Security and Privacy of Connected Vehicular Cloud Computing


Hongwei Li


Rongxing Lu


Jelena Misic


Mohamed Mahmoud

As a special cloud computing platform, connected vehicular cloud computing (CVCC), which seamlessly combines cloud computing and VANETs, has been recently proposed to accelerate the adoption of VANETs, and extends the traditional cloud infrastructure consisting of a majority of stationary nodes to the edge of vehicles. CVCC is a mobile computing paradigm that consists of in-motion vehicles cooperating with each other to achieve a bunch of practical applications, such as collaborative package delivery and information dissemination. Essentially, CVCC coordinates the computing, communication, sensing, and storage resources of vehicles on the road to balance the service requirements and hardware limitations. Because of these advantages, CVCC has been regarded as a key basis of future competition and innovation, and has attracted considerable attention from both industry and academia in recent years.

Nevertheless, different from the traditional cloud infrastructure, CVCC requires sophisticated security and privacy protection mechanisms as legitimate users and attackers have the same privileges in CVCC. Thus, attackers can utilize system loopholes to reach their goals, such as obtaining confidential information and tampering with the integrity of information and the availability of resources. Therefore, in order to enhance the security and scalability of CVCC, a set of security and privacy requirements such as authentication, nonrepudiation, anonymity, and traceability should be met in accordance with the expected characteristics of CVCC, and a number of crucial issues such as trust model, data security, connection fault, and query tracking attacks must be addressed. Although traditional security mechanisms are plentiful today, they are inadequate to solve the emerging security challenges in CVCC, as they are tailored to securing the conventional cloud paradigm or vehicular ad hoc networks (VANETs).

The response to our Call for Papers for this Special Issue was overwhelming, with 34 papers submitted from around the world. During the review process, each paper was assigned to and reviewed by multiple experts in the relevant areas, with a rigorous two-round review process. Thanks to the courtesy of the Editor-in-Chief of *IEEE Network*, Prof. Nei Kato, we were able to accept 12 excellent articles covering various aspects of security and privacy challenges of CVCC. In the following, let us introduce these articles and highlight their main contributions.

In "Fog-Aided Verifiable Privacy Preserving Access Control for Latency-Sensitive Data Sharing in Vehicular Cloud Computing," the authors propose a novel fog-to-cloud base architecture for data sharing in VCC. The scheme is a cryptography-based mechanism that conducts fine-grained access control. In their design, the complicated computation burden is securely outsourced to fog and cloud servers with confidentiality and privacy preservation. Meanwhile, with prediction of vehicles' mobility, pre-pushing data to specific fog servers can further reduce the response latency with no need to consume more resources of fog servers. In addition, with the assumption of no collusion between different providers of the cloud and fog servers, the proposed scheme can provide verifiable auditing of fog servers' reports. The scheme is provably secure against the existing adversaries and newborn security threats. Experiments show significant performance improvement in edge devices' cost overhead and response time.

Channel capacity, as the key parameter to measure channel utilization, plays an important role in ensuring the reliability of CVCC service and the integrity of transmission data. In past decades, the existing calculation methods could not solve the channel capacity problem in multi-participant VANETs. Different from the traditional calculation methods, in "A Secure and Efficient Transmission Method in Connected Vehicular Cloud Computing," the authors propose a novel calculation method by combining the core concepts of game theory and information theory. The proposed method can calculate the channel capacities of multiple vehicular networks efficiently, and has many potential applications in different services of CVCC.

CVCC can be applied in various scenarios, particularly in vehicular crowdsensing, as it can make full use of sensing, computing, and storage resources of the vehicles. However, malicious vehicles may impede its proliferation by providing untruthful data to affect the accuracy of sensing results. In "RTSense: Providing Reliable Trust-Based Crowdsensing Services in CVCC," the authors study how to provide reliable trust-based crowdsensing services in CVCC, called RTSense. First, they present the architecture of RTSense. After that, they focus on how to capture security and privacy in RTSense, and propose possible solutions including anonymous vehicle authentication, and interactive filtering truth discovery and trust management to achieve security assur-

ance and provide reliable crowdsensing services. Finally, they identify interesting future directions along with convincing solution ideas.

