Editorial

Distributed Secure Computing for Smart Mobile IoT Networks

Vishal Sharma, Daniel G. Reina, Zengpeng Li, Kathiravan Srinivasan, Navuday Sharma, and Vinod Karar

1Queen’s University Belfast, Belfast, NI BT7 1NN, UK
2University of Seville, Seville 41004, Spain
3School of Cyber Science and Technology, Shandong University, Qingdao 266237, China
4Vellore Institute of Technology, Vellore 632014, India
5Ericsson, Tallinn 11415, Estonia
6Central Scientific Instruments Organisation, Chandigarh 160030, India

Correspondence should be addressed to Vishal Sharma; vishal_sharma2012@hotmail.com

Received 22 February 2022; Accepted 22 February 2022; Published 15 April 2022

With billions of devices operations as a part of the Internet of Things (IoT), the operational complexity of the networks increases to many folds. In terms of threat detection, it requires moving from a centralised detection model to decentralised and distributed formations. Distributed computing facilitates better services; however, it has multiple ownership issues, requiring better system management [1]. With distributed systems, security needs to be revisited to make them afloat from cyber threats with new solutions, like sound and data steganography for authentication [2], preventing stealthy adversaries [3], access control [4], or network anomaly detection [5]. New and advanced solutions are required to solve the computationally intensive problems with better offloading in distributed setup targeting smart mobile IoT. Another prominent issue in distributed IoT networks is the data-islands dilemma [6], which requires intelligent and secure mechanisms to handle data integrity and privacy. Different solutions can be adapted like the use of distributed ledger technologies, such as blockchain [7], to take authorisation and access control of many portable devices without letting the system fall short of decentralised attacks; Iota Tangle [8] can be used mainly for securing IoT environment, or gossip protocol-based Hashgraph [9] can be used for increased fairness and better security constraints without using block-based architecture. Understanding smart devices privacy, trust, and security with better authentication protocols is another side to explore [10]. Several key issues need to be addressed by covering the gap in the literature, which must help answer concerns related to achieving password-based authentication, keeping data privacy, outsourcing security, and intelligent security solutions using machine learning.

In this special issue (SI), a total of ten articles were selected following a rigorous review process where the articles were handled without any competing conflict of interest. The articles in this SI cover a wide range of security and privacy issues in distributed computing related to IoT, blockchain, resource manipulation, industrial control systems, credit cards, smart homes, and aerial networks. Some of the highlights include the following: In [11], the authors proposed an A² chain that uses an edge computing setup to decentralise the services. This article relies on the usage of sidechain technologies to securely share the identity verification of IoT devices. The authors used the proposed blockchain setup to authenticate the 5G-enabled IoT devices. Overall, this approach reduces the authentication time and communication cost whereby consuming less storage space. In [12], the authors focused their work on user authorisation, where the primary task was to detect credit card frauds from imbalanced data logs. The authors relied on the machine learning models and suggested that RUSBoost be a more appropriate model when imbalanced records need to be evaluated for fraud detection. The authors used datasets to show the efficacy of their proposed solution. Their results showed a possibility of high precision between 94.20 and 99.30 for three different credit card datasets.
In the direction of distributed security, rogue devices can be much harmful in any setup. These devices can be silent attackers that use the system’s weak defence to launch attacks. The authors considered this area of research in [13], where they proposed a blockchain-based access control for mitigating rogue devices in IoT. The authors aimed at removing the centralised mode of detection by replacing architecture with the blockchain, which offers secure device registration using smart contracts. The access control mechanism prohibits unregistered devices, and the approach is evaluated using a case study and in-depth performance evaluations. Furthermore, in [14], the authors focused on secure deployment in flying ad hoc networks using identity-based generalised signcryption. Their proposed work used Mobile Edge Computing (MEC), where UAVs act as a MEC node with the role of offloading in the network. The proposed security scheme is based on a hyperelliptic curve. The authors formally verified their proposed security scheme using the AVISPA tool and compared it with five relevant security schemes against security functionalities.

Through its collection of diverse articles on distributed security, we believe that this special issue will benefit the research community.

Conflicts of Interest
The guest editors declare that they have no conflicts of interest regarding the publication of this special issue.

Vishal Sharma  
Daniel G. Reina  
Zengpeng Li  
Kathiravan Srinivasan  
Navuday Sharma  
Vinod Karar

Acknowledgments
The guest editors appreciate the high-quality submissions from the authors and the timely support of reviewers.

References