Journal of Ambient Intelligence and Humanized Computing (2022) 13:1255–1257
https://doi.org/10.1007/s12652-021-03645-4

EDITORIAL

Special issue on new advanced techniques in security of artificial intelligence

Mohammed Atiquzzaman[1] · Jin Li[2,3] · Witold Pedrycz[4]

Published online: 19 January 2022

The field that security of artificial intelligence (AI) has changed significantly in the past couple of years, and will likely continue to do so. On one hand, AI is widely used for security aspects of practical tasks for applications, including target detection, strategies optimization, and cybersecurity applications, etc. On the other hand, adversaries are exploiting these vulnerabilities to alter system behaviors, in order to serve a malicious goal. The vulnerabilities of AI include adversarial attacks, data privacy, and backdoor attacks, etc. AI models, therefore, need some security technologies to combat various attacks. Meanwhile, a safe AI model is crucial to ensure the security of its applications. The security of AI models in adversaries' environments has drawn a lot of attention in recent years.

In this special issue, we received 57 submissions in total. After rigorous review process, we finally have selected 27 papers with 47% acceptance rate about techniques in the security of AI. Here we introduce them from the following aspects including adversarial attacks, privacy-preserving, malware/anomaly detection, strategies optimization, and its applications.

AI models have been proved to be vulnerable to adversarial attacks. The malicious adversaries generate adversarial examples by carrying out generative adversarial networks (GANs), forcing the model to produce errors. AI models have been proved to be vulnerable to adversarial attacks. The malicious adversaries generate adversarial examples by carrying out generative adversarial networks (GANs), forcing the model to produce errors. In the paper titled ``DSCAE: A Denoising Sparse Convolutional Autoencoder Defense Against Adversarial Examples", authors Ye et al. present a method called denoising sparse convolutional autoencoder (DSCAE) to defense against adversarial perturbations. This is a preprocessing module works before the classification model, which can remove substantial amounts of the adversarial noise. In the generative adversarial network (GAN) field, authors Li et al. develop MRDGAN, a novel GAN model, in the work ``Multi-scale residual denoising GAN Model for Producing Super-Resolution CTA images". Similarly, authors Sun et al. present AGAN in their paper ``Blind Image Separation Based on Attentional Generative Adversarial Network", a single-channel blind image separation algorithm based on attention mechanism GAN.

Anomaly detection is an important research field for AI applications. In the paper titled ``Anomaly detection for industrial control operations with optimized ABC-SVM and weighted function code correlation analysis", authors Wan et al. present a novel feature extraction algorithm based on weighted function code correlation, which not only indicates the contribution of single function code in the whole function code sequence, but also analyzes the correlation of different function codes. In this work titled ``Community Detection Based on Similarities of Communication Behavior in IP Networks", a novel community detection method has been proposed for similarity of communication behavior between IP nodes (Zhang et al.). It is determined by analyzing the communication relationships and frequency of interactions between the nodes in the network. Work ``Towards Accurate Seismic Events Detection Using Motion Sensors on Smartphones" (Yuan et al.) presents a suite of algorithms for detecting anomalous seismic events from sampling data contaminated by users' operations. In the paper ``A Characteristic Standardization Method for Circuit Input Vectors Based on Hash Algorithm", the authors (Shi et al.) proposes

✉ Mohammed Atiquzzaman
atiq@ou.edu

Jin Li
jinli71@gmail.com

Witold Pedrycz
wpedrycz@ualberta.ca

[1] University of Oklahoma, Norman, OK, USA

[2] Guangzhou University, Guanghou, China

[3] Peng Cheng Laboratory, Shenzhen, China

[4] University of Alberta, Edmonton, AB, Canada

a characteristic standardization method for circuit input vectors based on the hash algorithm. Work ``Network performance analysis from binding number prospect" investigate the relationship between fractional matching extendable and binding number in networks, as well as the inner connection between the binding number and the fractional (g; f; n)-critical deleted graphs (Gao et al.). In the paper titled ``Deep Anomaly Detection in Expressway Based on Edge Computing and Deep Learning", authors (Wang et al.) applies edge computing method to vehicle target detection based on deep learning, and proves that edge computing can significantly improve the detection accuracy of target areas at a lower cost. In the paper `` Detecting Ransomware Attacks using Intelligent Algorithms: Recent Development and Next Direction from Deep Learning and Big Data Perspectives", authors (Bello et al.) aims to conduct a comprehensive survey on the detection of ransomware attacks using intelligent machine learning algorithms, unlike the previous reviews on ransomware attacks.

