
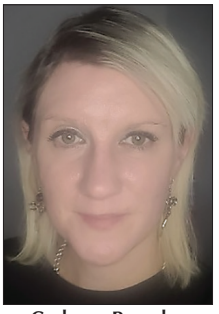

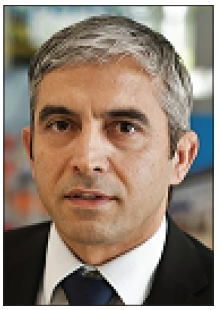


Ayoub Khan Cathryn Peoples Yingshu Li Mehrdad Dianati Anna Maria Vegni

Privacy, Trust and Reputation Management in Internet of Vehicles (IoV)

The emergence of the Internet of vehicles (IoV) in recent years holds great potential for enhancing the user experience by introducing more sophisticated services that do everything from guaranteeing the user's safety to enhancing their comfort. Vehicles, people, and roadside infrastructure all play important roles in building IoV ecosystem. In addition, a wide variety of communication methods coexist to guarantee the IoV's connectivity and stability. This multiplies the attack surface of the ecosystem and introduces new privacy, trust, and reputation concerns as a direct result of its variety. Due to the widespread nature of the IoV, it is imperative that services be privy to and able to incorporate concerns over user privacy. To protect passengers, drivers, and pedestrians from the dangers of insider attacks—in which communications from authorized users are tampered with or manufactured by malevolent organizations. Multiple variables are utilized to define peer-to-peer exchanges, and this information is then used to make a well-informed decision about whether or not to trust the vehicle in question. One typical method of indicating how much certain characteristics matter is to use a weighting factor. The quantities of the weighting factors are often set manually because there are no influencing variables taken into consideration when doing so. In accordance with this computed criterion, the peer vehicles are then categorized as either trustworthy or not. The use of adversary models in conjunction with trust management models to counter different kinds of insider attacks has been the subject of study. Adversary models help in identifying potential attackers, while trust management models help in determining the level of access and privileges that an individual should have based on their trustworthiness. The combination of these two models can improve the security of a system against insider attacks. This Special Issue (SI) is an effort to tackle some of these issues. The SI includes contributions from experts in the field and aims to provide insights and solutions to the challenges faced in the area of privacy, trust and reputation in IoV. It also highlights potential solutions and areas for future research.

The success of this SI is a testament to the collaborative efforts of the guest editors, the Editor-in-Chief, and managing editors of IEEE IoT Magazine, in promoting research and innovation in the field of IoV. Their dedication and hard work have paved the way for future advancements in this exciting area of technology.

We have received a large number of submissions, out of which 5 were selected through a rigorous review process. The editors are grateful to all authors for submitting such high-quality manuscripts as well as to the reviewers for their great support. The selected manuscripts cover a wide range of topics and are expected to make significant contributions to their respective fields. We look forward to encourage all authors to continue submitting their work for consideration.

The first article, titled "On-Demand Security Framework for 5GB Vehicular Networks" authored by Abdelwahab Boualouache *et al.*, have discussed that the successful collaboration between Vehicle-to-everything(V2X) nodes will ensure the development of robust machine learning models that can detect and prevent attacks in 5GB vehicular networks. This will ultimately enhance the security and safety of future smart transportation systems. However, while operating collaboratively, ensuring the machine learning model's security and data privacy is challenging. To address this challenge, future research could focus on developing more robust and secure machine learning algorithms and frameworks that can guarantee data privacy and security while maintaining high levels of accuracy. Additionally, collaborations between experts in machine learning, cybersecurity, and data privacy could help to identify potential vulnerabilities and develop effective mitigation strategies. The proposed framework enables federated learning workers to train machine learning models collaboratively without sharing their raw data, which ensures privacy preservation. Additionally, the use of blockchain and smart contracts provide a secure and transparent mechanism for managing interactions between the federated learning servers and workers. The framework enhances the accuracy by 14 percent and decreases the consensus time, at least by 50 percent, compared to related works.

