IJST
Integrated Journal of Science and Technology
IJST−Computer Science & Information Technology
Short Communication

Artificial Intelligence Techniques in Vehicular Cloud Computing Security

Noman mazher [1, *], Zilly Huma [2]

This paper explores the application of Artificial Intelligence (AI) techniques to enhance the security of Vehicular Cloud Computing. The study begins by examining the unique security concerns in VCC, such as data privacy, authentication, and the potential impact of malicious attacks on safety-critical applications. Traditional security mechanisms face limitations in addressing these challenges due to the complex and dynamic nature of vehicular environments. As a solution, AI techniques, including machine learning, deep learning, and anomaly detection, are proposed to provide adaptive and intelligent security measures. Machine learning algorithms are employed for real-time threat detection and classification, leveraging historical data to recognize patterns indicative of security breaches. Deep learning models, such as neural networks, enhance the accuracy of intrusion detection systems by automatically learning and adapting to evolving threats.

Keywords: Vehicular Cloud Computing (VCC), Artificial Intelligence (AI), Security, Machine Learning, Deep Learning, Anomaly Detection, Intrusion Detection Systems

[1] *Department of Information Technology, University of Gujrat, Pakistan*
[2] *Department of Physics, University of Gujrat, Pakistan*

[*] *Corresponding Author: noman.mazher@gmail.com*

Article timeline. RECEIVED 5 January 2024, ACCEPTED 9 January 2024, PUBLISHED 12 January 2024

1. Introduction

Vehicular Cloud Computing (VCC) represents a transformative paradigm that integrates cloud computing capabilities into vehicular networks, offering vehicles access to powerful computational resources, storage, and services[1]. This integration enables a wide range of applications, including real-time traffic management, navigation, and safety-critical communications. However, the dynamic and open nature of VCC introduces unique security challenges that necessitate innovative solutions to ensure the integrity, confidentiality, and availability of vehicular data and communication. In this context, the utilization of Artificial Intelligence (AI) techniques emerges as a promising approach to enhance the security posture of Vehicular Cloud Computing. Traditional security mechanisms, while effective in certain scenarios, struggle to adapt to the dynamic and evolving nature of vehicular environments. AI, with its adaptive and intelligent capabilities, offers a paradigm shift in addressing these challenges by providing real-time threat detection, dynamic access control, and continuous improvement of encryption protocols.

This paper aims to explore and discuss the application of various AI techniques in addressing the security concerns inherent to Vehicular Cloud Computing[2]. The focus areas include but are not limited to machine learning algorithms for threat detection, deep learning models for intrusion detection, anomaly detection techniques for abnormal behavior identification, and the integration of AI-driven encryption mechanisms to secure communication channels. The subsequent sections of this paper delve into the unique security challenges posed by VCC, highlighting the limitations of traditional security approaches in this context. The discussion then transitions to the proposed AI-driven solutions, emphasizing the adaptability and intelligence offered by machine learning, deep learning, and other AI techniques. Through simulations and experiments, the effectiveness of these AI-driven security measures will be evaluated in realistic VCC scenarios[3].

The ultimate goal of this research is to contribute to the development of robust and intelligent security solutions that can safeguard Vehicular Cloud Computing environments, ensuring the trustworthiness of data and the resilience of communication channels in the face of evolving security threats. Vehicular Cloud Computing (VCC) has emerged as a transformative paradigm that integrates cloud computing resources into vehicular networks, offering vehicles enhanced computational capabilities and connectivity for diverse applications and services. While VCC brings unprecedented opportunities for efficiency and innovation, it also introduces unique security challenges that demand advanced solutions. The dynamic nature of vehicular environments, coupled with the critical need for data privacy and safety, necessitates the exploration of cutting-edge technologies to ensure robust security.

This paper delves into the application of Artificial Intelligence (AI) techniques as a proactive and adaptive approach to addressing the security concerns inherent in Vehicular Cloud Computing. Traditional security mechanisms often fall short in dynamically changing scenarios, making the

incorporation of intelligent, learning-based approaches crucial for effective threat detection, prevention, and response[4]. The introduction outlines the key security challenges specific to VCC, emphasizing the importance of safeguarding data privacy, ensuring secure communication, and protecting safety-critical applications from malicious attacks. As vehicular networks become increasingly interconnected, the need for sophisticated security measures becomes paramount to prevent unauthorized access, data breaches, and potential threats to overall system integrity[5].

In this context, the integration of AI techniques, including machine learning, deep learning, and anomaly detection, is proposed as a means to fortify VCC security, Machine Learning Technologies for Secure Vehicular Communication in Internet of Vehicle, as shown in figure1.

