
# BRIEFING NOTES

# BN-72-Space and Cyberspace-Aug2021

## SECURITY AND PRIVACY ISSUES IN VEHICULAR CLOUD COMPUTING

Authors: Reza Bahrevar[1] and Kash Khorasani[2]
1 Graduate student, Department of Electrical and Computer Engineering, Concordia University, Montreal, Canada
2 Professor, Department of Electrical and Computer Engineering, Concordia University, Montreal, Canada

## SUMMARY

- Vehicular Ad hoc Network (VANET) is one of the concepts that is being developed with the advancements of IoT. VANET creates an Internet of Vehicles (IoV) such that the vehicles are equipped with sensory devices that provide computational, storage, as well as networking capabilities and functionalities.
- VANET-based systems will have a variety of applications such as entertainment, navigation, or distaste control. The effectiveness of these systems depends on low latency, wide reliable communication networks, and real-time data-processing capabilities.
- With spread of 5G technology getting closer to emergence of edge cloud computing services, next gen transportation systems, aerospace, and automotive industries will be promoting and implementing intelligent and novel applications of VANET. A number of benefits of this technology and possible challenges in terms of security and privacy need to be further investigated and analyzed.


## CONTEXT

- VANET will provide a distributed infrastructure that could be utilized for data storage, traffic management, surveillance, and infotainment purposes [1],[2].
- Vehicular cloud network connections can be established between the vehicles or from the vehicles to the designated cloud computing infrastructure (for example, a local fog computing server) [2].
- The vehicular cloud network will reduce the expenses of IoT computational resources for the vehicle manufacturers. It has applications in traffic management, where an unexpected incident due to a natural disaster, accidents, or repairs can be reported through a network of other vehicles [2],[3].
- It has applications in intelligence, surveillance, and reconnacance (ISR), where sensory devices can be installed on vehicles with image recognition capabilities that can be used for a variety of purposes, such as reporting suspicious activities, location detection, and emergency broadcasts [3],[4].
- It has applications in infotainment, where the client's data will be utilized for distributing information about the road, weather, or monitoring purposes for the driver [3].
- Safety regulation specific to adversarial based cyber-attacks, privacy concerns regarding location, shared information between the vehicles and networks, and issues on usage of image recognition devices are of the main concerns for this technology.

## CONSIDERATIONS

- Security and privacy considerations for vehicular cloud computing with respect to advancements made in IoT, edge-cloud and 5G should be further investigated.
- What are the policy considerations with respect to adversarial cyber-attacks and malicious intruders?
- How to ensure data transparency concerns and requirements are satisfied in the VANET while simultaneously develop security and privacy capabilities in these systems?

## NEXT STEPS

- One has to tackle privacy, safety, and security problems with respect to any given human-machine VANET application so that in infotainment, disaster control, or surveillance, different policies have to be considered.
- One should develop answers to the privacy challenges of VANET systems with respect to the IoT. We should categorize the policies related to the vehicle to vehicle as well as vehicle to the cloud infrastructure.
- For example, besides the vehicle to cloud protocols, vehicle to vehicle communication protocols must also follow high standards to prevent adversarial access and intrusions.
- Large-scale utilization of image processing technology should be closely monitored. For example, in surveillance and disaster control, only trusted or government-supervised companies should be allowed to perform these operations.
- An AI surveillance system should not be used as a judgment tool on the intent of a crime. This type of technology can cause damage to the trust of the society towards the government. Therefore, it must be ensured that these systems will gather and store information relevant to their intended use.
- One must provide a clear definition of sensitive data. For example, VANET technology can help in situations such as finding lost children. However, gathering image data from children can be considered problematic.
- One should look into the safety challenges associated with the IoT and transparency of these type of technologies. Are these systems tested and robust against adversarial attacks? For example, can an adversary take control of an autonomous system?
- Companies must be transparent in terms of the type of data that they store. There should be a mechanism in place that would enforce the removal of sensitive data. Edge servers also should be prohibited for sharing or selling sensitive data to third parties. However, the servers may be allowed to gather and buy non-sensitive necessary data from third parties to boost the performance of such systems.

## REFERENCES


[1] Alhilal, A., Braud, T. and Hui, P., 2020. Distributed Vehicular Computing at the Dawn of 5G: a Survey. arXiv preprint arXiv:2001.07077.

[2] Musaddiq, A., Ali, R., Bajracharya, R., Qadri, Y.A., Al-Turjman, F. and Kim, S.W., 2020. Trends, Issues, and Challenges in the Domain of IoT-Based Vehicular Cloud Network. In Unmanned Aerial Vehicles in Smart Cities (pp. 49-64). Springer, Cham.

[3] Al-Turjman, F., 2020. Unmanned Aerial Vehicles in Smart Cities. Springer Nature.

[4] Agarwal, Y., Jain, K. and Karabasoglu, O., 2018. Smart vehicle monitoring and assistance using cloud computing in vehicular Ad Hoc networks. International Journal of Transportation Science and Technology, 7(1), pp.60-73.