Guest Editorial Introduction to the Special Issue on Anomaly Detection in Emerging Data-Driven Applications: Theory, Algorithms, and Applications

WE ARE delighted to present this special issue on Anomaly Detection in Emerging Data-Driven Applications: Theory, Algorithms, and Applications. Anomaly detection plays an important part of knowledge and data engineering, such as cybersecurity, fintech, healthcare, public security and AI safety. However, large amounts of data have been generated through different types of objects, and it brings new challenges for anomaly detection research. The purpose of this special issue is to provide a forum for researchers and practitioners to present their latest research findings and engineering experiences in the theoretical foundations, empirical studies, and novel applications.

Zhang et al. in "CityNeuro: Towards Location and Time Prediction for Urban Abnormal Events" proposed a framework called CityNeuro that incorporates both environmental and historical influence for location and time prediction of urban abnormal events.

Wang et al. in "A2DJP: A Two Graph-based Component Fused Learning Framework for Urban Anomaly Distribution and Duration Joint-Prediction" proposed a novel Anomaly Distribution and Duration Joint-Prediction algorithm to simultaneously filtrate urban subregions.

Li et al. in "Adaptive Label Propagation for Group Anomaly Detection in Large-scale Networks" introduced a algorithm called Adaptive Label Propagation to solve the challenges of heterogeneous networks and overlapping groups in group anomaly detection in large-scale networks.

Deng et al. in "Markov-Driven Graph Convolutional Networksfor Social Spammer Detection" proposed an Adaptive Reward Markov Random Field layer and combined feature-based and propagation-based methods for spammer detection.

Borges et al. in "IoT Botnet Detection based on Anomalies of Multiscale Time Series Dynamics" proposed a solution for detecting botnet attacks in the Internet of Things by identifying anomalies in the temporal dynamics of devices.

Li et al. in "ECOD: Unsupervised Outlier Detection Using Empirical Cumulative Distribution Functions" presented the Empirical-Cumulative-distribution-based Outlier Detection algorithm to overcome challenges in outlier detection in large, high-dimensional datasets.

Kim et al. in "Active Learning for Human-in-the-Loop Customs Inspection" defined the problem of concept drifts in the context of customs fraud detection and proposed a novel hybrid sampling strategy based on active learning that combines exploration and exploitation strategies.

Ge et al. in "CollaborEM: A Self-supervised Entity Matching Framework Using Multi-features Collaboration" presented a self-supervised entity resolution framework via multi-features collaboration to obtain reliable EM results with zero human annotations and improve robustness.

Zhang et al. in "Adaptive Memory Networks with Self-supervised Learning for Unsupervised Anomaly Detection" proposed Adaptive Memory Network with Self-supervised Learning to enhance the generalization ability in unsupervised anomaly detection.

Gan et al in "Anomaly Rule Detection in Sequence Data" presented a new anomaly detection framework that enables Discovery of Utility-aware Outlier Sequential rules from a set of sequences.

Wang et al. in "Traffic Accident Risk Prediction via Multi-View Multi-Task Spatio-Temporal Networks" proposed a Multi-View Multi-Task Spatio-Temporal Networks model to forecast fine- and coarse-grained traffic accident risks of a city simultaneously.

Shangguan et al. in "Abnormal samples oversampling for anomaly detection based on uniform scale strategy and closed area" proposed a discrete synthetic minority oversampling technique to generate new samples, which handled the problem of the imbalance for the original dataset.

Jiao et al. in "Generative Evolutionary Anomaly Detection in Dynamic Networks" considered the challenge of modeling the correlation and driving mechanism between different abnormal behavior, and proposed a unified Generation model to analyze the dynamic network.

Asif et al. in "Identifying Anomalies while Preserving Privacy" related sensitive privacy to other important notions of data privacy to help port the technical developments and private mechanism constructions from these related concepts to sensitive privacy.

Wang et al. in "Concept Drift-based Runtime Reliability Anomaly Detection for Edge Services Adaptation" propose a concept drift-based runtime reliability anomaly detection approach for edge services adaptation.

Date of current version 8 November 2023.
Digital Object Identifier 10.1109/TKDE.2023.3301582

1041-4347 © 2023 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission.
See https://www.ieee.org/publications/rights/index.html for more information.

Choi et al. in "GAN-Based Anomaly Detection for Multivariate Time Series Using Polluted Training Set" proposed a novel GAN-based anomaly detection and localization framework along with a transformation method for multivariate timing anomaly detection.

Tong et al. in "Learning Discriminative Text Representation for Streaming Social Event Detection" proposed Text Similarity Contrastive Learning Neural Network to tackle the challenges of constantly changing context and unknown event categories.

Li et al. in "Discriminative Feature Mining Based on Frequency Information and Metric Learning for Face Forgery Detection" proposed a novel frequency-aware discriminative feature learning framework to learn more discriminative features with less optimization difficulty.

Zheng et al. in "Generative and Contrastive Self-Supervised Learning for Graph Anomaly Detection" proposed a Self-Supervised Learning for Graph Anomaly Detection method by constructing different contextual subgraphs based on a target node.

Liu et al. in "Anomaly Detection in Dynamic Graphs via Transformer" presented a novel Transformer-based Anomaly Detection framework for dynamic graphs by constructing a comprehensive node encoding strategy to represent each node's structural and temporal roles.

Ma et al. in "A Comprehensive Survey on Graph Anomaly Detection with Deep Learning" provided a systematic and comprehensive review of the contemporary deep learning techniques for graph anomaly detection and highlight twelve extensive future research directions.

Huang et al. in "Hybrid-Order Anomaly Detection on Attributed Networks" proposed a new deep learning model called Hybrid-Order Graph Attention Network to simultaneously detect the abnormal nodes and motif instances in an attributed network.

Li et al. in "BISSIAM: Bispectrum Siamese Network Based Contrastive Learning for UAV Anomaly Detection" a novel framework to identify UAV presence, types, and operation modes.

Li et al. in "End-to-End Transferable Anomaly Detection via Multi-spectral Cross-domain Representation Alignment" proposed a Multi-spectral Cross-domain Representation Alignment method for the anomaly detection in the domain adaptation setting.

The guest editors believe these articles represent the frontiers of current topics in the field of anomaly detection and hope these articles will stimulate further development in this area. We hope you enjoy this special issue and take some inspiration from it for your own future research.

JIANXIN LI
Beihang University
China
lijx@act.buaa.edu.cn

LIFANG HE
Lehigh University
USA
lih319@lehigh.edu

HAO PENG
Beihang University
Beijing 100191, China
penghao@buaa.edu.cn

PENG CUI
Tsinghua University
Beijing 100190, China
cuip@tsinghua.edu.cn

CHARU C. AGGARWAL
IBM Research
Yorktown Heights, NY 10598 USA
charu@us.ibm.com

PHILIP S. YU
University of Illinois at Chicago
Chicago, IL 60607 USA
psyu@uic.edu