In "Integrated Authentication and Key Agreement Framework for Vehicular Cloud Computing," the authors try to identify the security goals for the interoperability with VCC and provide an authentication and key agreement (AKA) framework for VCC. Specifically, the authors first present the research challenges and open problems for designing a reliable AKA with strong security guarantees for VCC. Then the authors propose an integrated AKA framework that integrates single-server 3-factor AKA protocol and non-interactive identity-based key establishment protocol. Finally, the authors prove the utility of the proposed scheme by conducting experiments on a simulated experimental platform.

In "Secure Outsourcing Computing in Connected Vehicular Cloud Computing," the authors aim to exploit new challenges of outsourcing computing in CVCC. Since pairing-based cryptographic primitives are of particular interest among the cryptographic tools used in CVCC, they devote their attention toward the security challenges and efficiency requirements of outsourcing pairing from vehicles to vehicles in CVCC. Furthermore, they give a pairing outsourcing protocol for illustration, which indicates that secure and effective pairing outsourcing in CVCC is possible. Furthermore, they also identify some future research directions in secure CVCC.

In "UAV-Empowered Edge Computing Environment for Cyber-Threat Detection in Smart Vehicles," the authors propose a data-driven transportation optimization model where cyber-threat detection in smart vehicles is done using a probabilistic data structure (PDS)-based approach. Based on triple Bloom filter and PDS, a new scheduling technique for load balancing is initially used to host the real-time data coming from different vehicles, and to distribute/collect the data to/from edges in a manner that minimizes the computational effort. The results obtained show that the proposed system requires comparatively less computational time and storage for load sharing, authentication, encryption, and decryption of data in the considered edge-computing-based smart transportation framework.

In "Secure and Efficient Privacy-Preserving Ciphertext Retrieval in Connected Vehicular Cloud Computing," the authors propose a ciphertext-based search system that exploits roadside units as super peers for CVCC. The proposed system supports ciphertext retrieval for related documents. In the proposed system, all computations and retrieval operations are handled by super stationary peers while the document is stored in the cloud to achieve high efficiency and security of the index structure. The proposed scheme can also reduce the impact of vehicle dynamics on the information retrieval process. The indexing efficiency in the system is also improved by utilizing a hybrid indexing structure in which binary trees are nested in a B+ tree. Through security analysis and performance evaluation, it is shown that the proposal can achieve acceptable security and efficiency.

Despite numerous benefits of connected vehicles, the technological developments have also created serious safety/security concerns. In "Connected Vehicles' Security from the Perspective of In-Vehicle Network," the authors recapitulate the diversified attack surfaces of connected vehicles related to the technological developments from the perspective of the in-vehicle network. For each of the attacks, the authors discuss the rationale and the concrete methods presented in the literature. In particular, they illustrate how to launch successful attacks through a controlled area network bus, electronic control units, and an in-vehicle infotainment system. The article also suggests some feasible solutions to the attacks demonstrated by the community. Considering the fact that vehicles are safety-critical, more practical and effective steps should be taken within the connected vehicle network toward securing the connected vehicles and protecting drivers and passengers.

High-speed rail (HSR), an increasingly efficient means of transportation, faces several challenges in terms of high-frequency handover at speeds over 300 km/h. This includes large volumes of data of different types and different degrees of importance. In "SVCC-HSR: Providing Secure Vehicular Cloud Computing for Intelligent High-Speed Rail," the authors propose a novel and practical secure vehicular cloud computing system for HSR (SVCC-HSR), based on the long-term research and practice in this field. SVCC-HSR not only considers the various technical features of vehicular cloud computing, but also addresses several special demands in the HSR context. The authors perform extensive experiments using various scenarios, including frequent handover scenarios in high-speed trains running at 300 km/h with large-volume data transmission scenarios in locomotive depots. The real-world experimental results demonstrate that SVCC-HSR achieves better performance on fast authentication, hierarchical attribute-based data encryption, and transmission.

In "Collaborative Security in Vehicular Cloud Computing: A Game Theoretic View," the authors first present a CVCC architecture and its applications. Then they study several security issues in vehicular cloud computing. Afterward, they model a CVCC network by a two-phase heterogeneous public good game (HPGG), and then investigate the influence of different incentive mechanisms and the structure of a complex network describing the vehicles' connectivity and the vehicles' investment rate. Finally, the authors come to a conclusion.