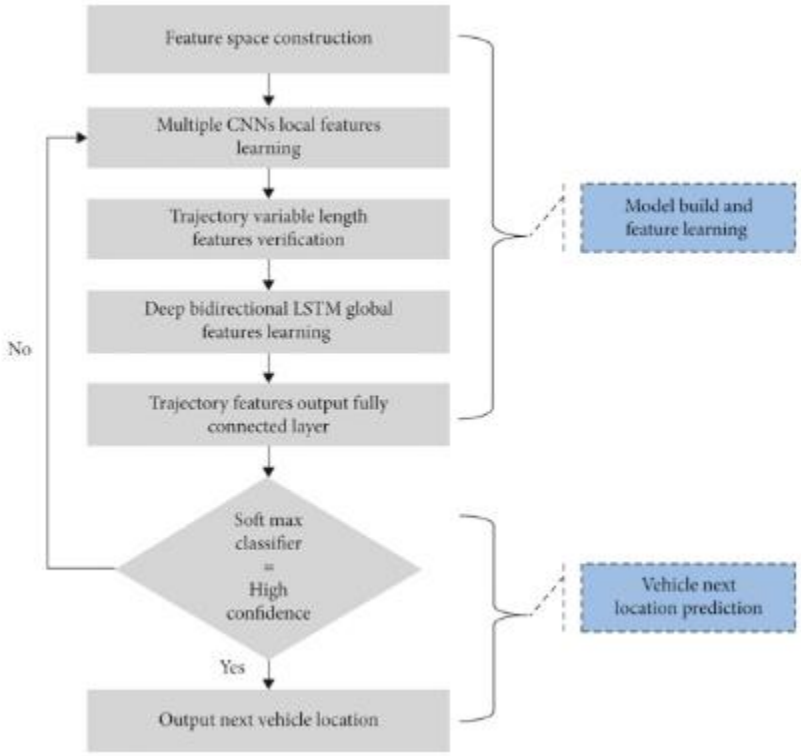

Figure 1. **Machine Learning Technologies for Secure Vehicular Communication**

Additionally, the paper explores the use of AI-driven encryption mechanisms and reinforcement learning for dynamic access control, aiming to enhance the overall resilience of VCC against a spectrum of security challenges. The subsequent sections of this paper will delve into a comprehensive exploration of the proposed AI-based security measures, their implementation, and their efficacy in real-world VCC scenarios[6]. Through simulations and experiments, the study aims to demonstrate the tangible benefits of AI-driven security solutions, paving the way for a secure and reliable deployment of Vehicular Cloud Computing technologies in the future.

2. A Comprehensive Study on the Integration of Artificial Intelligence for Vehicular Cloud Computing Security:

Vehicular Cloud Computing (VCC) represents a revolutionary paradigm that integrates cloud computing technologies into vehicular networks, offering a myriad of possibilities for intelligent transportation systems[7]. As vehicular environments become increasingly connected and data-driven, the promise of enhanced safety, traffic management, and in-car services is counterbalanced by the escalating challenges posed by cybersecurity threats. Recognizing the imperative to fortify the security infrastructure of VCC, this paper embarks on a comprehensive study focusing on the integration of Artificial Intelligence (AI) techniques to bolster Vehicular Cloud Computing security. VCC, with its dynamic nature and diverse applications, presents a unique set of security concerns that transcend traditional approaches. Data privacy, authentication, and the potential compromise of safety-critical systems underscore the need for innovative and adaptive security measures. In response to these challenges, AI emerges as a transformative solution, leveraging its learning, pattern recognition, and adaptability to address the intricate security landscape of Vehicular Cloud Computing.

The objective of this study is to delve into the multifaceted integration of AI in VCC security, examining the potential of machine learning, deep learning, and other AI techniques to enhance the robustness of security mechanisms[8]. As we navigate through the intricacies of securing connected vehicles and cloud infrastructure, the paper aims to provide a holistic understanding of how AI can be harnessed to identify and mitigate threats in real-time, secure communications, and fortify access control mechanisms. Vehicular Cloud Computing (VCC) represents a paradigm shift in the realm of intelligent transportation systems, offering a dynamic framework that intertwines vehicular networks with the power of cloud computing. This integration opens up a spectrum of possibilities, from optimized traffic management to the realization of connected and autonomous vehicles. However, the transformative potential of VCC is accompanied by a host of security challenges that demand innovative solutions. This paper embarks on a comprehensive exploration of the integration of Artificial Intelligence (AI) for enhancing the security of Vehicular Cloud Computing. In the face of evolving threats and the critical nature of vehicular networks, traditional security mechanisms reveal limitations in adaptability and resilience[9].

