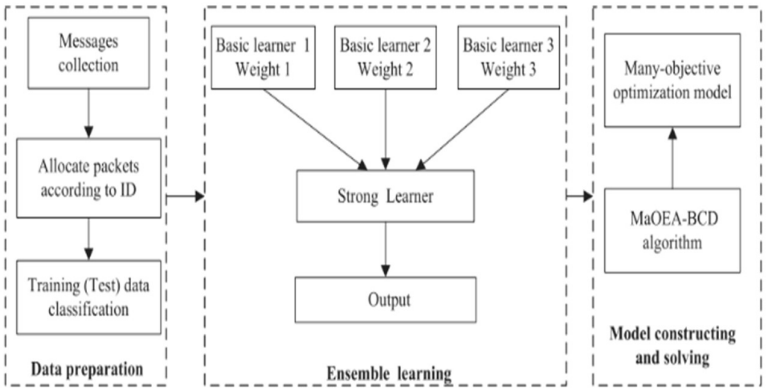

Fig 3: Implementation flow in [19]

The combination of deep learning and machine learning provides researchers with new insights into improving intrusion detection systems for vehicular networks. However, several challenges remain, including validating real-time performance, optimizing detection speed, and enhancing adaptability to evolving cyber threat.

The use of open-source CAN bus datasets allows the model to achieve better AUC and F-measure scores while decreasing FPR and loss compared to NSGA-III and GrEA algorithms. The research [19] shows successful results yet lacks immediate execution speed optimization and resource management development which calls for further study to improve vehicular system operational speed.

III. Emerging Approaches for Intrusion Detection in Vehicular and IoT Networks

Several studies have explored advanced intrusion detection techniques in vehicular and IoT networks, leveraging hybrid deep learning and machine learning approaches for enhanced security.

A. Machine Learning-Based IDS Approaches for Vehicular Networks

Modern vehicular networks require robust intrusion detection solutions as they face increasingly sophisticated cyber threats. In [20], researchers develop an intrusion detection system for VANETs that implements machine learning algorithms to analyze data from the ToN-IoT dataset. This research uses the Chi-square algorithm for feature selection, along with SMOTE for class balancing, on modern datasets instead of relying on outdated datasets such as KDD-CUP99 and NSL-KDD to improve detection capabilities.

XGBoost produces the best classification results compared to all other tested approaches for both binary and multi-class tasks. The research demonstrates improved detection accuracy with lower bias; however, it does not incorporate deep learning methods or explain how to deploy the IDS on distributed systems such as Apache Spark.

B. Hybrid Deep Learning Models for IoT and Industrial Networks

Growing industrial IoT (IIoT) network complexities make efficient intrusion detection systems increasingly important. The authors in [21] developed a hybrid IDS that combines CNN and LSTM networks to protect IIoT networks and tested the system using the X-IIoTID and UNSW-NB15 datasets. The application of the CNN-LSTM model achieves 99.84% accuracy in binary classification and 99.80% accuracy in multi-class classification on the X-IIoTID dataset, outperforming individual CNN and LSTM models.

The research demonstrates successful intrusion pattern detection; however, it does not discuss real-time deployment overheads or computational efficiency considerations. Future research should focus on developing lean implementation solutions while ensuring adaptability to evolving attack patterns in IIoT systems.

Lightweight models remain crucial for ensuring accurate intrusion detection in Industrial IoT (IIoT) networks. The research in [22] presents 1D-CNN-IDS, a one-dimensional CNN model designed as a computationally efficient IDS for IIoT environments. This model achieves a high accuracy of 99.90% in classifying nine cyberattacks while requiring minimal computational power. However, this work does not evaluate real-time scalability or adaptability to emerging attack patterns.

C. Advanced Security Approaches for Autonomous and Drone Networks

Smart transportation systems require new intrusion detection strategies as cybersecurity threats continue to emerge. Researchers in [23] present FED-IDS, an IDS that utilizes deep learning in a federated manner to protect blockchain-powered smart transportation networks. The model applies Car-Hacking and ToN-IoT datasets to improve intrusion detection while ensuring data privacy through blockchain-managed federated training. However, additional research is needed to address model convergence issues and resource limitations in edge environments introduced by federated learning systems.