There are many optimization strategies to help AI models accomplish their security targets. ``An Ant Colony Optimization Algorithm with Adaptive Greedy Strategy to Optimize Path Problems" (Li et al.) presents a new ant colony optimization algorithm based on adaptive greedy strategy (GSACO). In the paper ``Multi-Station Test Scheduling Optimization Method for Industrial Robot Servo System", a multi-station test scheduling optimization method, which combines IRSS sample-level scheduling and test item-level scheduling, was proposed (Tang et al.). In the paper ``Research Cooperations of Blockchain: Toward the View of Complexity Network", authors (Wang et al.) construct keyword and author collaboration networks after removing the unrelated and low-quality works. Then they delve into the characteristics of complex networks, such as degree distribution, betweenness, and closeness. The cost of ensuring protocol security by setting a really high utility function is often higher than the value of the protocol itself, and the protocol is only suitable for a single scene. To overcome this shortage, a secure two-party computing protocol based on entropic criterion and set the corresponding security entropic threshold according to different scenes is proposed in ``A New Entropic Criterion Model in Rational Secure Two-Party Computation" (Zhang et al.).

Privacy-preserving of AI data is an important research point. In the paper ``Verifiable and privacy preserving federated learning without fully trusted centers", authors Han et al. present a verifiable federated training scheme that supports privacy protection over deep neural networks. In this scheme, the key exchange technology is used to remove the trusted center, the double masking protocol is used to ensure that the privacy of users is not disclosed, and the tag aggregation method is used to ensure the correctness of the results returned by the server. Authors Ren et al. propose a novel lattice-based linkable ring signature scheme based on the Borromean ring signature in the work ``An Efficient Lattice-Based Linkable Ring signature Scheme with Scalability to Multiple Layer". In the paper ``Trust-based Secure Directed Diffusion Routing Protocol in WSN", authors Yu et al. designs an Energy Trust Model (ETM) by introducing the remaining energy and trust of a node. This paper further proposes a Trust-based Secure Directed Diffusion Routing protocol (TSDDR) based on the model. In the paper ``An Interactive Role Learning and Discovery Model for Multi-Department RBAC Building Based on Attribute Exploration" Shen et al. proposes an attribute exploration-based Role discovery model, in order to solve the problem of the auxiliary interactive Q&A based on attribute exploration being unable to support multi-person collaborative question-answering. Authors Dou et al. propose a secure and efficient privacy-preserving data aggregation algorithm (SECPDA) based on the original clustering privacy data aggregation algorithm (CPDA) in work ``A Secure and Efficient Privacy-Preserving Data Aggregation Algorithm". In the paper ``Aitac: An Identity-based Traceable Anonymous Communication Model", authors Li et al. present a new identity-based signature algorithm, and its security is proved via existential unforgeability against chosen-message attacks (EU-CMA). Work ``Multi-watermarking Algorithm for Medical Image Based on KAZE-DCT" (Zeng et al.) proposed a zero watermarking algorithm for medical images based on KAZE-DCT. KAZE-DCT is used to extract feature vectors of medical images, and perceptual hashing is used to obtain feature sequences of medical images. Then, chaotic mapping is used to encrypt the multi-watermark images, and the zero watermarking technology is applied to embed and extract the watermarks.

There are also other application studies of AI security. For IoT, authors Pampapathi et al. propose 'two' methods aimed at IoT data distribution to the cloud utilizing IANFIS in addition to secure transmission of those distributed data utilizing MECC in the paper ``Data Distribution and secure data transmission using IANFIS and MECC in IoT". Work ``A target detection and tracking method for security in intelligence of unmanned surface" Zhang et al. apply deep learning target detection and tracking methods on unmanned surface vehicles, which improves the intelligence and safety of unmanned surface vehicles. Aiming at insufficiently detailed description problem caused by the loss of edges during a single low-resolution (LR) image's reconstruction process, this paper entitled ``Dictionary Learning based on Structural Self-similarity and Convolution Neural Network" (Zhang et al.) proposes a novel algorithm for super resolution image reconstruction, which is based on fusion of internal structural self-similarity dictionary and external convolution neural network parameters learning model. In the paper ``Research on adaptive beacon message transmission power in VANETs”, authors Wang et al. proposes an adaptive beacon transmission power algorithm based on vehicle position prediction error. Work ``EdgeCRNN: An Edge-Computing Oriented Model of Acoustic Feature Enhancement for Keyword Spotting” Wei et al. present a new Convolutional Recurrent Neural Network (CRNN) architecture named EdgeCRNN for edge computing devices. Authors Zheng et al. propose to realize the unied management of resource pool by using the corresponding virtual storage space mapping algorithm in the paper ``Research on Mapping Algorithm of Distributed Virtual Storage Space Based on Digital Certicate Authentication”.

We hope that this special issue will become instrumental in better understanding the challenges of security of AI, and will stimulate further research pursuits and applications.

We would like to take this opportunity and express our thanks to the authors who enthusiastically contributed to this special issue and shared their recent research findings. Our thanks go to reviewers whose critical yet highly constructive input was very instrumental. We are grateful to the editors for providing us with the opportunity to present this special issue under the aegis of the Journal of Ambient Intelligence and Humanized Computing.