The second article, titled "Toward Green and Secure Communication in IoT-Enabled Maritime Transportation System" authored by Sandeep Verma *et al.*, presents a secure communication mode for maritime transportation systems (MTS). IoT has enabled the development of smart shipping, which has improved efficiency, safety, and sustainability in the maritime industry. With the integration of IoT in MTS, there is a potential for further optimization and automation of processes. Therefore, it is crucial to implement strong security measures in MTS such as encryption, authentication, and access control to protect the devices and the data they transmit. Additionally, regular updates and patches should be applied to address any vulnerabilities that may arise.

Extensive experiments of the proposed approach show that mode outperforms the state-of-the-art methods using a variety of performance measures as a benchmark. The model conserves the energy of IoT devices employed for MTS and it also ensures

the secure communication among them. This is achieved through the implementation of advanced algorithms that optimize the energy consumption of IoT devices while maintaining a high level of security in data transmission. Additionally, the model can be easily integrated into existing MTS systems, making it a practical solution for energy-efficient and secure communication.

The third article, titled "Lightweight Reputation Management for Multi-Role Internet of Vehicles" authored by Chaogang Tang *et al.*, presents that information-centric IoV, smart vehicles can collect and share real-time traffic information, while in the task-oriented IoV, they can perform tasks such as autonomous driving and intelligent transportation. This technology has the potential to revolutionize the way we think about transportation and mobility. However, malicious vehicles may undermine the trustworthiness of vehicles towards each other, and further damage these IoV networks. This highlights the importance of implementing robust security measures to prevent such attacks and ensure the safety of passengers and other road users. It also emphasizes the need for continuous monitoring and updating of these security measures to stay ahead of potential threats. Given the multiple roles undertaken by vehicles in IoV networks, authors aim to design a lightweight reputation-based mechanism for a hybrid IoV network in this article. This mechanism can realize real-time reputation updates and synchronization in the device edge-cloud continuum. The proposed mechanism can effectively enhance the security and reliability of the IoV network by identifying and isolating malicious nodes. Additionally, it can also improve the overall performance of the network by reducing communication overhead and latency.

The fourth article, titled "A Framework for Decentralised, Real-time Reputation Aggregation in IoV," authored by Haitham Mahmoud *et al.*, have expressed concern about the potential road accidents and collisions caused by malicious vehicles. Authors have argued that a reputation system can help to mitigate these concerns and allow users to have safe journeys by providing a way to identify and estimate the behaviour of individual vehicles and to take appropriate actions in case of any malicious behaviour. Reputation systems have been successfully implemented in various online platforms, such as e-commerce websites and social media networks, to foster trust among users. By leveraging similar mechanisms in the context of ride-sharing services, users can make informed decisions and feel more secure during their journeys. In this article, the authors propose a blockchain-based reputation system that protects participant's privacy while also providing secure and resilient reputation computation. The reputation value, which reflects the overall trustworthiness of vehicles, is determined using decentralized feedback from the vehicles. Authors have analyzed the security and privacy of the proposed system and provided computation and communication performance.

The fifth article, titled "Deep learning-based Network Intrusion Detection System for Internet of Medical Things," authored by Vinayakumar Ravi have presented a deep learning-based approach for network-based intrusion detection in the internet of medical things (IoMT) systems using features of network flows and patient biometrics. The proposed method efficiently learns the best feature representation by feeding data on network flows and patient biometrics to several hidden layers. For optimal feature extraction from deep learning's spatial and temporal properties, the network has a global attention layer. On the IoMT intrusion dataset, the proposed method showed a 3.9 percent increase in accuracy over the state-of-the-art approaches. The suggested model may be implemented as a network monitoring tool for IoMT to protect these systems against intrusion inside the healthcare and medical setting.

Finally, we would like to thank the authors, reviewers, managing editors, and the EiC for helping the Guest Editors to organize this timely SI. We hope that this work will encourage and motivate researchers from academic and industry to develop further novel ideas and algorithms to advance IoV systems.

We look forward to seeing the impact of the research presented in this special issue on the future of IoV.

Biographies

Ayoub Khan [SM] (ayoub.khan@ieee.org) is working as a Research Professor at the University of Bisha, Saudi Arabia. He is a passionate researcher and learner. His 14 years of experience have worn many hats: Scientist, Project Manager, Professor, and Vice President. He brings punctual compliance with the best quality standards of academic credentials to the work in the area of Blockchain, Intelligent transportation, Data Sciences, IoT, Cloud Computing, and Industrial Informatics. He received a Master's degree in Computer Science and Ph.D. in Computer and Electrical Engineering. He is contributing to the research community through various volunteer activities as an editor, reviewer, and chair. He has edited more than 10 journal special issues, and 20 books, and has a large number of publications in high-impact journals in the area of IoT, smart cities a blockchain. He is a senior member of the professional bodies of the ACM, ISTE, and EURASIP societies.

