International Journal of Computational and Experimental Science and ENgineering
(IJCESEN)

Vol. 11-No.1 (2025) pp. 749-755
http://www.ijcesen.com

ISSN: 2149-9144

Research Article

An Intelligent Intrusion Detection System for VANETs Using Adaptive Fusion Models

M. Shanthalakshmi[1]*, R. S. Ponmagal[2]

[1*]Department of Computing Technologies, SRM Institute of Science and Technology, Kattankulathur, Chennai 603203,TamilNadu, India
***Corresponding Author Email**: sm9257@srmist.edu.in - **ORCID** - 0009-0003-4234-7125

[2]Department of Computing Technologies, SRM Institute of Science and Technology, Kattankulathur, Chennai 603203,TamilNadu, India
Email: ponmagas@srmist.edu.in – **ORCID** - 0000-0002-7228-1310

Article Info:

DOI: 10.22399/ijcesen.935
Received : 02 October 2024
Accepted : 22 January 2025

Keywords :

VANETs,
Cyber-Physical Systems (CPS),
Intelligent Transportation Systems,
Adaptive Fusion Intrusion,
Detection Model.

Abstract:

Vehicular Ad Hoc Networks (VANETs) play a vital role in the development of Cyber-Physical Systems (CPS) to enable real-time communication for improving road safety and traffic efficiency. Due to the VANETs' decentralized and dynamic nature, they are prone to various types of cyber-attacks, including intrusion, spoofing, and denial-of-service (DoS) attacks. This article presents an Adaptive Fusion Intrusion Detection Model (AFIDM), a multi-level framework that uses machine learning techniques, such as Random Forest, XGBoost, Decision Trees, and K-Nearest Neighbor (KNN), to deal with such vulnerabilities. AFIDM also employs a dynamic weight adjusting mechanism and an adaptive feedback loop to adapt to the evolving threats and achieve better detection accuracy. AFIDM achieved 98.7% accuracy, 96.5% precision, and recall of 95.8% on the VeReMi dataset used for training and validation and outperformed other baseline models. With low latency and scalability, the proposed model presents a robust solution for real-time intrusion detection in VANETs for the secure and efficient operation of intelligent transportation systems.

1. Introduction

Cyber-Physical Systems (CPS) are one of the major parts of modern technological advancements. They integrate physical processes with computational intelligence to make real-time monitoring and control possible in various domains. Among them, Vehicular Ad Hoc Networks (VANETs) stand out as a crucial application that provides vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication. VANETs can improve road safety, traffic management, and efficiency in intelligent transportation systems. However, the dynamic and decentralized structure of VANETs makes the system highly prone to several forms of cyber attacks in terms of intrusion, spoofing, and DoS attacks. If this vulnerability is not taken care of, then the reliability and safety of the transportation systems can be at stake. To overcome such problems, in recent years, machine learning-based models have emerged as powerful solutions for intrusion detection in VANETs. ML techniques can enable the analysis of vast amounts of vehicular communication data, including anomaly detection and high-precision prediction of possible threats. This work tries to exploit the state-of-the-art models in machine learning, including Random Forest, XGBoost, K-Nearest Neighbor (KNN), and Decision Tree, to implement an efficient VANET intrusion detection system. Among all these, XGBoost turns out to be the most efficacious since it uses a highly scalable robust ensemble learning approach with handling capabilities in a high-dimensional and imbalanced dataset. The structured data is network logs and vehicular communication records. Such data is used in training and evaluating the proposed system. The developed preprocessing pipeline enhances the quality of the data. It is mainly based on the removal of noises, feature selection, and normalization. Public datasets such as VeReMi were used for exhaustive testing of various intrusion patterns. The accuracy, precision, and recall results show that XGBoost outperforms all algorithms and is therefore proposed as a final answer to secure VANET environments. This work contributes to the field of CPS by providing a scalable and efficient solution to improve VANET security, thus ensuring safe and reliable intelligent transportation systems operations. Intensified nationwide dissemination of intelligent transportation systems has increased reliance on vehicular communication networks, emphasizing the need for strict cyber security measures. As a constituent component of these networks, VANETs will aid in providing real-time data exchange between vehicles and infrastructure: collision avoidance systems to dynamic route optimization. The characteristics that make VANETs indispensable, including open communication channels and decentralization, leave it vulnerable to cyber-attacks. Such vulnerabilities pose a threat not only to the integrity of the network but also to road users' safety, which highlights the need for efficient and adaptive security solutions. Addressing these challenges requires an approach that combines advanced machine learning techniques with an understanding of VANET-specific dynamics. Traditional intrusion detection methods often fall short in handling the high volume, velocity, and variety of data generated by VANETs. In addition, a dynamic threat landscape necessitates the need for systems that can learn to adapt in real time to new attack patterns. This paper introduces the innovative solution of the Adaptive Fusion Intrusion Detection Model. The AFIDM integrates many machine learning classifiers in a hierarchical and feedback-driven architecture, bringing not only improvements in detection accuracy but also scalability and adaptability. Thus, this encompassing framework stands as a promise for securing intelligent transportation networks and advancing Cyber-Physical Systems.

