ABSTRACT
In Vehicular Ad-hoc Networks (VANETs), neighboring vehicles communicate with each other and with the roadside infrastructure about the traffic using wireless communication. Therefore, message authentication and trustworthiness of messages become crucial for monitoring traffic. In this paper, we propose an edge cloud-based decision-making model to provide accurate traffic information for possible events like congestion at an ROI. Security of event-related responses, and velocity and GPS coordinates reported by neighboring vehicles at the time of a request by ROI for every vehicle are used for accurately determining the traffic flow. We evaluate the performance of the proposed model using VENTOS and SUMO simulators, and a simulated cloud environment where the consensus-based and the driver-rating based models fail to provide the correct prediction when the number of malicious vehicles is in majority. We also compare our model against an existing peer-based authentication model, and show that our model offers low communication overhead and better resiliency against security attacks.