Leveraging the capabilities of AI becomes imperative to fortify VCC against an array of security concerns, including data privacy, authentication, and the integrity of safety-critical applications. The primary objective of this study is to provide a nuanced understanding of the challenges within VCC and to present a holistic framework that harnesses the potential of AI for addressing these challenges. Through an in-depth analysis of the unique security landscape of Vehicular Cloud Computing, we aim to demonstrate how AI, encompassing machine learning, deep learning, and other intelligent techniques, can serve as a catalyst for robust and adaptive security measures. The primary objective of this study is to explore how AI techniques can be strategically employed to

fortify the security posture of Vehicular Cloud Computing. AI offers a range of capabilities, including machine learning, deep learning, and anomaly detection, which can be harnessed to adaptively respond to emerging security threats. The integration of AI not only enhances the detection and mitigation of risks but also enables the development of proactive and intelligent security measures tailored to the specific challenges posed by VCC[10]. The Network as a Service and Storage as a Service for Cloud Computing in Vehicular Communication shown in figure 2.

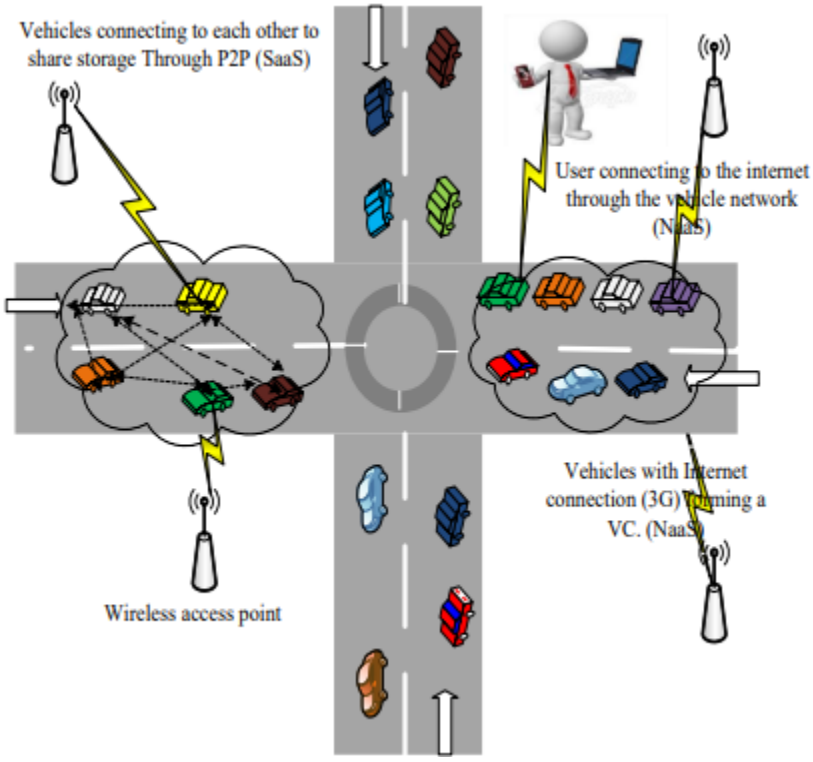

Figure 2. **The Network for Cloud Computing in Vehicular Communication**

3. A Deep Dive into Artificial Intelligence Solutions for Vehicular Cloud Computing Security:

The fusion of Vehicular Cloud Computing (VCC) with Artificial Intelligence (AI) marks a transformative convergence that holds the promise of revolutionizing the landscape of intelligent transportation systems[11]. As vehicles become increasingly connected and reliant on cloud services, the synergy of VCC and AI emerges as a potent solution to propel not only efficiency and convenience but also security in vehicular environments. This paper presents a comprehensive exploration, offering a deep dive into the integration of AI solutions to fortify the security aspects of Vehicular Cloud Computing. VCC introduces a paradigm shift in how vehicles interact with each other and their surrounding infrastructure, fostering the potential for dynamic traffic management, real-time communication, and an enhanced driving experience. However, the vast

amount of sensitive data generated in these interconnected systems, combined with the critical role of vehicular networks in safety-critical applications, amplifies the urgency of addressing security challenges.

This study focuses on unraveling the intricacies of Vehicular Cloud Computing security and delves into the application of advanced AI techniques to navigate and mitigate the evolving threats in this dynamic ecosystem. AI, encompassing machine learning, deep learning, and anomaly detection, presents an adaptive and intelligent approach to counteract the sophisticated security challenges inherent in VCC environments[12]. Vehicular Cloud Computing (VCC) stands at the forefront of technological innovation, blending cloud computing capabilities with the dynamic and mobile environment of vehicular networks. This convergence holds the promise of transforming transportation systems by enabling vehicles to leverage cloud resources for enhanced communication, navigation, and safety applications. However, this integration introduces a complex array of security challenges that demand sophisticated solutions to safeguard the integrity, privacy, and reliability of vehicular systems.