Network security has become a critical concern as drones steadily integrate into various commercial sectors. The authors in [24] propose a blockchain-based IDS for the Internet of Drones (IoD), incorporating Radial Basis Function Neural Networks (RBFNN) to enhance data integrity and security. The decentralized design eliminates single points of failure while outperforming existing techniques in specificity, recall, precision, and accuracy.

D. Advanced Machine Learning Approaches for Secure Vehicular and IoT Communications

Recent research has explored advanced machine learning and deep learning techniques for intrusion detection in autonomous vehicles, IoV, and intelligent transportation systems, addressing emerging cybersecurity challenges. The protection of in-vehicle communication systems remains crucial as modern vehicles become increasingly connected. The work in [25] develops an optimal cascade feature-level fusion method for detecting CAN bus anomalies by integrating spatial and temporal information. The model employs a two-parameter genetic algorithm for optimization before being tested using a paired t-test to ensure high reliability (fig 3.1(a)).

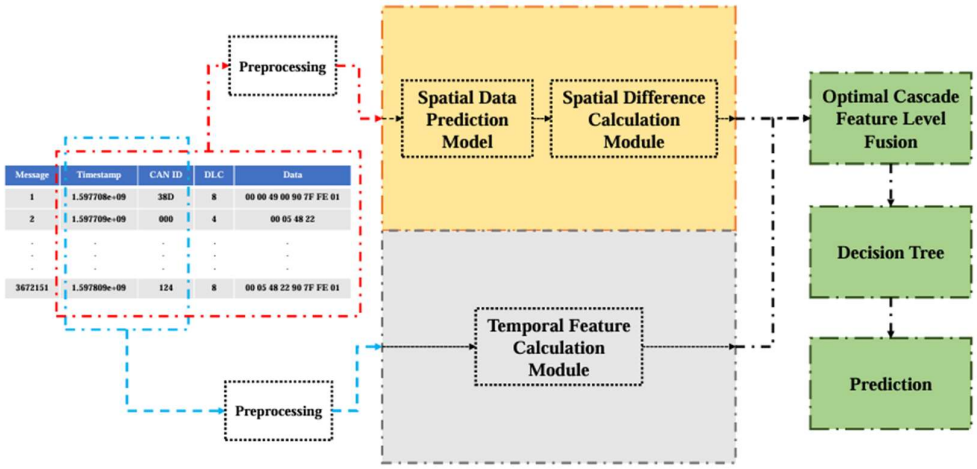

Fig 4 (a): Framework in [25]

Feature Space	Accuracy	Precision	Recall	F1-score
All Raw Features	0.9902	0.9335	0.9476	0.9405
1D-CNN-Based Optimal Cascade Feature-Level Fusion	0.9934	0.9604	0.9588	0.9596
xLSTM-Based Optimal Cascade Feature-Level Fusion	0.9934	0.9604	0.9592	0.9598
Simple RNN-Based Optimal Cascade Feature-Level Fusion	0.9934	0.9602	0.9588	0.9595
GRU-Based Optimal Cascade Feature-Level Fusion	0.9934	0.9609	0.9587	0.9598
LSTM-Based Optimal Cascade Feature-Level Fusion	0.9932	0.9588	0.9587	0.9588

Fig 4 (b): Final comparison for different feature spaces and model sin optimal cascade feature-level fusion [25]

This method delivers higher accuracy levels and improved F1-score performance across various datasets, outperforming existing solutions (fig 3.1(b)).

IV. VANET Intrusion-Detection Methodologies

V2X communication security now stands as a top priority due to progressive advancements in vehicular networks, aiming to prevent cyber threats. The authors in [26] developed a machine learning framework to detect intrusions in VANET communication systems by protecting vehicle-to-everything (V2X) networks. The paper demonstrates VANET security weak points while conducting evaluations between isolated ML solutions and ensemble solutions using VDOS-LRS data. The framework operates as a security system that specifically identifies DoS and DDoS attacks to guarantee better protection.

