Guest Editors' Introduction

Security, Trust and Privacy Solutions for Intelligent Internet of Vehicular Things—Part II

Uttam Ghosh
Meharry Medical College

Hellen Maziku
University of Dar es Salaam (UDSM)

Hari Prabhat Gupta
Indian Institute of Technology BHU

Biplab Sikdar
National University of Singapore

Joel J. P. C. Rodrigues
China University of Petroleum (East China)

The Internet of Things evolution has given birth to several new groundbreaking applications, such as the Internet of Vehicles (IoV), smart cities, and cyber-physical systems. In IoV, the vehicles include various smart devices to obtain and communicate information from surroundings. This information can be helpful in safe navigation, detecting hurdles, optimizing routes, and in traffic management. For efficient decision making, in IoVs, V2V and V2X communication have been used to complement on-board sensors inputs and provide better services. A key concern when relying on vehicle data is vulnerability to data. Therefore, the need is to discuss the solutions that provide security, trust and privacy (STP) to both communicating entities and secure vehicle data from malicious entities. The use of artificial intelligence (AI) in multidimensional makes them useful for the Internet of Vehicles Things (IoVT). An Intelligent Internet of Vehicle Things (IIoVT) gives the desired results in the given time constraints with less human effort.

The increasing number of IoVT results in an increase in data exploration and risk to STP. This Special Section selected seven articles to address the issues and challenges related to STP in Intelligent IoVT. We briefly introduce the accepted articles in the following.

The article titled "Sema-IIoVT: Emergent Semantic-Based Trustworthy Information-Centric Fog System and Testbed for Intelligent Internet of Vehicles," by Zhang et al., designs an efficient emergency content dissemination network for aggregating and analyzing emergency information. Further, the authors propose a semantic-based trustworthy routing scheme that filters fake content from malicious entities. Furthermore, they implement a real testbed and a simulator to evaluate the benefit and performance of their proposed system.

In "Smart Emotion Recognition Framework: A Secured IOVT Perspective," Paikrao et al. propose a frontend processing framework to stress emotion detection cases (anger, sad, fear, and happy) in different nonstationary noisy environments (car, airport, traffic, and train). Further, the authors present experimental results to

Digital Object Identifier 10.1109/MCE.2022.3216361
Date of current version 6 December 2022.

show that favorable performance in state-of-the-art stress monitoring yields high levels of consumer satisfaction for security in vehicle comparison to traditional frameworks.

The article titled "Cybersecurity Digital Labels for Connected and Autonomous Vehicles," by Khan et al. proposes an idea of digital labels for connected and autonomous vehicles (CAVs) to increase the consumers trust and awareness regarding the security level of their vehicle. The authors also present an architecture called Cybersecurity Box (CSBox) in which digital labels display and inform the CAV consumers and passengers about its cybersecurity health status.

In "Contract-Theory-Based Secure Spectrum Sharing Framework in Internet of Vehicles," Zhu et al. propose a contract-theory-based secure spectrum sharing framework that adopts the consortium blockchain to guarantee the security of spectrum sharing and utilizes the practical Byzantine fault-tolerant consensus algorithm to achieve consensus in IoV. The authors design a preference-based spectrum allocation algorithm to maximize the total utility of secondary users.

In "Unsupervised Deep Learning Approach for in-Vehicle Intrusion Detection System," Narasimhan et al. present an unsupervised deep learning architecture for detecting intrusions on a Controller Area Network (CAN) bus. The authors also evaluate to show that the proposed method performs better than the existing unsupervised methods. Continuing the theme of preserving security in Intelligence IoV is Man et al.'s article titled "AI-Based Intrusion Detection for Intelligence Internet of Vehicles." This article first briefly introduces the concept and features of IoV, and then reviews the related research on AI-based IoV intrusion detection systems. Further, the authors present the open challenges and future research directions.

We close this Special Section with the article titled "Deep Learning-Based Intrusion Detection System for Internet of Vehicles," in which Ahmed et al. present an IDS based on the deep learning architecture to protect the CAN bus vehicles. The authors conduct experiments using the CAN-intrusion-dataset and train the VGG architecture for the network attack patterns to detect attacks.

We are thankful to the authors for their excellent contributions to this Special Section. We would like to deliver our appreciation to all the reviewers for dedicating their efforts in reviewing the articles, and for their valuable comments and suggestions that significantly improve the quality of the articles. Also, we would like to express our sincere gratitude to the earlier Editor-in-Chief, Prof. Saraju P. Mohanty, and the present Editor-in-Chief, Associate Professor Norbert Herencsar, for providing this opportunity and their important guidance throughout the process. We hope that this Special Section will serve as a good reference for the researchers and scientists from academia and industry in the field of STP for the IIoVT.

Uttam Ghosh is an associate professor with the Computer Science and Data Science, School of Applied Computational Sciences, Meharry Medical College, Nashville, TN, USA. Ghosh received his Ph.D. degree in electronics and electrical communication engineering from the Indian Institute of Technology Kharagpur. Contact him at ghosh.uttam@ieee.org.

Hellen Maziku is an assistant professor with the Department of Computer Science and Engineering, College of Information and Communication Technologies, University of Dar Es Salaam, Dar Es Salaam, Tanzania. Maziku received her Ph.D. degree in electrical and computer engineering from Tennessee State University, Nashville, TN, USA. Contact her at maziku.hellen@udsm.ac.tz.

Hari Prabhat Gupta is an associate professor with the Department of Computer Science and Engineering, Indian Institute of Technology BHU, Varanasi, India. Gupta received his Ph.D. degree in computer science and engineering from the Indian Institute of Technology Guwahati. Contact him at hariprabhat.cse@iitbhu.ac.in.

Biplab Sikdar is an associate professor with the Department of Electrical and Computer Engineering, National University of Singapore, Singapore. Sikdar received his Ph.D. degree in electrical engineering from Rensselaer Polytechnic Institute, Troy, NY, USA. Contact him at elebisik@nus.edu.sg.

Joel J. P. C. Rodrigues is a professor with the College of Computer Science and Technology, China University of Petroleum (East China), Qingdao, China, and also a senior researcher with Instituto de Telecomunicações, Aveiro, Portugal. Rodrigues received his Ph.D. degree in computer science and engineering from the University of Beira Interior (UBI), Covilhã, Portugal. Contact him at joeljr@ieee.org.