CALL FOR PAPERS

IEEE Transaction on Knowledge and Data Engineering (TKDE)

Special Issue on

Special Issue on Anomaly Detection in Emerging Data-Driven Applications

Motivation

With the rapid development of emerging technologies and applications, large amounts of data have been generated through different types of objects, such as texts, images, graphs, videos, etc. This scenario has led to a renewed attention in anomaly detection and security issues, which are indispensable in many fields like cybersecurity, fintech, healthcare, public security and AI safety. Recently, various studies propose to leverage the power of machine learning and data analysis for anomaly detection, which have shown some promising results. However, many challenging problems still remain unsolved due to the complex nature of data. This special issue on Anomaly Detection in Emerging Data-Driven Applications will solicit recent advances in anomaly detection that exploit the data structures, semantics, dynamics and heterogeneity to provide more reliable and efficient anomaly detection systems.

Scope of Interest

This special issue solicits original and high-quality papers that address emerging research challenges in anomaly detection. Potential topics include but are not limited to the following:

(i) Theory/foundation of anomaly detection, e.g.,
- Optimization and learnability
- Anomaly explanation
- Reasoning model

(ii) Supervision in anomaly detection, e.g.,
- Semi-supervised anomaly detection
- Unsupervised anomaly detection
- Supervised anomaly detection
- Ensemble model

(iii) Anomaly detection based on deep learning, e.g.,
- Representation learning based methods
- Sequence learning based methods
- Reinforcement learning based methods
- Transfer learning models based methods
- Generative models

(iv) Business problems, e.g.,
- Financial fraud
- Risk modeling
- Intrusion/malware detection in systems
- Early detection of emerging phenomena

Usage behavior anomaly detection
Fake news and rumor detection in social media
Power grid anomaly detection

(v) Others, e.g.,

Human-in-the-loop anomaly detection
Spatial-temporal data anomaly detection
Biological and chemical anomaly detection
Anomaly detection in computer vision
Adversarial attacks on anomaly detection
Adversarial robustness on anomaly detection
Adversarial samples detection
Anomaly detection in federated learning

(vi) Survey

Survey for anomaly detection

Submission Guidelines and Important Dates:

Submitting authors should follow the Style and Author Guidelines for regular TKDE papers available at https://www.computer.org/csdl/journal/tk/write-for-us/15073. Note that mandatory over-length page charges and color charges will apply. Manuscripts should be submitted electronically to Manuscript Central at https://mc.manuscriptcentral.com/tkde-cs.

Submission Deadline for Papers: April 30, 2021
Completion of 1st Round of Reviews: August 18, 2021
Minor Revisions Due: October 18, 2021
Completion of 2nd Round of Reviews: November 18, 2021
Editorial Decisions Sent: December 31, 2021
Planned Publication: Late 2022

Guest Editors

Jianxin Li, Beihang University, China, lijx@act.buaa.edu.cn.
Lifang He, Lehigh University, USA, lih319@lehigh.edu.
Hao Peng, Beihang University, China, penghao@buaa.edu.cn
Peng Cui, Tsinghua University, China, cuip@tsinghua.edu.cn
Charu C. Aggarwal, IBM Research, USA, charu@us.ibm.com
Philip S. Yu, University of Illinois at Chicago, USA, psyu@uic.edu