This paper presents a comprehensive exploration, offering a deep dive into the application of Artificial Intelligence (AI) solutions to fortify the security landscape of Vehicular Cloud Computing[13]. As vehicles become increasingly connected and data-driven, the vulnerability to cyber threats escalates, requiring adaptive and intelligent security measures. Traditional security mechanisms are often insufficient to cope with the dynamic nature of vehicular environments and the evolving tactics employed by malicious actors. The primary goal of this study is to delve into the intricacies of employing AI solutions as a robust defense mechanism against security threats in Vehicular Cloud Computing. AI brings a suite of capabilities, including machine learning, deep learning, and anomaly detection, which can be tailored to address the unique challenges posed by the integration of cloud technologies into vehicular networks. By harnessing the power of AI, it becomes possible to not only detect and respond to security incidents in real-time but also to proactively adapt to emerging threats[14].

4. Conclusion:

In summary, this paper aims to provide a comprehensive understanding of the security challenges within Vehicular Cloud Computing and advocates for the integration of AI as a cornerstone for developing adaptive, intelligent, and robust security measures. As VCC continues to evolve, the symbiotic relationship between AI and vehicular security becomes increasingly imperative for ensuring a secure and resilient transportation ecosystem. The dynamic and open nature of VCC environments, coupled with the critical role these networks play in safety-critical applications, underscores the importance of robust security measures. The adaptive and intelligent nature of AI techniques, including machine learning, deep learning, and anomaly detection, has been harnessed to create a comprehensive security framework.

Data Availability. Not applicable.

Conflict of interest. Author declares no personal and/or financial conflict of interest regarding the publication of this research paper.

References

[1] B. Namatherdhala, N. Mazher, and G. K. Sriram, "Uses of Artificial Intelligence in Autonomous Driving and V2X communication," International Research Journal of Modernization in Engineering Technology and Science, vol. 4, no. 7, pp. 1932-1936, 2022.

[2] A. Masood, D. S. Lakew, and S. Cho, "Security and privacy challenges in connected vehicular cloud computing," IEEE Communications Surveys & Tutorials, vol. 22, no. 4, pp. 2725-2764, 2020.

[3] K. N. Qureshi, G. Jeon, and F. Piccialli, "Anomaly detection and trust authority in artificial intelligence and cloud computing," Computer Networks, vol. 184, p. 107647, 2021.

[4] H. Allam, J. Dempere, V. Akre, D. Parakash, N. Mazher, and J. Ahamed, "Artificial intelligence in education: an argument of Chat-GPT use in education," in 2023 9th International Conference on Information Technology Trends (ITT), 2023: IEEE, pp. 151-156.

[5] M. S. Alsayfi, M. Y. Dahab, F. E. Eassa, R. Salama, S. Haridi, and A. S. Al-Ghamdi, "Big data in vehicular cloud computing: review, taxonomy, and security challenges," Elektronika Ir Elektrotechnika, vol. 28, no. 2, pp. 59-71, 2022.

[6] A. Aliyu et al., "Cloud computing in VANETs: architecture, taxonomy, and challenges," IETE Technical Review, vol. 35, no. 5, pp. 523-547, 2018.

[7] N. Mazher, M. Alhadaad, and O. Shagdar, "A Brief Summary of Cybersecurity attacks in V2X Communication," 2022.

[8] M. S. Sheikh, J. Liang, and W. Wang, "Security and privacy in vehicular ad hoc network and vehicle cloud computing: a survey," Wireless Communications and Mobile Computing, vol. 2020, pp. 1-25, 2020.

[9] S. Achar and N. Mazher, "Practices and Limitations of Public Cloud Contracts," ed: vol.

[10] L. Hernandez, M. Hassan, and V. P. Shukla, "Applications of Cloud Computing in Intelligent Vehicles: A Survey," Journal of Artificial Intelligence and Machine Learning in Management, vol. 7, no. 1, pp. 10-24, 2023.

[11] N. Mazher, A. Brightini, and F. Haider, "Vehicular Platooning to be Secure against Cybersecurity Attacks," Authorea Preprints, 2022.

[12] J. Deng et al., "A Survey on Vehicular Cloud Network Security," IEEE Access, vol. 11, pp. 136741-136757, 2023.

[13] N. Kumar, J. P. Singh, R. S. Bali, S. Misra, and S. Ullah, "An intelligent clustering scheme for distributed intrusion detection in vehicular cloud computing," Cluster Computing, vol. 18, pp. 1263-1283, 2015.

[14] M. R. Belgaum, S. Musa, M. Alam, and M. Mazliham, "Integration challenges of artificial intelligence in cloud computing, Internet of Things and software-defined networking," in 2019 13th International Conference on Mathematics, Actuarial Science, Computer Science and Statistics (MACS), 2019: IEEE, pp. 1-5.