ACM Transactions on Internet Technology (TOIT)

https://dl.acm.org/journal/toit

Special Issue on

Cyber Security in Internet of Vehicles

Important Dates

Manuscript Submission:
January 31, 2021
First Notification:
April 5, 2021
Submission of Revised Manuscript:
June 2, 2021
Final Notification:
September 30, 2021
Final Paper Due:
December 10, 2021

Guest Editors

Dr. Ching-Hsien Hsu,
Chair Professor and Dean,
Asia University, Taiwan
Email: robertchh@asia.edu.tw

Dr. Amir H. Alavi,
University of Pittsburgh, USA
Email: alavi@pitt.edu

Dr. Mianxiong Dong
Muroran Institute of Technology, Japan
Email: mx.dong@csse.muroran-it.ac.jp

ACM TOIT Editor-in-Chief

Professor Ling Liu
School of Computer Science
Georgia Institute of Technology
ling.liu@cc.gatech.edu

Submission Instructions:

Please Refer to
http://toit.acm.org/authors.cfm

Please select "Cyber Security in Internet of Vehicles" in the TOIT Manuscript Central Website

In today's world, every individual possesses substantial complications relating to transportation systems such as congestion, vehicle parking difficulties, pollution caused by increased level of carbon dioxide emission, longer traveling times, road accidents, etc. These consequences are due to the rising number of vehicular systems and rapid urbanization processes. This leads to the development of modern technologies such as Intelligent Transport Systems (ITS), Vehicular ad-hoc Networks (VANET), VANET cloud (VC), and Internet of Vehicles (IoV). Among all these techniques, IoV remains to be the most prominent and emerging one. IoV is a series of interconnected vehicles that communicate with each other through a common public network. It is a highly integrated application of two major domains: IoT and ITS. The communication across the IoV network includes three different types, including Vehicle to Vehicle (V2V), Vehicle to Infrastructure (V2I), and Vehicle to Pedestrian (V2P).

Smart vehicles with progressive communication abilities do not only communicate with broadcast and navigation satellites but also with various smart devices such as roadside units, smart vehicles, and passenger smartphones. Since IoV has widespread interconnected networks with numerous users, it is obvious that there is an increased risk of security and privacy. These security and privacy risks may lead to serious consequences if they are not addressed and dealt in an appropriate manner. Some of the most common security and privacy issues across the IoV environment include tracking vehicle locations, hardware tampering, unauthorized data access, message modification, and fabrication. The intruders can even introduce an ambiguity across the network and steal confidential data with the inevitable loss of data integrity and privacy features. Thus, advanced security measures for IoV systems have become essential requirements.

In recent years, the concept of cybersecurity is immensely applied across various domains to protect networks, data, programs, and devices from security vulnerabilities and unauthorized data access. IoV transmits sensitive data across networks and to other devices for various means and confidentiality purposes. The possibility of cyber-attacks is comparatively higher when data transmission takes place more frequently through various nodes of IoV systems. Thus, the application of cybersecurity measures for IoV provides the most prominent solution for security and privacy.

This special issue mainly focuses on the development of various cybersecurity mechanisms for IoV systems with improved security and privacy features. Furthermore, it brings out the various researchers and industry people from different fields of computer science to come up with novel and effective cyber-security solutions for security protection in IoV systems.

Potential topics include but are not limited to the following:

- Security and Privacy in IoV using cybersecurity mechanisms,
- Enhanced cybersecurity mechanisms for Vehicle to Vehicle (V2V), Vehicle to Infrastructure (V2I) and Vehicle to Pedestrian (V2P) communication in IoV,
- Novel and efficient frameworks for improving trust based secure communication in IoV,
- Secure cloud assisted cybersecurity mechanisms for IoV,
- Trust based security algorithms for Social Internet of Vehicles (SIoV),
- Social Internet of Vehicles (SIoV): Architecture, security, privacy, and future directions,
- Security protocols for various applications of IoV using cybersecurity,
- Protection and management of cybersecurity across critical IoV systems,
- Secure authentication and access control mechanisms for IoV using cybersecurity,
- Novel and improved cybersecurity solutions for IoV in smart cities.