International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435 (Online) Volume 15, Issue 03, March 2026)

Next-Generation VANET Security: A Review of AI-Driven Intrusion and Anomaly Detection Models

Vaibhav Thorat[1], Dr. Mohit Singh Tomar[2]

[1]*Department of CSE, Sagar Institute of Research & Technology, Bhopal, M.P., India*
[2]*Assistant Professor & Head, Department of CSE, Sagar Institute of Research & Technology, Bhopal, M.P., India*

***Abstract*-- This paper presents a comprehensive review of next-generation security mechanisms in Vehicular Ad Hoc Networks (VANETs), with a particular focus on artificial intelligence (AI)-driven intrusion and anomaly detection models. As VANETs enable real-time communication among vehicles and infrastructure, they are highly vulnerable to diverse cyber threats such as spoofing, Sybil, and denial-of-service attacks. Traditional security approaches often fail to adapt to the dynamic and decentralized nature of VANET environments. Therefore, this review explores advanced AI techniques, including machine learning, deep learning, and hybrid models, for enhancing detection accuracy, scalability, and real-time response capabilities. It critically analyzes recent research contributions, datasets, performance metrics, and challenges associated with deploying AI-based security solutions in VANETs. Furthermore, the paper highlights emerging trends such as federated learning, edge intelligence, and blockchain integration, providing insights into future research directions for developing robust, adaptive, and intelligent VANET security frameworks.**

***IndexTerms* –Model, ML, VANET, AI.**

I. INTRODUCTION

Vehicular Ad Hoc Networks (VANETs) represent a transformative evolution in intelligent transportation systems, enabling seamless communication among vehicles (V2V) and between vehicles and infrastructure (V2I). These networks are designed to enhance road safety, traffic efficiency, and driving comfort by facilitating real-time data exchange such as traffic conditions, accident alerts, and navigation updates[1]. With the rapid advancement of connected and autonomous vehicles, VANETs are becoming a fundamental component of smart city ecosystems. However, the open and dynamic nature of VANET environments introduces significant security and privacy challenges that must be addressed to ensure reliable and trustworthy communication[2].

One of the major concerns in VANETs is their susceptibility to a wide range of cyberattacks. Due to decentralized architecture and high node mobility, attackers can exploit vulnerabilities to launch attacks such as Sybil attacks, spoofing, black hole attacks, and distributed denial-of-service (DDoS) attacks.

These threats can disrupt communication, inject false information, and compromise the safety of passengers and infrastructure. Traditional security mechanisms, including cryptographic techniques and rule-based intrusion detection systems, often struggle to cope with the highly dynamic topology and real-time constraints of VANETs[3].

In recent years, artificial intelligence (AI) has emerged as a powerful tool to address complex security challenges in VANETs. AI-driven models, particularly those based on machine learning (ML) and deep learning (DL), offer the ability to learn patterns from large datasets and detect anomalies or malicious activities with high accuracy. Unlike conventional methods, AI-based approaches can adapt to evolving attack patterns and provide proactive threat detection. Techniques such as support vector machines, decision trees, neural networks, and convolutional neural networks have been widely explored for intrusion detection in VANET environments[4].

Anomaly detection plays a crucial role in enhancing VANET security, as it focuses on identifying deviations from normal network behavior. AI-based anomaly detection models can analyze network traffic, vehicle behavior, and communication patterns to identify suspicious activities in real time. These models are particularly effective in detecting zero-day attacks and previously unseen threats, which are difficult to identify using signature-based methods. However, designing efficient anomaly detection systems for VANETs requires careful consideration of factors such as latency, computational overhead, and data heterogeneity[5].

The integration of advanced AI paradigms such as federated learning and edge computing is reshaping the landscape of VANET security. Federated learning enables collaborative model training across distributed nodes without sharing raw data, thereby preserving privacy and reducing communication overhead. Edge computing, on the other hand, allows data processing closer to the source, enabling faster response times and reducing reliance on centralized cloud infrastructure. These technologies are particularly suitable for VANETs, where low latency and data privacy are critical requirements[6].

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435 (Online) Volume 15, Issue 03, March 2026)

Despite the promising potential of AI-driven security solutions, several challenges remain in their practical deployment. One of the key issues is the availability of high-quality and labeled datasets that accurately represent real-world VANET scenarios[7]. Additionally, AI models are often vulnerable to adversarial attacks, where malicious inputs are designed to deceive the detection system. Ensuring robustness, scalability, and explainability of AI models is essential for their adoption in safety-critical applications such as intelligent transportation systems[8].

