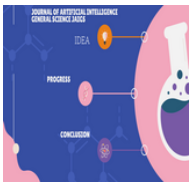
ISSN: 3006-4023 (Online), Vol. 2, Issue 1
Journal of Artificial Intelligence General Science (JAIGS)

journal homepage: **https://jaigs.org/index.php/JAIGS**



Security Challenges of Vehicular Cloud Computing

Jaydeep Thakker

Abstract

In the realm of Industry 4.0, the utilization of artificial intelligence (AI) and machine learning for anomaly detection faces challenges due to significant computational demands and associated environmental consequences. This study aims to tackle the need for high-performance machine learning models while promoting environmental sustainability, contributing to the emerging concept of 'Green AI.' We meticulously assessed a wide range of machine learning algorithms, combined with various Multilayer Perceptron (MLP) configurations. Our evaluation encompassed a comprehensive set of performance metrics, including Accuracy, Area Under the Curve (AUC), Recall, Precision, F1 Score, Kappa Statistic, Matthews Correlation Coefficient (MCC), and F1 Macro. Concurrently, we evaluated the environmental footprint of these models by considering factors such as time duration, CO2 emissions, and energy consumption during training, cross-validation, and inference phases.

While traditional machine learning algorithms like Decision Trees and Random Forests exhibited robust efficiency and performance, optimized MLP configurations yielded superior results, albeit with a proportional increase in resource consumption. To address the trade-offs between model performance and environmental impact, we employed a multi-objective optimization approach based on Pareto optimality principles. The insights gleaned emphasize the importance of striking a balance between model performance, complexity, and environmental considerations, offering valuable guidance for future endeavors in developing environmentally conscious machine learning models for industrial applications.

Keywords: Anomaly Detection, Green AI, Trustworthy AI, Machine Learning, Artificial Intelligence, Industrial Environments, Comparative Study, Environmental Impact.

Article Information:
Article history: Received: 01/02/2024 Accepted: 05/02/2024 Online: 10/03/2024 Published: 10/03/2024
Corresponding author: Jaydeep Thakker email: jaydeep2005@gmail.com

Introduction

By constantly connecting resources and gathering data, a vehicle cloud may be instantly constructed. Vehicles can access the cloud and receive get all of the necessary resources and apps they want when they need them. The VCC may be quite advantageous for vehicles, especially less expensive ones. For instance, in bad wealth automobiles without pricey radar cruise systems may request vehicle collision detection service. It is obvious that security and privacy concerns must be resolved if the VCC concept is to be widely adopted and have a substantial social impact.[1] Unlike traditional wireless networks, VANETs, or cloud computing, VCC has significant potential security and privacy issues. The number of vehicles rises in direct proportion to the enormous growth of the human population. According to statistics, there are already 1 billion automobiles on the road, and that number will double by 2050. Along with travel conveniences, this influx of vehicles creates other problems, such traffic congestion, roadside accidents, pollution, and more. To address these issues, the Intelligent Transport System (ITS) is a successful endeavor. To reach the goal of intelligent driving, these linked cars have embedded systems such as the onboard unit (OBU), electronic control unit, application unit, and head unit. Vehicle (V2V) communication models are used in ITS to enable vehicle-to-vehicle communication and the sharing of useful information. Vehicles can interact with linked Road Side Unit (RSU) systems on the side of the road via Vehicle- to- Infrastructure (V2I) communication.[2] It's also known as (Vehicle- to- Network)V2N . Through the use of computer equipment, like laptops or mobile phones, cars and pedestrians may interact while they are both on the road (V2P communication).[3]