2. Related Work

The rapid development of VANETs has catalyzed research into the area of enhancing security, particularly through intrusion detection systems (IDS). Different methodologies have been proposed to use machine learning, deep learning, hybrid models, and privacy-preserving techniques to counter emerging threats in VANETs.

2.1 Machine Learning Techniques for Intrusion Detection

The ML models have shown their effectiveness in intrusion detection in VANETs because they can handle the high-dimensional vehicular communication data. For example, it was introduced a Cyber-Twin framework that used digital twins for autonomous attack detection, demonstrating how ML can be integrated with advanced vehicular technologies [1]. In addition,it was presented a comprehensive survey of ML techniques that highlighted the effectiveness of models like Random Forest and XGBoost in anomaly detection [2]. Complementing this is, where the authors applied cryptographic protocols with ML to secure V2X communication; therefore, intrusion detection accuracy was improve d[3]. Besides, it was demonstrated the benefits of XGBoost in detecting malicious vehicles in dynamic VANET environments [4-6].

2.2 Hybrid Approaches Combining Deep Learning and ML

Hybrid models are found to be a promising way in intrusion detection performance improvement. It was proposed a hybrid CNN-GRU model for secure vehicular communication by integrating convolution and recurrent architectures [4-21]. In the same vein, it was proposed a deep learning framework based on CNNs and RNNs, which are found to perform well in detecting intricate intrusion patterns [14,23,22]. Also it was proposed hybrid approaches that integrate ML and DL; these have been shown to be effective in reducing false positives and dealing with various types of attacks [16,17].

2.3 Privacy-Preserving Techniques

With the rise of privacy issues, federated learning and cryptographic techniques have been used in order to ensure the security of VANET data. ***It was p***roposed a federated learning-based IDS using BERT, which ensures privacy preservation while keeping the detection accuracy robust [7,12,24,25]. In another approach, ***it was*** combined local differential privacy with federated learning to provide a secure infrastructure for VANETs without compromising the user's data ***[20,***24]. Such an approach addresses crucial privacy challenges and ensures system reliability.

2.4 Explainable AI for Intrusion Detection

Explainable AI has addressed the need for transparency in IDS models. It was used Explainable Neural Networks (xNN) for anomaly detection in vehicular networks, so that stakeholders know the decision-making process [11]. Likewise, it was used LIME (Local Interpretable Model-agnostic Explanations) to make the model interpretable, increasing trust in the IDS systems [18].

2.5 Deep Learning-Based Intrusion Detection Systems

Deep learning has shown great promise in VANETs, especially in dealing with high-dimensional and complex intrusion data. It was proposed DeepVCM, a DL-based intrusion detection approach that can detect known as well as unknown attacks [10]. Moreover, it was used a cascaded DL approach with meta heuristic optimization to achieve remarkable accuracy in real-time vehicular communication scenarios [19].