Another important aspect is the integration of blockchain technology with AI-based security frameworks. Blockchain can provide decentralized trust management, secure data sharing, and tamper-proof record keeping in VANETs. When combined with AI-driven intrusion detection systems, blockchain can enhance transparency and reliability, creating a more secure communication environment. This hybrid approach is gaining attention as a potential solution to address both security and trust-related challenges in VANET ecosystems[9][10].

The evolution of VANETs towards intelligent and autonomous transportation systems necessitates the development of robust and adaptive security mechanisms. AI-driven intrusion and anomaly detection models offer a promising solution by providing intelligent, scalable, and real-time threat detection capabilities. This review aims to explore the current state-of-the-art techniques, identify research gaps, and highlight future di

II. Background

S. E. C et al., [1] proposed a machine learning-based anomaly detection framework for VANETs using advanced data analytics techniques. The study focuses on identifying abnormal communication patterns rections for developing next-generation VANET security frameworks that can ensure safe, efficient, and reliable vehicular communication systems[11][12].

in vehicular networks to enhance security. Various ML classifiers were evaluated for detection accuracy and computational efficiency. The authors emphasized the importance of real-time data processing in highly dynamic VANET environments. Experimental results demonstrated improved detection rates compared to traditional methods. The model effectively reduced false positives while maintaining scalability. The work highlights the role of AI in strengthening VANET security. However, further optimization is required for large-scale deployment.

M. A. Habeeb et al., [2] presented a machine learning approach to enhance security and performance in VANETs against adversarial attacks.

The study addressed vulnerabilities caused by malicious nodes manipulating network behavior. Different ML models were trained to detect and mitigate adversarial patterns. The authors also analyzed the trade-off between security and network performance. Their findings showed significant improvements in resilience against sophisticated attacks.

The approach ensures better reliability in communication systems. However, the model requires continuous updates to handle evolving threats. The research contributes to robust AI-driven VANET security solutions.

N. J. Yothi et al., [3] introduced enhanced machine learning techniques for improving VANET security. The study explored hybrid ML models combining multiple classifiers for better accuracy. It focused on detecting intrusions in real-time vehicular communication. The proposed system demonstrated superior performance over standalone models. The authors highlighted the importance of feature selection in improving detection efficiency. Simulation results confirmed reduced detection latency. The model also showed adaptability to dynamic network conditions. This work supports the integration of intelligent security mechanisms in VANETs.

S. H. Hussen et al., [4] discussed key challenges and approaches of applying machine learning in VANET environments. The paper provided a detailed overview of security threats and ML-based solutions. It analyzed issues such as data heterogeneity, mobility, and scalability. The authors compared different ML algorithms used for intrusion detection. They also identified limitations in existing approaches. The study emphasized the need for lightweight and efficient models. It suggested future directions for improving AI-based VANET security. The work serves as a foundational reference for researchers.

A. R. Gad et al., [5] developed an intrusion detection system for VANETs using machine learning with the ToN-IoT dataset. The study evaluated multiple classifiers to detect cyber threats effectively. The proposed system achieved high accuracy in identifying malicious activities. The authors focused on optimizing detection performance using real-world datasets. Results showed improved precision and recall compared to existing methods. The model demonstrated robustness against various attack types. However, dataset dependency remains a limitation. The research highlights the importance of dataset-driven AI models.

T. N. Canh et al., [6] proposed a machine learning-based approach for detecting malicious vehicles in VANET communications. The study focused on identifying nodes that disrupt network operations. Various ML algorithms were implemented to classify normal and malicious behavior.

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435 (Online) Volume 15, Issue 03, March 2026)

The system achieved high detection accuracy with minimal delay. The authors emphasized the importance of real-time threat identification. The approach enhances trust in vehicular communication systems. However, scalability challenges persist in dense networks. The work contributes to intelligent threat detection mechanisms.

S. Ftaimi et al., [7] conducted a benchmarking study of machine learning algorithms in VANET environments. The research compared multiple classifiers based on performance metrics such as accuracy, precision, and execution time. The study provided insights into the strengths and weaknesses of different algorithms. Results indicated that ensemble methods outperform traditional classifiers. The authors highlighted the importance of selecting appropriate models for specific VANET scenarios. The benchmarking approach aids in decision-making for researchers. However, real-time implementation was not fully explored. The work supports performance optimization in VANET security.

M. Nema et al., [8] proposed an RSA-based encryption mechanism for securing intelligent traffic systems in VANETs. The study focused on enhancing data confidentiality using IEEE 802.11p communication standards. The encryption model ensured secure message transmission between vehicles. Experimental results showed improved security against unauthorized access. The authors highlighted the importance of cryptographic techniques in VANET security. However, the approach may introduce computational overhead. The work complements AI-based security models with encryption techniques. It provides a hybrid perspective on secure VANET communication.