The complexity of vehicular communication makes hierarchical security solutions increasingly important. The authors in [27] developed an intelligent hierarchical security framework that uses machine learning models to enhance intrusion detection capabilities for VANETs. The system deploys fast-operating, lightweight ML models at its entry levels to detect threats but utilizes advanced complex models at upper tiers for precise attack identification.

Through its implementation, the framework ensures complete authentication, privacy, and anonymity for vehicular networks. IDS framework demonstrates effective experimental outcomes by achieving high detection accuracy while maintaining low false positive rates.

The study in [28] introduces a lightweight trust model based on machine learning techniques to enhance security and privacy in VANETs.

V. Discussion

A. Key Findings

The review reveals that hybrid deep learning models significantly outperform traditional machine learning algorithms in detecting cyber threats within vehicular networks. Approaches combining CNN, LSTM, GRU, and optimization strategies such as Particle Swarm Optimization (PSO) and Genetic Algorithms (GA) have demonstrated high accuracy, often exceeding 99%, in classifying various attack types. Notably, the integration of spatial and temporal features—enabled through hybrid architectures—has been instrumental in improving detection precision and reducing false positives.

In the domain of Industrial IoT (IIoT) and in-vehicle networks, models like CNN-LSTM and attention-based GRUs have successfully captured complex intrusion patterns. Additionally, lightweight CNN architectures and the use of Principal Component Analysis (PCA) have contributed to reducing computational overhead, making these models more viable for real-world deployments.

B. Key Research Gaps Identified

Despite the promising results across various IDS models, several key gaps remain. First, a majority of models are evaluated on limited or outdated datasets, which restricts their generalizability to newer and more sophisticated attack types.

Many studies focus on static evaluations and lack testing in dynamic, real-time vehicular environments, where latency, adaptability, and energy constraints are crucial.

Second, while hybrid models improve detection accuracy, their computational cost and implementation feasibility in resource-constrained environments like in-vehicle systems or UAVs are rarely assessed. Additionally, there is minimal research on adversarial robustness.

Another gap is the absence of standardized benchmarks and evaluation protocols across studies. Variations in datasets, feature engineering, and validation methods make it difficult to compare performance consistently.

C. Future Directions for Study and Implementation

To address the identified gaps, future research should emphasize real-time adaptability and lightweight deployment. Models must be tested under dynamic vehicular conditions with limited computing resources, using embedded systems or edge devices [29].

There is also a growing need to incorporate transfer learning and zero-shot learning to improve model generalization across diverse traffic patterns and attack types. Such approaches can significantly reduce dependency on large, labelled datasets and enhance adaptability to unseen scenarios [30].

Moreover, research should focus on enhancing adversarial robustness by integrating defense mechanisms such as adversarial training, model uncertainty estimation, and anomaly-aware loss functions [31].

Finally, developing standardized benchmarks, including multi-modal, encrypted, and real-world datasets, will be essential for fostering comparative evaluations and validating the scalability of proposed models.

D. Practical Implications

The growing integration of connected and autonomous vehicles necessitates robust and intelligent cybersecurity solutions. This study highlights hybrid deep learning-based intrusion detection systems (IDS), such as CNN-LSTM and GRU-based models, which can be integrated in ECUs or onboard diagnostic systems to detect malicious activity with high detection accuracy and reduced false positive rates. These models are well-suited for safety-critical applications like V2X communications and smart traffic systems. Optimization techniques like particle swarm and genetic algorithms further enhance their real-time performance.

In addition to their technical advantages, blockchain-based and federated learning IDS enhance data integrity and privacy, making them ideal for decentralized environments [32]. As the automotive industry advances toward electric, 6G, and edge AI technologies, these IDS frameworks offer scalable, secure foundations for future mobility systems [33].