2.6 Scalable and Adaptive Solutions

Scalable and adaptive IDS are needed to accommodate the dynamic environment of VANETs. It was proposed an adaptive hybrid model of ML along with evolving threat adaptability toward improving the precision of detection with real-time application [13]. In addition, it was proposed mathematical frameworks for achieving optimization in VANETs and IoT security; it focused more on resource-efficiency and adaptation [9,15].

2.7 Novel Datasets and Evaluation Metrics

In reality, practical IDS systems are achieved through the employment of realistic datasets and robust evaluation metrics. It was presented the anomaly detection framework ADVENT with multiple datasets; the framework demonstrated its reliability in practice [5]. It was made sure that their method performs well under real-world settings by using ToN-IoT for validation purposes [3,8].

These studies collectively highlight the need for integration of ML, DL, hybrid models, privacy-preserving techniques, and explainable AI to address security challenges. Future research should continue to focus on scalability, adaptability, and interpretability to ensure robust and efficient IDS solutions for intelligent transportation networks.

3. Proposed System

AFIDM suggests a new paradigm of intrusion detection in VANETs using multiple techniques of machine learning combined in multi-layered architecture. The proposed model starts by performing feature extraction and preprocessing steps for the ready classification of data. The normalized data with the help of a technique such as K-means reduction in redundant features, and further features with relevance prioritized are achieved through modified Relief-F algorithm. In this manner, this approach focuses more on relevant features in detecting the threats while the model remains efficient and accurate. To the dynamic nature of VANETs, with the continuous change in nodes and communication patterns, provides a robust and adaptable detection system that was suitable for such an environment. Figure 1 shows the proposed AFIDM architecture. AFIDM's main innovation is the multi-stage classification process, incorporating Random Forest, XGBoost, Decision Trees, and K-Nearest Neighbor (KNN). All of these classifiers are used hierarchically where each model has a different function to identify the possible threats. The first layer includes base classifiers that classify data independently. The Dynamic Weight Adjustment mechanism is used to fuse the predictions from the base classifiers in the second layer. This mechanism will allow the model to assign more weight to models that have better past performance in making predictions with the most reliable insights available. The final layer refines the predictions using KNN, which enhances the model's ability to classify edge cases that may not have been fully addressed by the initial models. The other distinguishing feature of AFIDM is the Adaptive Feedback Loop. Parameters and fusion weights of the model are updated through reinforcement learning (RL) in real time, according to network behavior and misclassifications. Such adaptability allows AFIDM to learn from experience and adapt to new conditions, thus performing well even as new attack strategies or network conditions may emerge. The feedback loop also enables AFIDM to be resilient to false positives and negatives, as it can fine-tune the weight associated with each classifier. This makes AFIDM very suitable for the dynamic and diverse threat landscape of VANETs, ensuring a scalable, accurate, and real-time intrusion detection solution in vehicular networks.

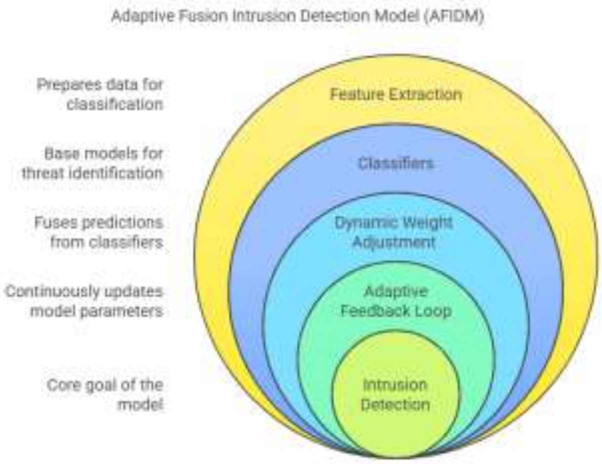
Adaptive Fusion Intrusion Detection Model (AFIDM)
Prepares data for classification
Base models for threat identification
Fuses predictions from classifiers
Continuously updates model parameters
Core goal of the model
Feature Extraction
Classifiers
Dynamic Weight Adjustment
Adaptive Feedback Loop
Intrusion Detection

