



Secure V2V and V2I Technologies for the Next-Generation Intelligent Transportation Systems

Sudip Mittal, University of North Carolina Wilmington

This installment of Computer's series highlighting the work published in IEEE Computer Society journals comes from IEEE Transactions on Services Computing.

Vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) technologies are transforming the digital landscape. The automotive industry is shifting into a new digital

age, where connected vehicles and smart cars are starting to collaborate among themselves with less reliance on human drivers. This communication is especially useful when considering their benefits toward smart cities. Smart vehicles can exchange information with each other, physical infrastructure like roadside units, and even potentially pedestrians. These use cases present bountiful opportunities for cities to address a number of issues, from traffic management to even the prevention of potential collisions. Despite the benefits, V2V and V2I communication technologies also present a broad attack surface

for cybercriminals. Some examples include stealing private data, remotely hijacking a vehicle, and coordinating roadside infrastructure attacks.

M. Gupta et al.¹ present an approach to securing V2V and V2I communication by utilizing cloudlets to ensure the confidentiality, integrity, and authentication of messages across a system. In addition, they discuss

Digital Object Identifier 10.1109/MC.2020.3042227
Date of current version: 11 February 2021



an attribute-based access control model for V2V and V2I called the *attribute-based intelligent transportation system (AB-ITS)*. The proposed cloudlet architecture is depicted in Figure 1. Trusted edge infrastructures produced by city administrators will

The automotive industry is shifting into a new digital age, where connected vehicles and smart cars are starting to collaborate among themselves with less reliance on human drivers.

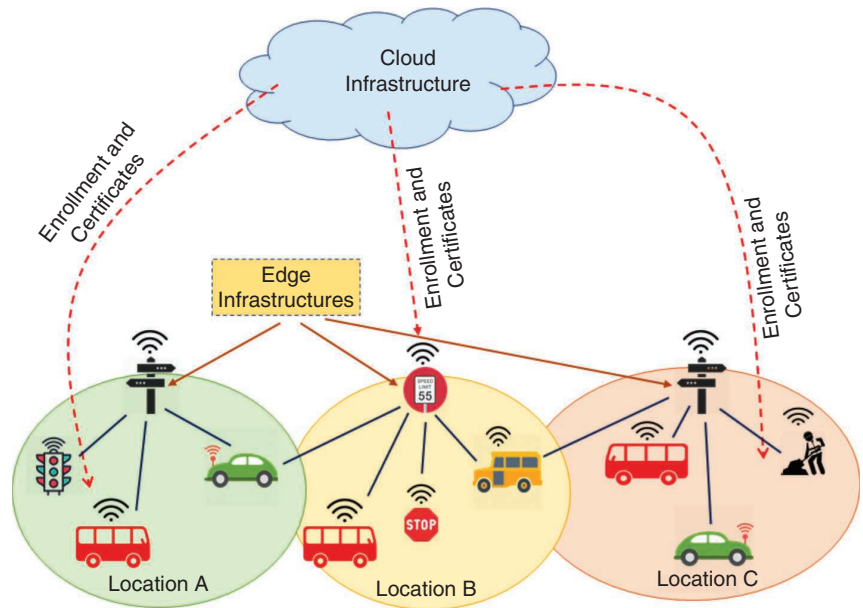


FIGURE 1. The proposed trusted cloudlet architecture. (Taken from Gupta et al.¹)

operate as intermediaries between vehicles and entities inside the city's geographic range by relaying secured messages. At the edge, messages are validated by a set of predetermined security policies before being forwarded across the interconnected network. Figure 2 illustrates a conceptual AB-ITS model. The attributes developed in the AB-ITS are supported by the cloudlets. A source initiates operations on cloudlets and can be a set of vehicles, a transportation infrastructure, or administrative users. Trusted cloudlets (TCs) enroll devices into a system through the use of a traditional public key infrastructure scheme. Target vehicles (V_T) and source vehicles must be a part of the same TC to communicate. Authorization policies and attributes define operations for the overall secure functioning of the ecosystem. Policies and attributes are also dynamic in nature and can shift to fit changing circumstances or communication preferences in a city.

A proof-of-concept implementation of the AB-ITS was simulated on the Amazon Web Services Internet of Things platform. The authors modeled

