Guest Editorial Preface

Special Issue on the Combination of Cyber Security and Artificial Intelligence

Liehuang Zhu, Beijing Institute of Technology, China

Guanglu Sun, Harbin University of Science and Technology, China

Bing Xia, Zhongyuan University of Technology, China

Lei Xu, Beijing Institute of Technology, China

Artificial intelligence is the most amazing technology of mankind to date, which has the revolutionary impact on industrial development and even modern society. AI research tries to make machines realize human-like functioning in many fields, such as information processing and security.

The past decade has witnessed the rapid development of AI in many aspects, especially in the field of cyberspace security playing an increasingly important role. Academia and industry have developed various machine learning or deep learning algorithms. They use them to detect cyber-attacks, software vulnerabilities, and malware analysis and so on, and a large number of research results have been published. At the same time, due to the emergence of adversarial learning, malicious samples are created by attacks to contaminate the training data, threatening the security of artificial intelligence and machine learning algorithms. This journal mainly focuses on the cutting-edge contributions and progress made by academia and industry in the integration of artificial intelligence and network security.

The organisers of Special Issue of Combination of Cyber Security and Artificial Intelligence wanted to pay tribute to the most advanced solutions, challenges, and future trends, especially the application of artificial intelligence to the following areas of cyber security.

This special issue of International Journal of Digital Crime and Forensics (IJDCF) contains nine research papers. These papers in this special issue cover a range of aspects of cyber security, from case studies in fundamental security, to the AI theories and models applied in cyber security to enhance processing ability, as well as discussions on supporting the security systems in intelligent detection. Each of these papers has undergone full double blind peer review, prior to being selected for this special issue.

The first paper is "Web Vulnerability Detection Analyzer Based on Python." Dawei Xu and Tianxin Chen explore how improving vulnerability scanners to better detect vulnerabilities on websites. The system is written in Python language realized cross-platform operation requirements and uses logs to record the response information realized the requirements of vulnerability verification. In their paper they conduct vulnerability scanning tests on hundreds of websites, and get good results.

Aiming at the current software cost model and optimal release research, which does not fully consider the actual faults in the testing phase, a cost-reliability SRGM evaluation and selection algorithm SESABCRC is proposed by Wenqian Jiang. In his paper "SRGM Decision Model Considering Cost-Reliability," he gives the corresponding cost function based on the proposed SRGM. Furthermore, an optimal release strategy is proposed in view of given restricted reliability target requirements and the uncertainty that the actual cost may exceed the expected cost. Finally, the proposed SRGM can be applied to describe the testing process of the software through actual failure dataset verification and proves superior to other models.

Shaobo Zhang and Yuhang Liu propose a novel IDS using deception technology solution to avoid ICS being intruded in their paper "A Novel IDS Securing Industrial Control System of Critical Infrastructure Using Deception Technology." With this well-designed system, the authors successfully collect and analyze a large quantity of malicious data generated by different attackers. Furthermore, the authors can identify existing attacks and prevent future attacks by utilizing analysed data.

The recording of face information causes potential cyber security risks and personal privacy disclosure risks to the public. Jing Wang, Jianhou Gan, Jun Wang, Juxiang Zhou and Zeguang Lu use face anonymity to protect face privacy in their paper "Face Anonymity Based on Facial Pose Consistency." They design a conditional automatic encoder using image restoration data pre-processing method. The proposed method can generate high-resolution images that maintain the pose of the original face. The generated image can be used for identity-independent computer vision tasks.

The existing cross-chain technology has the problem of identity privacy leakage. Xiubo Liang and Yu Zhao design a cross-chain privacy protection scheme for consortium blockchains based on group signature, certificate authority, and relay chain in their paper "A Privacy Protection Scheme for Cross-Chain Transaction Based on Group Signature and Relay Chain." The scheme is divided into three cross-chain service layers, called the management layer. Through this scheme, the identity privacy of both parties to the transaction can be protected during the cross-chain transaction process.

To reduce the dependence on depth annotation data and the geometric structure constraints, Ye Hua and Quxi Long in the paper "Monocular Depth Matching With Hybrid Sampling and Depth Label Propagation" propose a simple and effective monocular depth estimation model. They improve the model's ability to express the classification of the target and improve the interpretability of the model. Applying this method to the sampling module and depth mapping module of the deep learning network can promote deep learning 3d applications more robust.

Wan Chen, Daojun Han, Lei Zhang, Qi Xiao, Qiuyue Li, and Hongzhen Xiang explore how to reduce the time-consuming of overall and single role engineering for role-based access control (RBAC) system in their paper "A Model Study on Hierarchical Assisted Exploration of RBAC." They consider the problem that system role generation time will increase exponentially when system users or permissions increase sharply from the point of view of reducing the overall system time and local subsystem time. Based on previous theories of RBAC and attribute exploration, they put forward the relevant definitions and theorems, and give a model according to these theorems.

In the field of assessment of the network security situation, the previous work used the sparrow search algorithm (SSA) to optimize the backpropagation neural network (BPNN), but the SSA algorithm often falls into a local optimum due to fast convergence. In the paper "A Model of Network Security Situation Assessment Based on BPNN Optimized by SAA-SSA," they introduce a simulated annealing algorithm (SAA) to improve SSA and propose an assessment network security situation model based on BPNN improved by SAA-SSA, and the accuracy and validity of the model are proven by experiments.

The software remains static leads to the imbalance between offense and defense is the topic under discussion. The N-Variant eXecution (NVX) system is a heterogeneous software system to alleviate the current threats. In the paper "Security Enhancement Through Compiler-Assisted Software Diversity With Deep Reinforcement Learning," Junchao Wang, Jin Wei, Jianmin Pang, Fan Zhang, and Shunbin Li discuss how to enhance the diversity of NVX systems. They enhance the diversity of variants with a compiler-assisted approach, and use a deep reinforcement learning (DRL)-based algorithm to generate variants, ensuring the high diversity of the system.

IJDCF is proud to bring you this special issue. We hope that reading these high-quality papers will inspire you to make your own submissions to future IJDCF journal, and to support the cyber security research community. May these contributions pave the way for the broad and open waters ahead with all the new developments in cyber security and AI.

Liehuang Zhu
Guanglu Sun
Bing Xia
Lei Xu
Guest Editors
IJDCF