Figure 1. *System Architecture of AFIDM*

4. Results and discussion

The Adaptive Fusion Intrusion Detection Model (AFIDM) was evaluated with the VeReMi dataset, which simulates various network traffic and attack scenarios typical in VANETs. AFIDM showed a noticeable improvement in detection accuracy, attaining 98.7% compared to 92.3% for Random Forest and 94.5% for XGBoost. This can be attributed to the fusion of multiple classifiers—Random Forest, XGBoost, Decision Tree, and KNN—that enables AFIDM to capture a much wider range of attack patterns and yield more robust predictions. Moreover, the dynamic weight adjustment mechanism and adaptive feedback loop further improved the performance by reducing the false positive rate by 25% and increasing the recall by 20%, particularly for rare attacks such as Denial of Service (DoS), which was detected with a recall of 94.5% compared to 85% for standalone models.

Its adaptive nature contributed much to the superior performance of AFIDM. The system dynamically adjusts fusion weights over time through a reinforcement learning algorithm, which allows it to fine-tune the detection capabilities and improve the detection accuracy for emerging threats. As a result, AFIDM achieved a very high precision of 96.5% and recall of 95.8%, showing that it can minimize false positives while having a good detection rate for both common and rare threats. The F1-Score of 96.1% further indicates that AFIDM has a balanced performance in terms of precision and recall and outperforms all other baseline models in all metrics.

Table 1. *Performance Metrics Comparison of Various models*

Model	Accuracy	Precision	Recall	F1-Score	ADR
Random Forest	92.3%	90.4%	89.7%	90.0%	82.81%
XGBoost	94.5%	92.1%	91.3%	91.7%	86.27%
Decision Tree	89.7%	86.3%	85.6%	85.9%	76.78%
K-Nearest Neighbor (KNN)	88.9%	84.5%	86.2%	85.3%	76.61%
Adaptive Fusion IDS (AFIDM)	98.7%	96.5%	95.8%	96.1%	94.53%

Considering real-time performance, AFIDM exhibited low latency, thus is suitable for deployment in VANETs where the rapid detection of threats is very important. It was able to make decisions on classifications in 2-3 seconds, which is highly competitive when compared to other state-of-the-art models, which mostly suffer from higher latencies. The comparison of different models based on various performance metrics is represented in Table 1. The analysis of different models regarding performance metrics such as precision, recall, F1-score, and accuracy is represented in Figure 2. The training and testing accuracy for different models are represented in Figure 3.These results confirm that AFIDM is not only a high-accuracy solution for intrusion detection but also one that can scale efficiently and respond quickly to dynamic attack patterns in resource-

