Security and Communication Networks

Special Issue on
Big Data Analytics for Cyber Security

CALL FOR PAPERS

The era of Internet of Things with billions of connected devices has created an ever larger surface for cyber attackers to exploit, which has resulted in the need for fast and accurate detection of those attacks. The developments in mobile computing, communications, and mass storage architectures in the past decade have brought about the phenomenon of big data, which involves unprecedented amounts of valuable data generated in various forms at a high speed. The ability to process these massive amounts of data in real time using big data analytics tools brings along many benefits that could be utilized in cyber threat analysis systems. By making use of big data collected from networks, computers, sensors, and cloud systems, cyber threat analysts and intrusion detection/prevention systems can discover useful information in real time. This information can help detect system vulnerabilities and attacks that are becoming prevalent and develop security solutions accordingly.

Big data analytics will be a must-have component of any effective cyber security solution due to the need of fast processing of the high-velocity, high-volume data from various sources to discover anomalies and/or attack patterns as fast as possible to limit the vulnerability of the systems and increase their resilience. Even though many big data analytics tools have been developed in the past few years, their usage in the field of cyber security warrants new approaches considering many aspects including (a) unified data representation, (b) zero-day attack detection, (c) data sharing across threat detection systems, (d) real time analysis, (e) sampling and dimensionality reduction, (f) resource-constrained data processing, and (g) time series analysis for anomaly detection.

This special issue solicits original contributions that utilize and build big data analytics solutions for cyber security. Novel, multidisciplinary solutions that target any area of cyber security, as well as generic, interoperable big data analytics architectures for cyber security are particularly encouraged.

Potential topics include but are not limited to the following:

- Big data analytics for intrusion detection in Internet of Things (IoT) systems
- Big data analytics for cloud systems security
- Malware detection using big data analytics
- Cyber threat intelligence using big data analytics
- Big data processing architectures for threat detection
- Dimensionality reduction and sampling techniques for valuable cyber security data extraction
- Advanced persistent threat (APT) detection techniques in big data analytics
- Machine learning algorithms for effective detection of cyber-attacks with big data analytics
- Representation of cyber-attack data for cross-platform processing
- Network forensics using big data analytics
- Stream data processing for real time threat analysis
- Zero-day attack detection using big data analytics

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

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

Lead Guest Editor
Pelin Angin, Middle East Technical University, Ankara, Turkey
pangin@ceng.metu.edu.tr

Guest Editors
Bharat Bhargava, Purdue University, West Lafayette, USA
bbshail@purdue.edu

Rohit Ranchal, IBM Watson Health Cloud, Armonk, USA
ranchal@us.ibm.com

Submission Deadline
Friday, 25 January 2019

Publication Date
June 2019