Security and Communication Networks

Special Issue on
Intrusion Detection and Prevention in Cloud, Fog, and Internet of Things

WILEY | Hindawi

CALL FOR PAPERS

Internet of Things (IoT), cloud, and fog computing paradigms are as a whole provision a powerful large-scale computing infrastructure for many data and computation intensive applications. Specifically, the IoT technologies and deployment can widely perceive our physical world at a fine granularity and generate sensing data for further insight extraction. The fog computing facilities can provide computing power near the IoT devices where data are generated, aiming to achieve fast data processing for time critical applications or save the amount of data transmitted into cloud for storage or further processing. The cloud computing platforms can offer big data storage and large-scale processing services for cheap long-term storage or data intensive analytics with more advanced data mining models. Hence, it can be seen that the IoT/fog/cloud computing infrastructures can support the whole lifecycle of large-scale applications where big data collection, transmission, storage, processing, and mining can be seamlessly integrated. However, these state-of-the-art computing infrastructures still suffer from severe security and privacy threats because of their built-in properties such as the ubiquitous-access and multitenancy features of cloud computing, or the limited computing capability of IoT devices. The expanded attack surface and the lack of effective security and privacy protection measures are still one of the barriers of widely deploying applications on the IoT/fog/cloud infrastructure.

Intrusion detection and prevention systems that monitor the devices, networks, and systems for malicious activities and policy violations are one of the key countermeasures against cybersecurity attacks. With a wide spectrum, the detection and prevention systems vary from antivirus software to hierarchical systems monitoring the traffic of an entire backbone networks. In general, intrusion detection systems can be categorized into two groups, that is, signature-based detection (malicious patterns are already known) and anomaly-based detection (no patterns are given). Traditional methods and systems might fail to be directly applicable to the state-of-the-art computing paradigms and infrastructure as mentioned above. Novel intrusion detection and prevention algorithms and systems are in demand to cater for the new computing infrastructure and newly emerging cybersecurity attacks and threats, with taking into account the factors such as algorithmic scalability, computing environment heterogeneity, and data diversity and complexity. Extensive research is required to conduct more scalable and effective intrusion detection and prevention in IoT/fog/cloud. Many relevant theoretical and technical issues have not been answered well yet. So, it is high time to investigate the related issues in intrusion detection and prevision in IoT, fog, and cloud computing by examining intrusion detection and prevision algorithms, methods, architecture, systems, platforms, and applications in detail, hence the call for this special issue.

Potential topics include but are not limited to the following:

- Theories and modeling for intrusion detection and prevention
- New challenges brought by IoT/fog/cloud to intrusion detection and prevention
- Intrusion detection and prevention system and architecture design
- IoT, fog, and/or cloud computing based intrusion detection and prevention systems
- Network based and host-based intrusion detection systems
- Signature based intrusion detection and prevention
- Anomaly analysis based intrusion detection and prevention
- Anomaly/outlier/emerging event detection theories and modeling
- Anomaly/outlier detection applications and systems in IoT, fog, and cloud computing
- Supervised and unsupervised learning for intrusion detection
- Computational intelligence for intrusion detection and prevention systems
- Light-weight and time-critical intrusion detection and prevention systems
- Distributed and scalable detection and prevention systems
- Privacy-preserving intrusion detection and prevention
- Cryptographical theories and techniques for intrusion detection and prevention
- Information hiding and encryption
- Security issues and challenges in cloud, edge, fog, and IoT

Authors can submit their manuscripts through the Manuscript Tracking System at https://mts.hindawi.com/submit/journals/scn/idp/.

Papers are published upon acceptance, regardless of the Special Issue publication date.

Lead Guest Editor
Xuyun Zhang, University of Auckland, Auckland, New Zealand
xuyun.zhang@auckland.ac.nz

Guest Editors
Yuan Yuan, Michigan State University, East Lansing, USA
yyuan@msu.edu

Zhili Zhou, University of Windsor, Windsor, Canada
zhou_zhili@163.com

Shancang Li, University of the West of England, Bristol, UK
shancang.li@uwe.ac.uk

Lianyong Qi, Qufu Normal University, Qufu, China
lianyongqi@gmail.com

Deepak Puthal, University of Technology Sydney, Sydney, Australia
deepak.puthal@uts.edu.au

Submission Deadline
Friday, 24 August 2018

Publication Date
January 2019