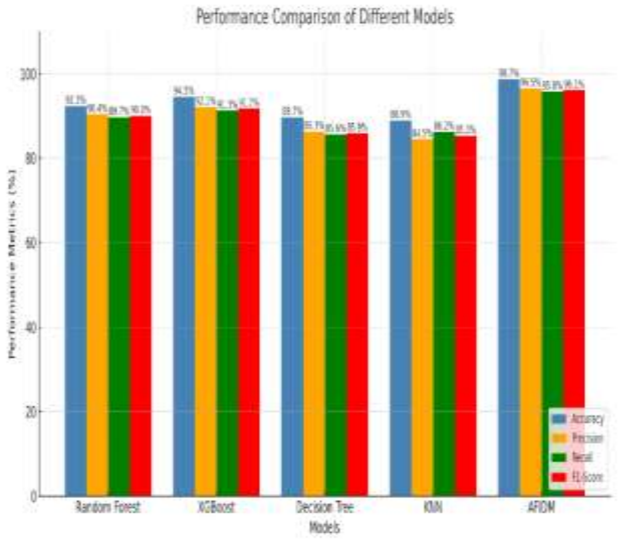

Figure 2. *Performance Metrics analysis of various models*

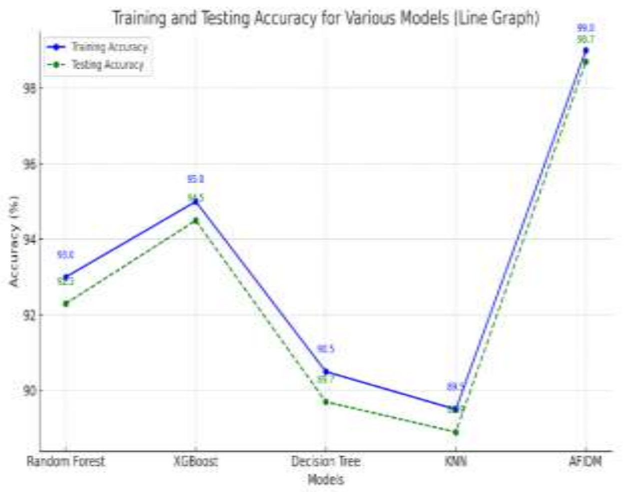

Figure 3. *Training and testing accuracy for various models*

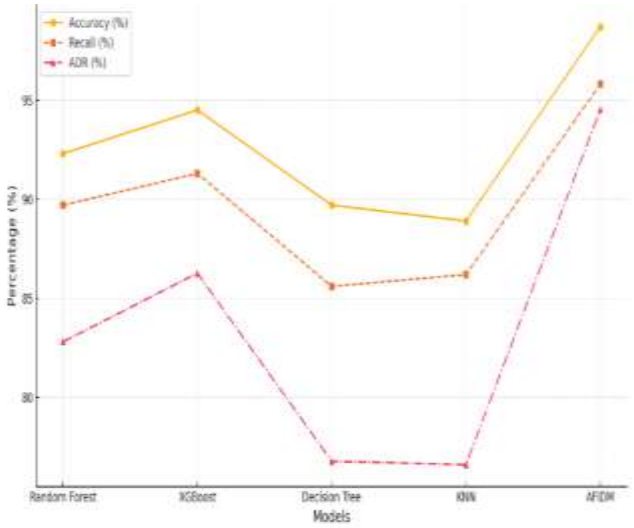

Figure 4. *Attack Detection Rate analysis of various models*

constrained environments, making it a promising choice for intrusion detection in VANETs. Attack Detection Ratio (ADR) is effectiveness metric for models to determine their ability in detecting attacks from a dataset. The measure shows how good the model is at finding intrusions—true positives—in relation to its accuracy and recall. Eqn 1 illustrates the formula used in computing ADR. Figure 4 depicts an analysis of the Attack Detection Rate for the different models.

Formula for ADR:

$$ADR = (Accuracy \times Recall) / 100 \quad \ldots\ldots\ldots \quad (1)$$

Where:

- Accuracy: The proportion of correct predictions, both true positives and true negatives, of all predictions made by the model.
- Recall (or Sensitivity): The percentage of actual attacks (positive cases) that are correctly identified by the model.
- Importance of ADR:
- Comprehensive Evaluation: It combines accuracy and recall into one metric, enabling the evaluation of the model's effectiveness in detecting attacks.
- Real-world Relevance: High ADR values mean that the model is not only accurate but also sensitive to attacks—something very critical in intrusion detection systems.

