Editorial Preface

Special Issue on "Machine Learning Techniques for Information Security and Data Privacy"

Kanubhai Patel, Faculty of Computer Science and Applications, Charotar University of Science and Technology, Changa, India

Laura Sani, University of Parma, Parma, Italy

Gianfranco Lombardo, Department of Engineering and Architecture, University of Parma, Parma, Italy

The continuous development of increasingly sophisticated and accurate machine learning models is enabling several changes in different fields of science as in human activities, letting them play the role of fundamental tools in a wide range of disciplines. One of the factors that have most contributed to the diffusion and use of machine learning models is represented by the increasing availability of the so-called Big Data, on which machine learning algorithms perform statistical inference in both a supervised and unsupervised way. This allows one to find general rules which can then be applied to new unseen data.

The processing, transmission and storage of Big Data still pose challenges and are open to several risks from an information security point of view as well as novel kinds of dangers for public safety and privacy preservation. At the same time, progress in machine learning and the automatic analysis of huge amounts of data also permit to study and develop new algorithms and models for improving security at different levels. This special issue provides an overview about current research progress and future directions at the intersection of these research fields with the hope that scholars and experts of both sectors can take advantage of them.

The first article of this special issue aims at detecting different categories of cyberbullying in social networks using an unsupervised approach (i.e., subtractive clustering and fuzzy c-means clustering). The identified categories can be used to analyse various kinds of threats and their impact on the victims. The second article proposes a two-stage system for automobile insurance fraud detection, combining fuzzy c-means clustering, genetic algorithm optimization and supervised learning. The performance of the proposed system is assessed through a comparative analysis with another state-of-the-art approach.

The third article presents a novel key exchange protocol implemented as a use-case in a sample e-commerce application running on a mobile device. The main goal of this paper is to evaluate the performance of this protocol in comparison with other industrial and state of the art solutions. The fourth article presents a neural network-based approach for live detection of Distributed Denial of Service (DDoS) attacks in software defined networking (SDN) environments. The authors propose also a live mitigation process.

The fifth article presents a multi-level clustering approach for the anonymization of large-scale physical activity data for health-care research. The proposed approach has been compared to other conventional methods, showing its efficiency and effectiveness. The sixth article presents a methodology to identify the minimum feature set for malware detection by combining Rough Set dependent feature significance and Ant Colony Optimization (ACO) with a minimum loss of accuracy in two different datasets. The seventh article focuses on the application of an unsupervised Machine Learning technique to Intrusion Detection Systems. In particular, the authors propose a clustering-based outlier detection (CBOD) method to classify normal and intrusive patterns in networks.

The papers selected for this Special Issue cover various important topics regarding Machine Learning applications to Information Security and Data Privacy, highlighting the current progress and future research directions. We would like to thank the reviewers and the editorial board for their help and support, and the authors for their contributions. We hope that the research work published in this issue may further extend the use of machine learning techniques to solve problems in information security and data privacy fields.

Kanubhai Patel
Laura Sani
Gianfranco Lombardo
Guest Editors
IJISP