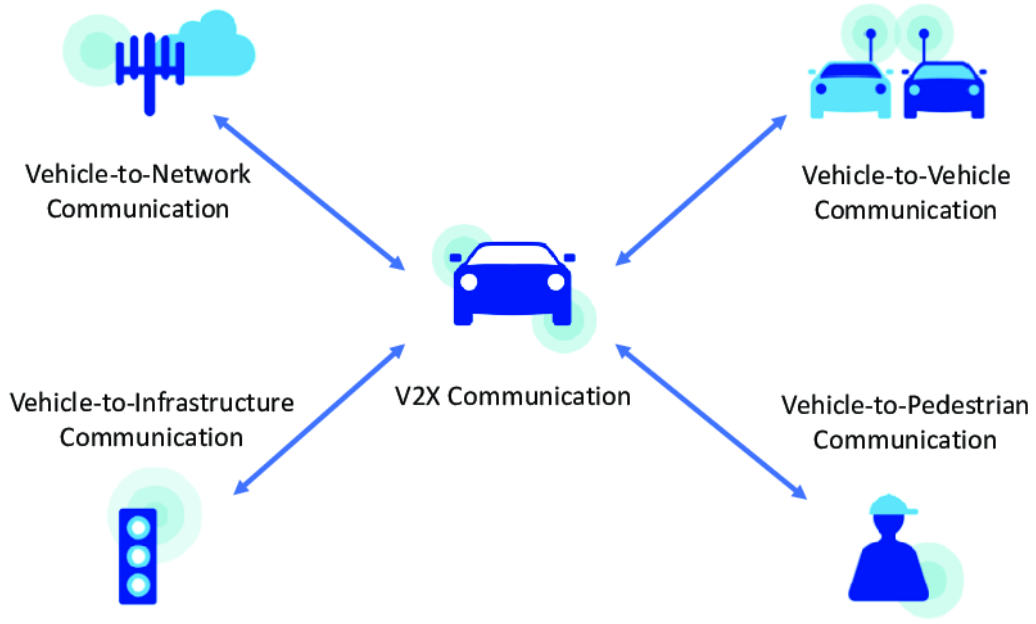


Figure.1 Vehicle Communication Model

To establish the above connections, a vehicular ad-hoc network (VANET) is created. VANET is a wireless connection architecture for offering automobile safety and also non-safety services. Dedicated Short Range Communication (DSRC), the most popular V2X interaction technology, enables communication between cars and other connected devices in VANET. Additionally, Long Term Evolution (LTE), also known as V2X-LTE, has attracted a lot of attention in the V2X communication community. Additionally, 5G technologies are finding a place in the V2X communication paradigm.[4] Vehicular Cloud Computing (VCC) is a brand-new hybrid system that aims to take

advantage of the computing power of VANET devices in order to provide consumers with useful services on a pay-as-you-go basis. In order to create a cloud of shared resources with plenty of computing resources, VCC works in conjunction with VANET elements like RSU or cars within a defined range (almost 300 meters). To handle constraints and overloaded service expectations, VCC strives to manage onboard computers, storage resources, sensor equipment, and communication facilities. The most important applications offered by VCC are traffic management, data outsourcing, outsourced computing, access control, data sharing, and additional value-added services, including entertainment, traffic safety, autonomous driving, and road management. Due to its unique characteristics, such as the cloud's multi-tenancy, quick services, high vehicle movement, and short range of linked devices, the security of VCC is the largest problem in the VCC tale.[5] We will discuss security needs and potential threats will be discussed in the following section.

Vcc Security Assessment

Security requirements and a hypothetical assault against VCC are presented in this section. VCC has additional security difficulties in addition to the inherent security constraints of cloud computing. The primary feature of VCC that sets it apart from CC is the dynamic switching of the available computer resources. Furthermore, VCC cars are unreliable since they enter a shared resource pool for a brief time before leaving.[6] One car never has a neighbor who remains for a long time, and each vehicle has a neighbor who frequently changes, which makes it difficult to build confidence. The resources that offer computational services to other resources may also be used by possible malicious vehicles due to VCC. These features add further difficulties to the security problems with cloud computing.

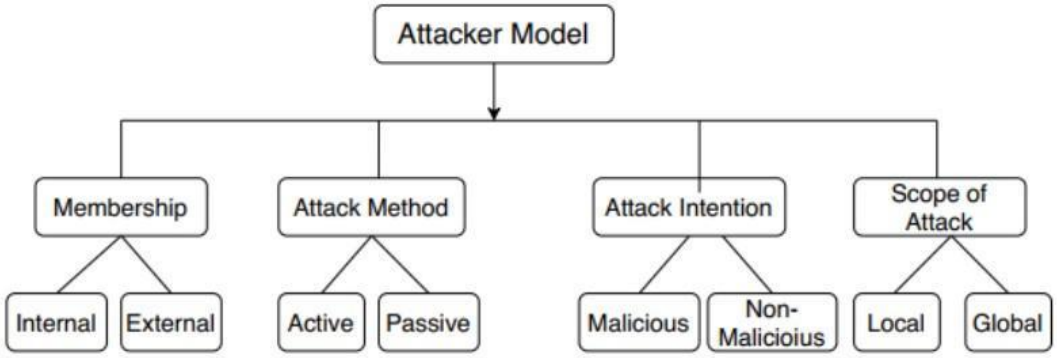


Figure.2 Vehicular cloud computing Attack Model

Internal intruders have given VCC members permission to access and make use of VCC resources legally. External intruders attack by maliciously gaining access to VCC even if they are not permitted to do so. They could physically harm RSUs or other stationary infrastructure, for instance. Messages, signals, and other sources can all be promptly attacked by an active assault, such as by inserting a bogus message. The security of data stored in the cloud is threatened by active attackers. Important papers, saved data, more private information, and executable code can all be included in this material. Passive attackers use the information for future use, as opposed to active attackers who actively modify data. They might function in a wireless network as an eavesdropper.[7]