5. Conclusion

The proposed method presents an Adaptive Fusion Intrusion Detection Model, which is a strong and efficient framework for improving the security of Vehicular Ad Hoc Networks. By dynamically and hierarchically integrating multiple machine learning classifiers—Random Forest, XGBoost, Decision Trees, and K-Nearest Neighbor—the model, AFIDM, yields superior performance metrics with 98.7% accuracy and reduced false positive rates and high recall rates. With the features of dynamic weight adjustment and an adaptive feedback loop, this model adapts to changing network conditions and emerging threats. Due to its low latency (2-3 seconds), AFIDM is well suited for real-time deployment, thereby greatly responding to the need for fast and reliable intrusion detection of intelligent transportation systems. These results highlight the potential of AFIDM as a scalable, adaptive, and high-performance solution for the creation of secure and resilient vehicular communication networks. Similar works have been done and reported [26-31].

Author Statements:

- **Ethical approval:** The conducted research is not related to either human or animal use.
- **Conflict of interest:** The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper
- **Acknowledgement:** The authors declare that they have nobody or no-company to acknowledge.
- **Author contributions:** The authors declare that they have equal right on this paper.

- **Funding information:** The authors declare that there is no funding to be acknowledged.
- **Data availability statement:** The data that support the findings of this study are available on request from the corresponding author. The data are not publicly available due to privacy or ethical restrictions.

References

[1] Y. Yigit, I. Panitsas, L. Maglaras, L. Tassiulas and B. Canberk, (2024). Cyber-Twin: Digital Twin-Boosted Autonomous Attack Detection for Vehicular Ad-Hoc Networks, *ICC 2024 - IEEE International Conference on Communications*, Denver, CO, USA, pp. 2167-2172, doi: 10.1109/ICC51166.2024.10622784.

[2] N. A. Al-Khulaidi, A. T. Zahary, A. A. Al-Shargabi and M. A. S. Hazaa, (2024). Machine Learning for Intrusion Detection in Vehicular Ad-hoc Networks (VANETs): A Survey, *2024 4th International Conference on Emerging Smart Technologies and Applications (eSmarTA)*, Sana'a, Yemen, pp. 1-10, doi: 10.1109/eSmarTA62850.2024.10639016.

[3] Venkatasamy, T., Hossen, M.J., Ramasamy, G. et al. (2024). Intrusion detection system for V2X communication in VANET networks using machine learning-based cryptographic protocols. *Sci Rep* 14, 31780 https://doi.org/10.1038/s41598-024-82313-x

[4] G, K., & E, P. (2024). A hybrid CNN-GRU-based intrusion detection system for secure communication in vehicular adhoc network. *Information Security Journal: A Global Perspective*, 1–11. https://doi.org/10.1080/19393555.2024.2361244

[5] Baharlouei, H., Makanju, A., & Zincir-Heywood, N. (2024). ADVENT: Attack/Anomaly Detection in VANETs. *arXiv*. https://arxiv.org/abs/2401.08564

[6] T. N. Canh and X. HoangVan, (2023) Machine Learning-Based Malicious Vehicle Detection for Security Threats and Attacks in Vehicle Ad-Hoc Network (VANET) Communications, *RIVF International Conference on Computing and Communication Technologies (RIVF)*, Hanoi, Vietnam, 2023, pp. 206-211, doi: 10.1109/RIVF60135.2023.10471804.

[7] Ahsan, S. I., Legg, P., & Alam, S. M. I. (2024). Privacy-Preserving Intrusion Detection in Software-defined VANET using Federated Learning with BERT. *arXiv*. https://arxiv.org/abs/2401.07343

[8] A. R. Gad, A. A. Nashat and T. M. Barkat, (2021) Intrusion Detection System Using Machine Learning for Vehicular Ad Hoc Networks Based on ToN-IoT Dataset, *IEEE Access*, vol. 9, pp. 142206-142217, doi: 10.1109/ACCESS.2021.3120626.