R. Pandey et al., [9] presented a comparative study of machine learning algorithms including Random Forest, SVM, and Naive Bayes. Although focused on sentiment analysis, the study provides valuable insights into classifier performance. The results demonstrated that Random Forest achieved higher accuracy in classification tasks. The authors emphasized the role of feature engineering in improving model performance. The findings can be extended to VANET intrusion detection systems. The study highlights the importance of selecting suitable ML models. It contributes to optimization strategies in AI-based systems. The work supports model evaluation in security applications.

R. Tiwari et al., [10] analyzed spectrum sensing performance in cognitive radio networks with joint transmission techniques. The study focused on improving communication efficiency and reliability. It evaluated different sensing techniques under varying conditions. The results showed enhanced detection accuracy and reduced interference.

Although not directly related to VANET security, the concepts are applicable to vehicular communication systems. The work highlights the importance of efficient spectrum utilization. It provides insights for improving VANET communication frameworks. The study contributes to network performance optimization.

M. Patel et al., [11] conducted a result analysis of pilot-assisted channel estimation in MIMO-STBC systems. The research focused on improving signal reliability in time-varying fading channels. The study demonstrated enhanced performance using pilot-based techniques. The findings are relevant for VANET communication reliability. The authors highlighted the importance of accurate channel estimation. Improved signal quality can support secure data transmission. The work indirectly contributes to VANET security frameworks. It strengthens the communication backbone of vehicular networks.

D. Sahu et al., [12] proposed a sustainable machine learning approach for real-time DDoS attack detection in Industry 4.0 cyber-physical systems. The study focused on efficient and scalable detection mechanisms. The model achieved high accuracy with reduced computational cost. The authors emphasized real-time threat mitigation capabilities. The approach is highly relevant to VANET security due to similar network dynamics. It supports proactive defense against large-scale attacks. The study highlights sustainability in AI-based security systems. The work contributes to advanced intrusion detection frameworks.

III. Challenges

The implementation of AI-driven intrusion and anomaly detection models in Vehicular Ad Hoc Networks (VANETs) presents several critical challenges due to the highly dynamic, decentralized, and real-time nature of vehicular communication environments. While artificial intelligence offers promising capabilities for improving detection accuracy and adaptability, practical deployment faces limitations related to data availability, computational constraints, security vulnerabilities, and system scalability. Additionally, the integration of advanced technologies such as edge computing, federated learning, and blockchain introduces further complexity in terms of coordination, latency, and interoperability. Addressing these challenges is essential to ensure the development of robust, efficient, and reliable next-generation VANET security frameworks.

1. Data Scarcity and Quality Issues

One of the major challenges is the lack of high-quality, labeled datasets that accurately represent real-world VANET scenarios.

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435 (Online) Volume 15, Issue 03, March 2026)

Most available datasets are either simulated or limited in diversity, which affects the generalization capability of AI models. Poor data quality can lead to inaccurate predictions and reduced detection performance.

2. High Mobility and Dynamic Topology

VANETs are characterized by rapidly changing network topologies due to vehicle mobility. This dynamic nature makes it difficult for AI models to maintain consistent performance, as patterns learned during training may quickly become outdated in real-time scenarios.

3. Real-Time Processing Constraints

Intrusion detection in VANETs requires immediate response to potential threats. However, many AI models, especially deep learning approaches, require significant computational resources and processing time, making real-time implementation challenging.

4. Scalability Issues

As the number of connected vehicles increases, the volume of data generated grows exponentially. AI-based systems must be scalable enough to handle large-scale networks without compromising performance or increasing latency.

5. Vulnerability to Adversarial Attacks

AI models themselves can be targeted by adversarial attacks, where malicious inputs are designed to mislead the system. This can result in incorrect classification of attacks or normal behavior, compromising the security framework.

6. Computational and Energy Constraints

Vehicles and roadside units often have limited computational power and energy resources. Deploying complex AI models in such environments can lead to inefficiency and increased operational costs.

7. Privacy and Data Security Concerns

Sharing data among vehicles and infrastructure raises privacy issues, as sensitive information such as location and driving patterns may be exposed. Ensuring secure and privacy-preserving data exchange is a significant challenge.

8. Integration and Interoperability Issues

Integrating AI-based security models with existing VANET protocols and emerging technologies like blockchain and edge computing is complex. Ensuring seamless interoperability among different systems and standards remains a critical hurdle.