VI. CONCLUSION

The growing reliance on intelligent vehicular and IoT communication infrastructures has made robust intrusion detection systems an essential component of network security. This review analyzed hybrid IDS frameworks that integrate deep learning and machine learning to enhance threat detection capabilities. CNN-LSTM and GRU-based architectures, along with optimized ensemble methods, consistently achieved high accuracy, F1-scores, and low false positives.

Key advancements highlighted in this review include the use of hybrid feature extraction, dimensionality reduction through PCA and mutual information, and the incorporation of metaheuristic optimization techniques such as particle swarm and genetic algorithms. Moreover, IDS frameworks have evolved to address specific network segments, including CAN bus traffic, IoV communications, UAV control systems, and 6G-enabled vehicular networks. The lack of real-time testing and deployment, especially in constrained environments like onboard vehicle ECUs or UAV systems, hinders practical implementation.

Furthermore, scalability, model update mechanisms, and computational overhead remain major concerns, particularly for models intended to function in mobile, high-speed, and heterogeneous network environments. This review also advocates for cross-domain validation using diverse datasets and real-time performance benchmarking to ensure broader applicability.

REFERENCES

[1] Sharma, Sparsh, et al. "A detailed tutorial survey on VANETs: Emerging architectures, applications, security issues, and solutions." International Journal of Communication Systems 34.14 (2021): e4905.

[2] Hemalathaa, R., and J. Abdul Samath. "A survey: security challenges of VANET and their current solution." Turkish Journal of Computer and Mathematics Education 12.2 (2021): 1239-1244.

[3] Rao, B. Tarakeswara, RSM Lakshmi Patibandla, and V. Lakshman Narayana. "Comparative study on security and privacy issues in VANETs." Cloud and IoT-Based Vehicular Ad Hoc Networks (2021): 145-162.

[4] Asra, Sahabdeen Aysha. "Security issues of vehicular ad hoc networks (VANET): A systematic review." TIERS Information Technology Journal 3.1 (2022): 17-27.

[5] Al-Shareeda, Mahmood A., and Selvakumar Manickam. "A systematic literature review on security of vehicular ad-hoc network (vanet) based on veins framework." IEEE Access 11 (2023): 46218-46228.

[6] Lee, Michael, and Travis Atkison. "VANET applications: Past, present, and future." Vehicular Communications 28 (2021): 100310.

[7] Mahi, Md Julkar Nayeen, et al. "A review on VANET research: Perspective of recent emerging technologies." IEEE Access 10 (2022): 65760-65783.

[8] AlMarshoud, Mishri, Mehmet Sabir Kiraz, and Ali H. Al-Bayatti. "Security, privacy, and decentralized trust management in VANETs: A review of current research and future directions." ACM Computing Surveys 56.10 (2024): 1-39.

[9] Zhang, SuYu, et al. "Improving performance and data transmission security in VANETs." Computer communications 180 (2021): 126-133.

[10] Abdelmaguid, Mohammed A., Hossam S. Hassanein, and Mohammad Zulkernine. "Attack endgame: Proactive security approach for predicting attack consequences in VANET." ICC 2023-IEEE International Conference on Communications. IEEE, 2023.

[11] Al-Ani, Ruqayah, et al. "Privacy and safety improvement of VANET data via a safety-related privacy scheme." International Journal of Information Security 22.4 (2023): 763-783.

[12] Mazhar, Sheraz, et al. "State-of-the-art authentication and verification schemes in vanets: A survey." Vehicular Communications (2024): 100804.