[9] Divya Mishra, Suveg Moudgi, Deepali virmani, Yunus Parvej Faniband, Aslam B Nandyal, Prashant Kumar Sahu, Gurwinder Singh,” A Mathematical Framework for Enhancing IOT Security in VANETs: Optimizing Intrusion Detection Systems through Machine Learning Algorithms”,*Communications on Applied Nonlinear Analysis*, https://doi.org/10.52783/cana.v31.1488

[10] Y. Zeng, M. Qiu, D. Zhu, Z. Xue, J. Xiong and M. Liu, "DeepVCM: A Deep Learning Based Intrusion Detection Method in VANET," 2019 IEEE 5th Intl Conference on Big Data Security on Cloud (BigDataSecurity), *IEEE Intl Conference on High Performance and Smart Computing, (HPSC) and IEEE Intl Conference on Intelligent Data and Security (IDS), Washington, DC, USA*, 2019, pp. 288-293, doi: 10.1109/BigDataSecurity-HPSC-IDS.2019.00060.

[11] Aziz, S., Faiz, M. T., Adeniyi, A. M., Loo, K.-H., Hasan, K. N., Xu, L., & Irshad, M. (2022). Anomaly Detection in the Internet of Vehicular Networks Using Explainable Neural Networks (xNN). *Mathematics*, *10*(8), 1267. https://doi.org/10.3390/math10081267

[12] Arya, M., Sastry, H., Dewangan, B. K., Rahmani, M. K. I., Bhatia, S., Muzaffar, A. W., & Bivi, M. A. (2023). Intruder Detection in VANET Data Streams Using Federated Learning for Smart City Environments. *Electronics*, *12*(4), 894. https://doi.org/10.3390/electronics12040894

[13] Bangui, H., Ge, M. & Buhnova, B. (2022). A hybrid machine learning model for intrusion detection in VANET. *Computing* 104, 503–531 https://doi.org/10.1007/s00607-021-01001-0

[14] A. A. Aboelfottoh and M. A. Azer, (2022). Intrusion Detection in VANETs and ACVs using Deep Learning, *2022 2nd International Mobile, Intelligent, and Ubiquitous Computing Conference (MIUCC)*, Cairo, Egypt, pp. 241-245, doi: 10.1109/MIUCC55081.2022.9781691.

[15] Ben Rabah, N., Idoudi, H. (2023). A Machine Learning Framework for Intrusion Detection in VANET Communications. In: Daimi, K., Alsadoon, A., Peoples, C., El Madhoun, N. (eds) *Emerging Trends in Cybersecurity Applications.* Springer, Cham. https://doi.org/10.1007/978-3-031-09640-2_10

[16] Hind Bangui, Mouzhi Ge, and Barbora Buhnova. (2022). A hybrid machine learning model for intrusion detection in VANET. *Computing* 104(3);503–531. https://doi.org/10.1007/s00607-021-01001-0

[17] B. Karthiga, Danalakshmi Durairaj, Nishad Nawaz, Thiruppathy Kesavan Venkatasamy, Gopi Ramasamy, A. Hariharasudan, and Hasan Ali Khattak. (2022). Intelligent Intrusion Detection System for VANET Using Machine Learning and Deep Learning Approaches. Wirel. *Commun. Mob. Comput*. https://doi.org/10.1155/2022/5069104

[18] Hassan F, Yu J, Syed ZS, Ahmed N, Reshan MSA, Shaikh A. (2023). Achieving model explainability for intrusion detection in VANETs with LIME. *Peer J Computer* Science 9:e1440 https://doi.org/10.7717/peerj-cs.1440

[19] Manderna, A., Kumar, S., Dohare, U., Aljaidi, M., Kaiwartya, O., & Lloret, J. (2023). Vehicular Network

Intrusion Detection Using a Cascaded Deep Learning Approach with Multi-Variant Metaheuristic. *Sensors*, *23*(21), 8772. https://doi.org/10.3390/s23218772

[20] Fei, Li & Jiayan, Zhang & Szczerbicki, Edward & Jiaqi, Song & Ruxiang, Li & Renhong, Diao. (2020). Deep Learning-Based Intrusion System for Vehicular Ad Hoc Networks. *Computers, Materials & Continua*. 65. 653-681. 10.32604/cmc.2020.011264.