Comparison of malicious and non-malicious attackers

Despite their gain, the malevolent attacker has harmful objectives. This type of attacker has the ability to introduce malware into the system, causing disruption or even system failure. A greedy attacker who intends to attack the system personally is another name for a non-malicious attacker. They may, for instance, inform people about the emergency system and reduce traffic.[8] Different types of attackers have different ranges of attack. Limited automobiles are affected by the neighborhood attacker. They may, for instance, set up listening posts for a select group of VCC organizations or adjacent automobiles. The global attacker, in comparison, has a larger domain and the ability to command additional VCC units, allowing them to access a wider variety of data in the vehicular cloud network.[9] According to the aforementioned concept, a Global Passive Attacker (GPA), whether internal or external, may cause the most damage by listening in on global broadcast information and violating location privacy for their targeted range of vehicles. GPA can build its listening post by utilizing already-existing infrastructures like RSU.

Requirement for Security and Possible Attacks

An important requirement of VCC is authenticity, which separates harmful from genuine organizations from the harmful ones.The VCC system ought to be able to identify genuine VCC entities. Message authentication and user authentication are two further categories of authentication needs. On the basis of a predetermined set of regulations, it should be assured that only authorized VCC entities have access to excellent VCC service. To specify which VCC entity may access particular VCC services, there needs to be some sort of Service Level Agreement (SLA).[10] The process of sending communications across VCC entities on time in order to prevent service disruption is covered by the availability requirement. Availability may be achieved with a low-cost cryptographic approach to guarantee that communications get to their destination in the required amount of time without being tempered. Information security is a necessity for sending data to a target entity in its original form. Since most messages in the VCC environment are visible to everyone, data confidentiality is not given primary importance. It is mostly required for some private communications between two parties. Data transit between two entities should be independently verified to look for any signs of data manipulation, deletion, or change.

CONCLUSION

This study provides a comprehensive review of vehicular cloud computing networks, including a discussion of the key ideas and security concerns. A new hybrid technology that combines cloud computing and intelligent transportation systems is called vehicular cloud computing. Cloud computing for vehicles requires close attention in the area of security. We discussed the security issues and difficulties posed by a unique approach to VANETs by moving VANETs to the clouds. We started by outlining the security and privacy issues that networks using vehicular cloud computing must deal with, as well as some potential security fixes. Although some of the solutions can make use of the current security methods, there are several particular difficulties. On the same cloud server, attackers can physically assemble. High mobility and erratic interaction are fundamental characteristics of vehicles. Intelligent transportation systems must be implemented in a methodical and synthetic approach because of the extensive effort being done on security and privacy in VC. Vehicular cloud computing networks can only offer reliable and workable security and privacy solutions with coordinated efforts and tight collaboration among several institutions, including law enforcement, the government, the automotive car industry, and academia.

References

[1] G. Sriram, "Security challenges of vehicular cloud computing," *International Research Journal of Modernization in Engineering Technology,* 2022.

[2] G. Yan, D. Wen, S. Olariu, and M. C. Weigle, "Security challenges in vehicular cloud computing," *IEEE Transactions on Intelligent Transportation Systems,* vol. 14, no. 1, pp. 284-294, 2012.

[3] H. Goumidi, Z. Aliouat, and S. Harous, "Vehicular cloud computing security: A survey," *Arabian Journal for Science and Engineering,* vol. 45, pp. 2473-2499, 2020.

[4] M. K. Sharma and A. Kaur, "A survey on vehicular cloud computing and its security," in *2015 1st International conference on next generation computing technologies (NGCT)*, 2015: IEEE, pp. 67-71.

[5] M. Whaiduzzaman, M. Sookhak, A. Gani, and R. Buyya, "A survey on vehicular cloud computing," *Journal of Network and Computer applications,* vol. 40, pp. 325-344, 2014.

[6] F. Ahmad, M. Kazim, A. Adnane, and A. Awad, "Vehicular cloud networks: Architecture, applications and security issues," in *2015 IEEE/ACM 8th International Conference on Utility and Cloud Computing (UCC)*, 2015: IEEE, pp. 571-576.

[7] G. Yan, D. B. Rawat, and B. B. Bista, "Towards secure vehicular clouds," in *2012 Sixth International Conference on Complex, Intelligent, and Software Intensive Systems*, 2012: IEEE, pp. 370-375.

[8] H. Li, R. Lu, J. Misic, and M. Mahmoud, "Security and privacy of connected vehicular cloud

computing," *IEEE Network,* vol. 32, no. 3, pp. 4-6, 2018.

[9] A. Alamer, Y. Deng, G. Wei, and X. Lin, "Collaborative security in vehicular cloud computing: A game theoretic view," *IEEE Network,* vol. 32, no. 3, pp. 72-77, 2018.

[10] M. Gerla, "Vehicular cloud computing," in *2012 The 11th annual mediterranean ad hoc networking workshop (Med-Hoc-Net)*, 2012: IEEE, pp. 152-155.