[13] Goyal, Amit Kumar, et al. "Systematic study of VANET: Applications, challenges, threats, attacks, schemes and issues in research." Green Computing in Network Security (2022): 33-52.
[14] Al-Mekhlafi, Zeyad Ghaleb, et al. "Coherent taxonomy of vehicular ad hoc networks (vanets)-enabled by fog computing: a review." IEEE Sensors Journal (2024).
[15] Rajapaksha, Sampath, et al. "Ai-based intrusion detection systems for in-vehicle networks: A survey." ACM Computing Surveys 55.11 (2023): 1-40.
[16] Lo, Wei, et al. "A hybrid deep learning based intrusion detection system using spatial-temporal representation of in-vehicle network traffic." Vehicular Communications 35 (2022): 100471.
[17] Yang, Li, and Abdallah Shami. "A transfer learning and optimized CNN based intrusion detection system for Internet of Vehicles." ICC 2022-IEEE International Conference on Communications. IEEE, 2022.
[18] Alferaidi, Ali, et al. "Distributed Deep CNN-LSTM Model for Intrusion Detection Method in IoT-Based Vehicles." Mathematical Problems in Engineering 2022.1 (2022): 3424819.
[19] Zhang, Zhixia, et al. "A many-objective optimization based intelligent intrusion detection algorithm for enhancing security of vehicular networks in 6G." IEEE Transactions on Vehicular Technology 70.6 (2021): 5234-5243.
[20] Gad, Abdallah R., Ahmed A. Nashat, and Tamer M. Barkat. "Intrusion detection system using machine learning for vehicular ad hoc networks based on ToN-IoT dataset." IEEE access 9 (2021): 142206-142217.
[21] Altunay, Hakan Can, and Zafer Albayrak. "A hybrid CNN+ LSTM-based intrusion detection system for industrial IoT networks." Engineering Science and Technology, an International Journal 38 (2023): 101322.
[22] M. Arsalan, M. Mubeen, M. Bilal and S. F. Abbasi, "1D-CNN-IDS: 1D CNN-based Intrusion Detection System for IIoT," 2024 29th International Conference on Automation and Computing (ICAC), Sunderland, United Kingdom, 2024, pp. 1-4, doi: 10.1109/ICAC61394.2024.10718772.
[23] M. Abdel-Basset, N. Moustafa, H. Hawash, I. Razzak, K. M. Sallam and O. M. Elkomy, "Federated Intrusion Detection in Blockchain-Based Smart Transportation Systems," in IEEE Transactions on Intelligent Transportation Systems, vol. 23, no. 3, pp. 2523-2537, March 2022, doi: 10.1109/TITS.2021.3119968.
[24] Heidari, Arash, Nima Jafari Navimipour, and Mehmet Unal. "A secure intrusion detection platform using blockchain and radial basis function neural networks for internet of drones." IEEE Internet of Things Journal 10.10 (2023): 8445-8454.
[25] Fatahi, Mohammad, et al. "An Optimal Cascade Feature-Level Spatiotemporal Fusion Strategy for Anomaly Detection in CAN Bus." arXiv preprint arXiv:2501.18821 (2025).
[26] Ben Rabah, Nourhene, and Hanen Idoudi. "A machine learning framework for intrusion detection in VANET communications." Emerging trends in cybersecurity applications. Cham: Springer International Publishing, 2022. 209-227.
[27] Gonçalves, Fábio, Joaquim Macedo, and Alexandre Santos. "An intelligent hierarchical security framework for vanets." Information 12.11 (2021): 455.
[28] Junejo, Muhammad Haleem, et al. "Lightweight trust model with machine learning scheme for secure privacy in VANET." Procedia Computer Science 194 (2021): 45-59.
[29] Sheikh, Muhammad Sameer, and Jun Liang. "A comprehensive survey on VANET security services in traffic management system." Wireless Communications and Mobile Computing 2019.1 (2019): 2423915.
[30] Abassi, Ryma. "VANET security and forensics: Challenges and opportunities." Wiley Interdisciplinary Reviews: Forensic Science 1.2 (2019): e1324.
[31] Mustafa, Ahmed Shamil, et al. "VANET: towards security issues review." 2020 IEEE 5th international symposium on telecommunication technologies (ISTT). IEEE, 2020.
[32] Hussain, Rasheed, Fatima Hussain, and Sherali Zeadally. "Integration of VANET and 5G Security: A review of design and implementation issues." Future Generation Computer Systems 101 (2019): 843-864.
[33] Arif, Muhammad, et al. "SDN-based VANETs, security attacks, applications, and challenges." Applied Sciences 10.9 (2020): 3217.