Guest Editors' Introduction

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

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 have given birth to several new groundbreaking applications, such as the Internet of Vehicles (IoV), smart cities, and cyber-physical systems. In the Internet of Vehicles, 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 compliment onboard sensor inputs and provide better services. A key concern when relying on vehicle data is vulnerable 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 Vehicular Things. An Intelligent Internet of Vehicle Things gives the desired results in the given time constraints with less human effort.

Digital Object Identifier 10.1109/MCE.2022.3207333
Date of current version 6 October 2022.

The increasing number of Internet of Vehicle Things (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.

In "Privacy-Preserving Deep Reinforcement Learning in Vehicle Ad Hoc Networks," U. Ahmed, et al. propose a deep-reinforcement learning method to sensitize the private information for a given vehicle connected over vehicle ad hoc networks, maintaining a balance between security and privacy through any sanitization process. Furthermore, the authors provide a set of recommendations and potential applications for the vehicle ad hoc networks as use cases.

In "Security, Trust, and Privacy for the Internet of Vehicles: A Deep Learning Approach," G. Muhammad and M. Alhussein, propose a deep learning model to process the data generated by the IoVT. In addition, this article addresses several STP issues in an intelligent transportation system.

Continuing the theme of preserving security and privacy in an intelligent transportation system (ITS) is M. Abdel-Basset et al.'s article titled

Published by the IEEE Consumer Technology Society

"Toward Privacy Preserving Federated Learning in Internet of Vehicular Things: Challenges and Future Directions." This article studies to figure out the potential of the federated learning (FL) approach in developing efficient decentralized solutions that consider the security and privacy concerns of the IoVT system. Furthermore, the authors introduce a federated graph convolutional recurrent network to learn spatial-temporal information for traffic flow forecasting.

The article titled "Secure, Privacy Preserving and Verifiable Federating Learning Using Blockchain for Internet of Vehicles," by B. Ghimire and D. B. Rawat, presents a practical prospect of blockchain empowered FL to realize fully secure, privacy preserving, and verifiable FL for the IoV that is capable of providing secure and trustworthy ITS services.

In "BIIoVT: Blockchain-Based Secure Storage Architecture for Intelligent Internet of Vehicular Things," S. K. Singh et al. propose a blockchain-based secure storage architecture for IIVoT to mitigate the issues related to security and privacy. The authors validate the results of their proposed architecture and show an outstanding balance of secure storage and efficiency for the IoVT compared to the similar existing methods.

The article titled "Intrusion Detection System Based Security Mechanism for Vehicular Ad-Hoc Networks for Industrial IoT," by S. Singh et al., presents a study on various challenges and problems associated with intrusion detection system (IDS) usage in VANETs. The authors also present a novel proposal on the use of a honeypot along with the existing IDS for VANETs to enhance the detection capabilities of IDS such that they can detect both the existing as well as zero-day based unknown attacks.

We close this Special Section with the article titled "On the Role of Futuristic Technologies in Securing UAV-Supported Autonomous Vehicles," by M. Aloqaily et al., focuses on the role of futuristic technologies in securing unmanned aerial vehicles (UAV) and autonomous vehicle (AV) technologies. Specifically, the authors discuss the role of blockchain and AI in providing security to the integrated UAV-AV.

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 to 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, Assoc. Prof. 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 research works and scientists from academia and industry in the field of STP for Intelligent Internet of Vehicular Things.

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

Hellen Maziku is currently 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. She received the 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 currently an Associate Professor with the Department of Computer Science and Engineering, Indian Institute of Technology BHU, India. Contact him at hariprabhat.cse@iitbhu.ac.in.

Biplab Sikdar is currently an Associate Professor with the Department of Electrical and Computer Engineering, National University of Singapore, Singapore. He received the Ph.D. degree in computer science and engineering from the Indian Institute of Technology Guwahati, Guwahati, India. Contact him at elebisik@nus.edu.sg.

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