Electric vehicles cloud and edge (EVCE) computing is an attractive network paradigm involving seamless connections among heterogeneous vehicular contexts. It will be a trend along with electric vehicles (EVs) becoming popular in vehicle-to-everything (V2X). The EVs act as potential resource infrastructures referring to both information and energy interactions, and there are serious security challenges for such hybrid cloud and edge computing. In "Blockchain-Enabled Security in Electric Vehicles Cloud and Edge Computing," the context-aware vehicular applications are identified according to the perspectives of information and energy interactions. Blockchain-inspired data coins and energy coins are proposed based on distributed consensus, in which data contribution frequency and energy contribution amount are applied to achieve the proof of work. Security solutions are presented for securing vehicular interactions in the EVCE computing.

Last but not least, in "Secrecy-Driven Resource Management for Vehicular Computation-Offloading Networks," the authors focus on the eavesdropping attack when vehicular users (VUs) deliver computation tasks to cloud/edge servers over RF channel. They take the tool of physical layer security and investigate the resource management for secrecy provisioning when the VUs offload computation tasks. They

then discuss three promising technologies, non-orthogonal multiple access, multi-access-assisted computation-offloading, and mobility- and delay-aware offloading, which facilitate the enhancement of secrecy against the eavesdropping attack. Finally, as a detailed example of multi-access-assisted computation offloading, the authors present a case study on the optimal dual-connectivity-assisted computation task offloading with secrecy provisioning and show the performance of the proposed computation offloading.

Finally, we would like to express our thanks to all the authors for their support and excellent contributions. We also would like to thank all the reviewers for their volunteered efforts in reviewing the papers, and for their insightful comments and constructive suggestions for improving the quality of the articles. Respectfully, we appreciate the advice and support of the Editor-in-Chief of *IEEE Network*, Prof. Nei Kato, for his help in the whole publication process.

Biographies

Hongwei Li [M] is currently the head of and a professor in the Department of Information Security, School of Computer Science and Engineering, University of Electronic Science and Technology of China. He received his Ph.D. degree in computer software and theory from the same university in 2008. He worked as a postdoctoral fellow in Department of Electrical and Computer Engineering at the University of Waterloo for one year. His research interests include network security, applied cryptography, and trusted computing. His research is supported by the National Science Foundation of China, the Ministry of Science and Technology of China, the Ministry of Industry and Information Technology, and China Unicom. He serves as an Associate Editor of *Peer-to-Peer Networking and Applications*, and a Guest Editor for the *IEEE Internet of Things Journal* Special Issue on Big Security Challenges in Big Data Era. He also serves on the Technical Program Committees for many international conferences, such as IEEE INFOCOM, IEEE ICC, IEEE GLOBECOM, IEEE WCNC, IEEE SmartGridComm, BODYNETS, and IEEE DASC. He is a member of China Computer Federation and the China Association for Cryptologic Research.

Rongxing Lu [SM] has been an assistant professor at the Faculty of Computer Science, University of New Brunswick, Canada, since August 2016. Before that, he worked as an assistant professor at the School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore, from April 2013 to August 2016. He worked as a postdoctoral fellow at the University of Waterloo from May 2012 to April 2013. He was awarded the prestigious Governor General's Gold Medal when he received his Ph.D. degree from the Department of Electrical and Computer Engineering, University of Waterloo in 2012, and won the 8th IEEE Communications Society Asia Pacific Outstanding Young Researcher Award in 2013. His research interests include applied cryptography, privacy enhancing technologies, and IoT-big data security and privacy. He currently serves as the Vce-Chair (Publication) of the IEEE ComSoc Communications and Information Security Technical Committee.

Jelena Misic [F] is a professor of computer science at Ryerson University in Toronto, Ontario, Canada. She has published over 100 papers in archival journals and more than 160 papers at international conferences in the areas of wireless networks and security and privacy, in particular wireless personal area network and wireless sensor network protocols, performance evaluation, and security. She serves on the Editorial Boards of *IEEE Network*, *IEEE Transactions on Vehicular Technology*, *Computer Networks*, *Ad Hoc Networks*, *Security and Communication Networks*, *the International Journal of Sensor Networks*, and the *International Journal of Telemedicine and Applications*. She is a member of ACM.

Mohamed Mahmoud received his Ph.D. degree from the University of Waterloo in April 2011. Then he worked as a postdoctoral fellow at the University of Waterloo and Ryerson University. Currently, he is an assistant professor in the Department Electrical and Computer Engineering, Tennessee Tech University. His research interests include security and privacy preservation in smart grid, vehicular ad hoc networks, sensor networks, and others. He has received the NSERC-PDF and MITACS-PDF (two Canadian national awards). He won the Best Paper Award from IEEE ICC '09 and IEEE WCNC '16.