IV. Conclusion

The advancement of Vehicular Ad Hoc Networks (VANETs) toward intelligent and autonomous transportation systems necessitates robust, adaptive, and intelligent security solutions. This review highlights that AI-driven intrusion and anomaly detection models significantly enhance the capability to identify and mitigate complex cyber threats in dynamic vehicular environments. Techniques based on machine learning, deep learning, and hybrid approaches demonstrate improved accuracy, scalability, and real-time responsiveness compared to traditional methods. However, challenges such as data limitations, computational constraints, adversarial vulnerabilities, and integration complexities must be addressed to ensure practical deployment. The incorporation of emerging technologies like federated learning, edge computing, and blockchain further strengthens the potential for secure and decentralized VANET ecosystems. Overall, future research should focus on developing lightweight, explainable, and privacy-preserving AI models to build reliable and next-generation secure vehicular communication systems.

REFERENCES

[1] S. E. C, S. S, VR, R. M and N. T, "Anomaly Detection in VANET Using Machine Learning-Based Data Analytics," *2025 IEEE Pune Section International Conference (PuneCon)*, Pune, India, 2025, pp. 1-6, doi: 10.1109/PuneCon67554.2025.11378696.

[2] M. A. Habeeb, Y. L. Khaleel, and A. R. Abdulnabi, "Enhancing security and performance in vehicular adhoc networks: A machine learning approach to combat adversarial attacks," Mesopotamian Journal of Computer Science, pp. 122–133, 2024.

[3] N. J Yothi and R. Patil, "Enhanced machine learning based techniques for security in vehicular ad-hoc networks," in 2023 International Conference on Advancement in Computation & Computer Technologies (In CACCT), IEEE, pp. 386–393, 2023.

[4] S. H. Hussen and M. A. Mohammed, "Problems and the approaches of machine learning in vehicle ad hoc networks," in ITM Web of Conferences, vol. 64, p. 01004, EDP Sciences, 2024.

[5] A. R. Gad, A. A. Nashat, and T. M. Barkat, "Intrusion detection system using machine learning for vehicular ad hoc networks based on ToN-IoT dataset," IEEE Access, vol. 9, pp. 142206–142217, 2021.

[6] T. N. Canh and X. HoangVan, "Machine learning-based malicious vehicle detection for security threats and attacks in vehicle ad-hoc network (VANET) communications," in 2023 RIVF International Conference on Computing and Communication Technologies (RIVF), IEEE, pp. 206–211, 2023.

[7] S. Ftaimi and T. Mazri, "Benchmarking study of machine learning algorithms case study: VANET network," in Emerging Trends in ICT for Sustainable Development: The Proceedings of NICE2020 International Conference, Cham : Springer International Publishing, pp. 171–179, 2021.

[8] M. Nema, S. Stalin and R. Tiwari, "RSA algorithm based encryption on secure intelligent traffic system for VANET using Wi-Fi IEEE 802.11p," *2015 International Conference on Computer, Communication and Control (IC4)*, Indore, India, 2015, pp. 1-5, doi: 10.1109/IC4.2015.7375676.

[9] R. Pandey, P. K. Patidar, P. Verma, G. H. Anjum Khan, S. Harne and R. Tiwari, "A Comparative Study of Random Forest, SVM, and Naive Bayes for Sentiment Analysis Optimization," *2024 IEEE 2nd International Conference on Innovations in High Speed Communication and Signal Processing (IHCSP)*, Bhopal, India, 2024, pp. 1-4, doi: 10.1109/IHCSP63227.2024.10959957.

[10] R. Tiwari and K. Mishra, "Performance Analysis of Spectrum Sensing over Cognitive Radio Network with Joint Transmission," 2022 IEEE International Conference on Current Development in Engineering and Technology (CCET), Bhopal, India, 2022, pp. 1-6, doi: 10.1109/CCET56606.2022.10080214.

[11] M. Patel and R. Tiwari, "A result analysis of pilot assisted channel estimation in MIMO-STBC systems over time-varying fading channels," 2017 International Conference on Information, Communication, Instrumentation and Control (ICICIC), Indore, India, 2017, pp. 1-4, doi: 10.1109/ICOMICON.2017.8279145.

[12] D. Sahu, R. Pandey, N. Sahu, M. Chahar, S. Shukla and R. Tiwari, "Sustainable Machine Learning for Real-Time DDoS Attack Detection and Mitigation in Industry 4.0 CPS," *2024 International Conference on Recent Advances in Science and Engineering Technology (ICRASET)*, B G Nagara,Mandya, India, 2024, pp. 1-6, doi: 10.1109/ICRASET63057.2024.10894989.