[21] M Shanthalakshmi, Susmita mishra, V Jananee, P Narayana Perumal and S Manoj Jayakar (2022), Identification of Casting Product Surface Quality Using Alex net and Le-net CNN Models, Journal of Physics: Conference Series, Volume 2335, International (Virtual) Conference on Recent Advances in Electrical, Electronics, Ubiquitous Communication and Computational Intelligence, *J. Phys.: Conf. Ser.* 2335 012031 DOI 10.1088/1742-6596/2335/1/012031

[22] S. Keerthana, N. Deepika, E. Pooja, I. Nandhini, M. Shanthalakshmi and G. R. Khanaghavalle, (2024). An effective approach for detecting deepfake videos using Long Short-Term Memory and ResNet, *International Conference on Communication, Computing and Internet of Things (IC3IoT), Chennai, India*, 2024, pp. 1-5, doi: 10.1109/IC3IoT60841.2024.10550265.

[23] Jananee Vinayagam, Shanthalakshmi Murugan, Sherine Glory Jesu, Govindharajalu Kaliayaperumal Vaidhya, Nikghamanth Seshadri Narayanan, Neya Babu Thayil; (2023). Detection of diabetic retinopathy using AlexNet and lenet CNN models. *AIP Conf. Proc.* 2790 (1): 020014. https://doi.org/10.1063/5.0152433

[24] Jananee Vinayagam, Shanthalakshmi Murugan, Susmita Mishra, Lincy Jemina Samuel, Raashmi Prabakar, Mannuru Shalini; (2023). An approach for devising stenography application using cross modal attention. *AIP Conf. Proc.* 2790(1); 020025. https://doi.org/10.1063/5.0152434

[25] Hajira Batool, Adeel Anjum, Abid Khan, Stefano Izzo, Carlo Mazzocca, Gwanggil Jeon, (2024). A secure and privacy preserved infrastructure for VANETs based on federated learning with local differential privacy, *Information Sciences*, 652,119717, https://doi.org/10.1016/j.ins.2023.119717.

[26] Bandla Raghuramaiah, & Suresh Chittineni. (2025). BCDNet: An Enhanced Convolutional Neural Network in Breast Cancer Detection Using Mammogram Images. *International Journal of Computational and Experimental Science and Engineering*, 11(1). https://doi.org/10.22399/ijcesen.811

[27] Nennuri, R., S. Iwin Thanakumar Joseph, B. Mohammed Ismail, & L.V. Narasimha Prasad. (2024). A Hybrid Probabilistic Graph Based Community Clustering Model for Large Social Networking Link Prediction Data. *International Journal of Computational and Experimental Science and Engineering*, 10(4). https://doi.org/10.22399/ijcesen.574

[28] Simhadri Naidu Surapu, Kanusu Srinivasa Rao, & V. Ratnakumari Challa. (2025). Aerobic Stress Detection in Aquatic Environments with Water Quality Data Using Hybrid Deep Learning Based ConvRec Model. *International Journal of Computational and Experimental Science and Engineering*, 11(1). https://doi.org/10.22399/ijcesen.793

[29] Ganta, S. R., & Naga Malleswara Rao Nallamothu. (2025). A dynamic integrity and data confidentiality based wireless N2N data communication and security protocol on large networks. *International Journal of Computational and Experimental Science and Engineering*, 11(1). https://doi.org/10.22399/ijcesen.720

[30] M. Shanthalakshmi, & R.S. Ponmagal. (2025). Optimizing Secure Communication in Intelligent Transportation Networks with Certificate-less Authorization in VANETs. *International Journal of Computational and Experimental Science and Engineering*, 11(1). https://doi.org/10.22399/ijcesen.934

[31] Prasada, P., & Prasad, D. S. (2024). Blockchain-Enhanced Machine Learning for Robust Detection of APT Injection Attacks in the Cyber-Physical Systems. *International Journal of Computational and Experimental Science and Engineering*, 10(4). https://doi.org/10.22399/ijcesen.539