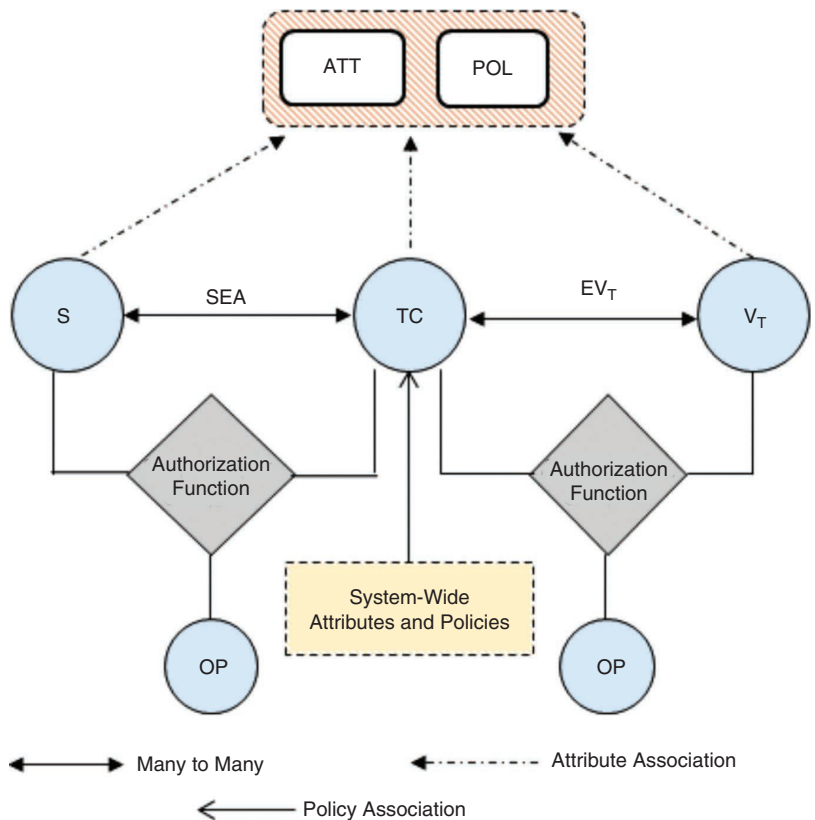



FIGURE 2. An AB-ITS communication model. ATT: attributes; POL: policies; S: source; TC: trusted cloudlets; V_T : target vehicles; OP: operations; SEA: source entity attribute relations; EV_T : vehicle to trusted cloudlet relations. (Taken from Gupta et al.¹)

situations such as ice-on-road and compromised rogue vehicles. The performance of the model can be measured by the execution time of attribute-based security policies against the number of vehicles associated with a cloudlet. The authors found that the total trip time was comparable to that for a peer-to-peer ITS despite variations due to network traffic and latency. In a large city, more cloudlets and

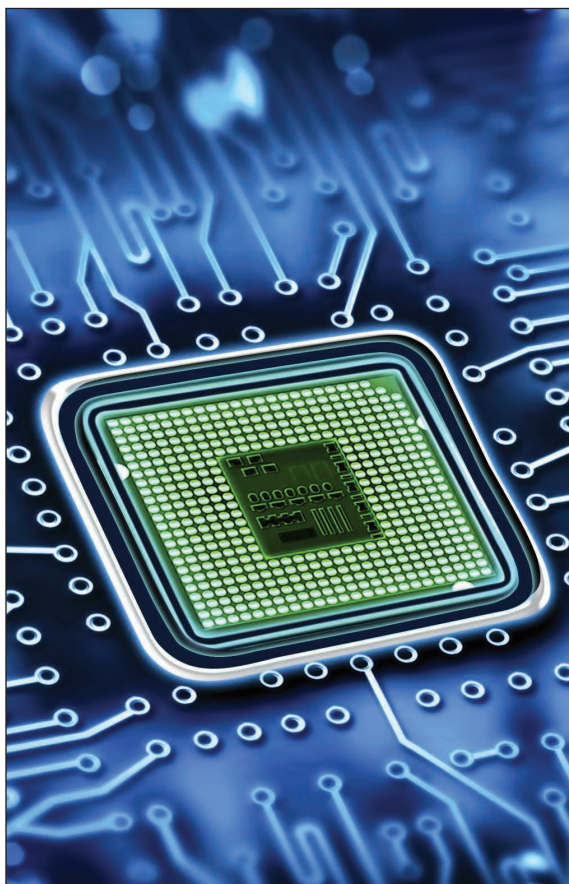
infrastructure devices can be installed to reduce the crowding of vehicles within one cloudlet, improving the execution time. 

REFERENCE

1. M. Gupta, J. Benson, F. Patwa, and R. Sandhu, "Secure V2V and V2I communication in intelligent transportation using cloudlets." *IEEE Trans. Services Comput.*, vol. 13, no. 14,

pp. 1-13, Sept. 22, 2020. doi: 10.1109/TSC.2020.3025993.

SUDIP MITTAL is an assistant professor in the Department of Computer Science at the University of North Carolina Wilmington, Wilmington, North Carolina, 28403, USA. Contact him at mittals@uncw.edu.



IEEE TRANSACTIONS ON

COMPUTERS

Call for Papers: *IEEE Transactions on Computers*

Publish your work in the IEEE Computer Society's flagship journal, *IEEE Transactions on Computers*. The journal seeks papers on everything from computer architecture and software systems to machine learning and quantum computing.

Learn about calls for papers
and submission details at
www.computer.org/tc.

