Neural Computing and Applications (2022) 34:15099–15100
https://doi.org/10.1007/s00521-022-07535-4

EDITORIAL

Special issue on large-scale neural computing and cybersecurity opportunities using artificial intelligence

Sumarga Kumar Sah Tyagi[1] · Elias Pimenidis[2] · Sanjeev Jain[3] · Will Serrano[4]

Received: 13 June 2022 / Accepted: 13 June 2022 / Published online: 28 June 2022

Guest Editor's Note

Cybersecurity appears to dominate the computing scene nowadays with organisations and individuals around the world seriously concerned about the safety of their computer systems and the integrity of the data they store and process. As cyber criminals are getting smarter, defenders of computer systems are becoming more innovative and they increasingly seek the support of artificial intelligence and more specifically that of Neural Computing to do so. Within such an environment, the guest editors sought and assembled a range of papers providing insights into the modern challenges to cybersecurity and the means that neural computing is offering to support the safety of online systems. The following works provide a view of a wide ranging research and allows the reader to widen their outlook as to current and forthcoming work in the field.

In "Mitigation of black hole attacks using firefly and artificial neural network" Rani, Kavita, Verma, Rawat, and Dash, explore the Firefly Algorithm with Artificial Neural Networks in attempting to enhance the Ad hoc On-Demand Distance Vector routing protocol. The authors perceive this as critical in combating black hole attacks and offering secure routing in Mobile Ad hoc Networks (MANET).

Gera and Sinha, delve into the world of social media and more specifically that of tweeter. In their work "C-ANN: a deep leaning model for detecting black-marketed colluders in Twitter social network". They explore the potential of Artificial Neural Networks is exploring and exposing collusion attempts in bolstering the popularity of tweeter accounts, for commercial gain.

In similar fashion, Jain, Kumar and Shrivastava, combine the predictions of a hierarchical attention network (HAN) and a multilayer perceptron (MLP) using context-based (text + meta-features) and user-based features, respectively. This is expected to address the serious issue of doctored narrative and fake rumours in social media. Their work is titled "CanarDeep: a hybrid deep neural model with mixed fusion for rumour detection in social data streams".

"Detecting and Responding to Hostile Disinformation Activities on Social Media using Machine Learning and Deep Neural Networks", by Cartwright, Frank, Weir, and Padda, is another article focusing on the potential of Machine Learning in responding to social media doctoring of public opinion in serious political situations. The authors draw examples from the case of Russian interference with the American Presidential elections in 2016.

In "HamDroid: permission-based harmful android anti-malware detection using neural networks" Seraj, Khodambashi, Pavlidis, and Polatidis, present their solution in detecting fake anti-malware in android environment. They employ a customized multilayer perceptron neural network.

Internet of Things (IoT) is an area that is experiencing rapid growth and at the same time many challenges. In their attempt to deliver an efficient and lightweight Network Intrusion and Detection System, suitable for IoT, Basati and Faghih propose the use of a very lightweight and efficient neural network based on the idea of deep feature extraction. Their work is titled "DFE: efficient IoT network intrusion detection using deep feature extraction".

Pokhrel, takes a more forward in the future look of IoT security in "Learning from data streams for automation and orchestration of 6G industrial IoT: toward a semantic communication framework". The author proposes a Federated Learning empowered architecture that could offer efficient support in averting anticipated challenges to 6G.

✉ Elias Pimenidis
Elias.Pimenidis@uwe.ac.uk

[1] Zhongyuan University of Technology, Zhengzhou, China

[2] University of the West of England, Bristol, UK

[3] Indian Institute of Information Technology Design and Manufacturing, Jabalpur, India

[4] University College London, London, UK

Security of industrial and critical infrastructure is an area that has benefited considerably from Neural Computing applications.

Automatic Differentiation Variational Inference (ADVI) Restricted Boltzmann Machine (RBM) to perform real-time anomaly detection of industrial infrastructure is proposed by Demertzis, Iliadis, Pimenidis, and Kikiras, in their work titled "Variational restricted Boltzmann machines to automated anomaly detection".

"Pipeline risk big data intelligent decision-making system based on machine learning and situation awareness" focuses on urban underground pipeline systems and their preventative maintenance. The authors, Zhong, Zhang, and Zhang, explore pipeline risk big data intelligent decision-making systems based on machine learning and situational awareness.

Kure, Islam and Mouratidis, propose a novel integrated cyber security risk management (i-CSRM) framework that predicts risk types through machine learning techniques, and by assessing the effectiveness of existing controls. Their work is titled "An integrated cyber security risk management framework and risk predication for the critical infrastructure protection".

"Non-intrusive load monitoring algorithm based on household electricity use habits" is the work by Yin, Li, Xu, Li, Yang and Du, that monitors the load security and efficiency of electricity networks. They do so by employing a non-intrusive load, based on household electrical habits, and by studying the relationship between household electricity consumption habits and load status decomposition method.

To address the challenges of clarity and efficiency of ship detection in aerial images, a synthetic ship detection dataset is employed to support the experimentation with various methods in overcoming some of the major challenges in this problem. He, Huang, Shen, and Wu, claim in their work "Delve into balanced and accurate approaches for ship detection in aerial images" that their method perform well and efficiently.

The guest editors were impressed with the quality of the work submitted and the range of problems addressed. We hope that the readers will find this collection of papers, attractive and useful for their own research and inspiration.

Guest Editors

Sumarga Kumar Sah Tyagi
Elias Pimenidis
Sanjeev Jain
Will Serrano

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.