Cathryn Peoples (cathryn.j.peoples@ieee.org) received a B.A. degree in business studies with computing, an M.Sc. degree in telecommunications and internet systems, and a Ph.D. degree in networking from Ulster University, U.K., in 2004, 2005, and 2009, respectively. She is currently employed as a Research Associate at Ulster University working on Service Level Agreements for the Internet of Things. Cathryn is also employed by The Open University in the School of Computing and Communications within the Faculty of Science, Technology, Engineering & Mathematics as an Associate Lecturer in Software Engineering. She became a member of IEEE in 2008, and an Editor-in-Chief of the *EAI Endorsed Transactions on Cloud Systems* in January 2020. Her research interests include cloud management, cross-layer protocol optimization, delay-tolerant networking, smart cities, and green IT.

Yingshu Li (yili@gsu.edu) received her Ph.D. and M.S. degrees from the Department of Computer Science and Engineering at the University of Minnesota-Twin Cities. She received her BS degree from the Department of Computer Science and Engineering at the Beijing Institute of Technology, China. She is currently a Professor in the Department of Computer Science at Georgia State University. Her research interests include Privacy-aware Computing, the Internet of Things, Social Networks, and Wireless Networking. She is the recipient of an NSF CAREER Award. Her research has been supported by the National Science Foundation, the U.S. Department of State, and some other academic and industrial sponsors. She regularly publishes in scholarly journals, conference proceedings, and books, and her publications have received around 10,000 citations. She has been serving as an associate/guest editor for many prestigious journals including *ACM Transactions on Sensor Networks*, *IEEE Transactions on Computers*, *IEEE Transactions on Network Science and Engineering*, *IEEE Internet of Things Journal*, etc. She has also been serving as a General/Program Chair and TPC member for many international conferences such as CIKM, ICDCS, INFOCOM, IPCCC, WASA, etc.

Mehrdad Dianati (m.dianati@warwick.ac.uk) is the Director of Intelligent Vehicles Research and technical research lead in the area of Networked Intelligent Systems at the Warwick Manufacturing Group (WMG). He has over 29 years of combined industrial and academic experience, with 20 years in various leadership roles in multi-disciplinary collaborative R&D projects. Mehrdad works with the Automotive and ICT industries as the primary application domains of my research. He is also Co-Director of Warwick's Centre for Doctoral Training on Future Mobility Technologies, training doctoral researchers in the areas of intelligent and electrified mobility systems in collaboration with the experts in the field of electrification from the Department of Engineering of the University of Warwick. Currently, Mehrdad is the Field Chief Editor of *Frontiers in Future Transportation*.

Anna Maria Vegni [SM] (annamaria.vegni@uniroma3.it) is a tenure-track Assistant Professor in the Department of Engineering at Roma Tre University (Rome, Italy), since March 2020. She received a Ph.D. degree in Biomedical Engineering, Electromagnetics, and Telecommunications from the Department of Applied Electronics, Roma Tre University, in March 2010. She received the 1st and 2nd level Laurea Degree cum laude in Electronics Engineering at Roma Tre University, in July 2004, and 2006, respectively. In 2009, she was a visiting researcher in the Multimedia Communication Laboratory, directed by Prof. Thomas D.C. Little, at the Department of Electrical and Computer Engineering, Boston University, Boston, MA. Her research activity focused on vehicular networking supported by heterogeneous wireless networks. She is a member of the ACM. In June 2021, she got the Italian Habilitation (Abilitazione Scientifica Nazionale) for Full Professorship in Telecommunication Engineering. She is involved in the organization of several IEEE and ACM international conferences and is a member of the editorial board of *IEEE Communications Magazine*, *Ad Hoc Networks*, *Journal of Networks and Computer Applications*, *Nanocomnet Elsevier journals*, *WINET Springer*, *IEEE JCN*, *ITU J-FET*, and *ETT Wiley journal*.