Hindawi
Security and Communication Networks
Volume 2021, Article ID 9870129, 2 pages
https://doi.org/10.1155/2021/9870129

*Editorial*

# Machine Learning: The Cyber-Security, Privacy, and Public Safety Opportunities and Challenges for Emerging Applications

**Kehua Guo**,[1] **Zhiyuan Tan**,[2] **Entao Luo**,[3] **and Xiaokang Zhou**[4]

[1]*Central South University, Changsha, China*
[2]*Edinburgh Napier University, Edinburgh, UK*
[3]*Hunan University of Science and Engineering, Yongzhou, China*
[4]*Shiga University, Hikone, Japan*

Correspondence should be addressed to Kehua Guo; guokehua@csu.edu.cn

Received 17 November 2021; Accepted 17 November 2021; Published 3 December 2021



In recent years, as there is continuous advancement of emerging applications such as cyber-physical systems, social networks, e-commerce, and 5G systems, the collection, processing, and analysis of enterprise, government, and personal data have become greatly convenient and widespread, which makes sensitive information more vulnerable to abuses. Therefore, it is urgent to explore secure mechanisms and technologies tailored for emerging applications.

Machine learning (ML) has recently gained a renewed interest as the technology powering it has become more widely available and accessible to organizations of all sizes. Applications using machine learning are being deployed in contexts and for purposes that were not even imaginable a few years ago. From a cybersecurity, privacy, and public safety angle, ML brings about both opportunities and challenges for emerging applications. On the one hand, ML can help interested parties to better protect privacy in challenging situations, improving the state-of-the-art security solutions. On the other hand, ML also presents risks of opaque decision making, biased algorithms, and safety vulnerabilities, challenging traditional notions of privacy protection.

This special issue aims to provide a forum for those from academia and industry to communicate their latest results on theoretical advances and industrial case studies that combine ML techniques, such as reinforcement learning, adversarial machine learning, and deep learning, with significant problems in cybersecurity, privacy, and public safety. Research papers can be focused on offensive and defensive applications of ML to security. Submissions can contemplate original research, serious dataset collection and benchmarking, or critical surveys. Review articles are also welcome.

Potential topics include but are not limited to the following:

(1) Security machine learning modelling and architecture
(2) Secure multiparty computation techniques for machine learning
(3) Attacks against machine learning
(4) Machine learning threat intelligence
(5) Machine learning for cybersecurity
(6) Machine learning for intrusion detection and response
(7) Machine learning for multimedia data security
(8) Machine learning for public safety

After a thorough review process, this special issue has selected a set of eight papers to provide new insights on the abovementioned research areas.

The paper entitled "An Automatic Source Code Vulnerability Detection Approach Based on KELM" by Gaigai Tang, Lin Yang, Shuangyin Ren, Lianxiao Meng, Feng Yang, and Huiqiang Wang proposes to use extreme learning machine (ELM) to effectively improve the iterative training efficiency. In the preprocessing of this framework, they introduce doc2vec for vector representation and multilevel symbolization for program symbolization. Their experimental results show that doc2vec vector representation brings faster training and better generalizing performance than word2vec.

The paper entitled "Malicious URL Detection Based on Improved Multilayer Recurrent Convolutional Neural Network Model" by Zuguo Chen, Yanglong Liu, Chaoyang Chen, Ming Lu, and Xuzhuo Zhang addresses the problem that is hard to fully express the text information of the traditional malicious uniform resource locator (URL) and proposes an improved multilayer recurrent convolutional neural network model based on the YOLO algorithm. Compared with Text-RCNN, BRNN, and other models, their experimental results show that the method detects malicious URLs more quickly and effectively and has high accuracy, high recall rate, and high accuracy.

The paper entitled "Towards Efficient Video Detection Object Super-Resolution with Deep Fusion Network for Public Safety" by Sheng Ren, Jianqi Li, Tianyi Tu, Yibo Peng, and Jian Jiang proposes an efficient video detection object super-resolution with a deep fusion network for public security. By combining the advantages of the pixel-based super-resolution algorithm and the feature space-based super-resolution algorithm, they improve the resolution and the visual perception clarity of the key objects. Extensive experimental evaluations show the efficiency and effectiveness of their method.

The paper entitled "Creating Ensemble Classifiers with Information Entropy Diversity Measure" by Jiangbo Zou, Xiaokang Fu, Lingling Guo, Chunhua Ju, and Jingjing Chen proposes an ensemble classifier generating algorithm to improve the accuracy of an ensemble classification and to maximize the diversity of its component classifiers. Compared with existing classifier methods, it is demonstrated that their method has an obvious lower memory cost with higher classification accuracy.

The paper entitled "Fabric Defect Detection in Textile Manufacturing: A Survey of the State of the Art" by Chao Li, Jun Li, Yafei Li, Lingmin He, Xiaokang Fu, and Jingjing Chen presents a thorough overview of algorithms for fabric defect detection. First, they briefly introduce the importance and inevitability of fabric defect detection towards the era of manufacturing of artificial intelligence. Second, a systematic literature review on defect detection methods is present. Thirdly, the deployments of fabric defect detection algorithms are discussed in their study. They provide a reference for researchers and engineers on fabric defect detection in textile manufacturing.

The paper entitled "An Approach Based on the Improved SVM Algorithm for Identifying Malware in Network Traffic" by Bo Liu, Jinfu Chen, Songling Qin, Zufa Zhang, Yisong Liu, Lingling Zhao, and Jingyi Chen presents an approach for identifying malware in network traffic, called network traffic malware identification (NTMI). Their evaluation results suggest that the NTMI approach can lead to higher accuracy while achieving a lower false positive rate compared with other identification methods. On average, the NTMI approach achieves an accuracy of 92.5% and a false positive rate of 5.527%.

The paper entitled "Representativeness-Based Instance Selection for Intrusion Detection" by Fei Zhao, Yang Xin, Kai Zhang, and Xinxin Niu proposes two instance selection algorithms to handle balanced and imbalanced data problems for intrusion detection. Compared with other algorithms on the benchmark data sets of intrusion detection, their experimental results verify the effectiveness of the proposed instance selection algorithms and demonstrate that the proposed algorithms can achieve a better balance between accuracy and reduction rate or between balanced accuracy and reduction rate.

The paper entitled "Fail-Stop Group Signature Scheme" by Jonathan Jen-Rong Chen, Yi-Yuan Chiang, Wang-Hsin Hsu, and Wen-Yen Lin proposes a fail-stop group signature scheme (FSGSS) that combines the features of group and fail-stop signatures to enhance the security level of the original group signature. Based on the aforementioned objectives, this study proposes three lemmas and proves that they are indeed feasible.

## Conflicts of Interest

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

## Acknowledgments

In preparing this special issue, we would like to thank all the editors for their support. Furthermore, we would also like to thank Kehua Guo, Entao Luo, Zhiyuan Tan, and Xiaokang Zhou for helping with all cases that needed specific consideration. We thank all reviewers of the manuscripts for this special issue; their efforts have improved the quality of the volume considerably. We also thank the authors for participating in and contributing to this special issue.

*Kehua Guo*
*Zhiyuan Tan*
*Entao Luo*
*Xiaokang Zhou*