symmetry

MDPI

Editorial

Symmetry-Adapted Machine Learning for Information Security

Jong Hyuk Park

Department of Computer Science and Engineering, Seoul National University of Science and Technology (SeoulTech), 232 Gongneung-ro, Nowon-gu, Seoul 01811, Korea; jhpark1@seoultech.ac.kr

Received: 15 June 2020; Accepted: 16 June 2020; Published: 22 June 2020

Abstract: Nowadays, data security is becoming an emerging and challenging issue due to the growth in web-connected devices and significant data generation from information and communication technology (ICT) platforms. Many existing types of research from industries and academic fields have presented their methodologies for supporting defense against security threats. However, these existing approaches have failed to deal with security challenges in next-generation ICT systems due to the changing behaviors of security threats and zero-day attacks, including advanced persistent threat (APT), ransomware, and supply chain attacks. The symmetry-adapted machine-learning approach can support an effective way to deal with the dynamic nature of security attacks by the extraction and analysis of data to identify hidden patterns of data. It offers the identification of unknown and new attack patterns by extracting hidden data patterns in next-generation ICT systems. Therefore, we accepted twelve articles for this Special Issue that explore the deployment of symmetry-adapted machine learning for information security in various application areas. These areas include malware classification, intrusion detection systems, image watermarking, color image watermarking, battlefield target aggregation behavior recognition models, Internet Protocol (IP) cameras, Internet of Things (IoT) security, service function chains, indoor positioning systems, and cryptoanalysis.

Keywords: symmetry; intrusion detection system; machine learning; image watermarking; information security; IoT security; indoor positioning system

1. Introduction

In the current era, information, and communication technology (ICT) supports a large amount of data to provide intelligent services to next-generation industries. However, this data surge has also generated data protection challenges and created the problem of catastrophic cyberattacks. The challenges of data security are rising due to the increasing number of web-connected devices, including Internet of Things (IoT) devices and smartphones. The International Data Corporation (IDC) has forecasted that the number of connected IoT devices will reach 41.6 billion and that 79.4 zettabytes (ZB) of data will be generated by 2025. This statistic demonstrates that data growth will create significant data security problems in ICT systems. Many next-generation industries, mainly financial companies, have started investing over 10% of their total ICT budget in preventing and mitigating network and computer security threats. However, defense attempts against security threats still fail due to a lack of skilled cyber talent and the existence of low-security policies. Moreover, the changing behaviors of many security attacks, including ransomware, advanced persistent threat (APT), visualization, data compression, and supply chain attacks, result in the failure of conventional security mechanisms.

Symmetry-adapted machine-learning has shown encouraging signs of relieving security risks in ICT systems. It is a subset of artificial intelligence (AI) that relies on the principles of processing future events by learning from past events or historical data. The autonomous nature of symmetry-adapted machine-learning supports effective data processing and analysis for security detection in ICT systems without the interference of human authority. Many industries, including Amazon, Facebook, and Google, are developing machine learning-adapted solutions to support security for smart hardware, distributed computing, and the cloud. Machine learning also enables accurate product recommendations, dynamic news feeds, and smart search engines in a secure manner. Various symmetry-adapted machine-learning paradigms, including generative adversarial networks, continuous learning, one-shot learning, and deep learning have been developed to perform data processing and analysis tasks in ICT systems. These paradigms can be adapted to detect security threats, such as software exploits and unknown malware.

This Special Issue, *Symmetry-Adapted Machine Learning for Information Security*, includes the development of novel approaches with innovative architectural designs and frameworks for security attack mitigation in ICT systems by employing various machine learning paradigms. These machine learning paradigms consist of knowledge models, deep reinforcement learning, singular value decomposition, shuffled singular value decomposition, convolutional neural networks, and Q-learning. In the working period of our Special Issue, we received many submissions from many different countries, which were found to make significant contributions to the main topics of interest for the Special Issue. However, only twelve high-quality papers were accepted after three rounds of strict and rigorous review processes. Specifically, the accepted papers focus on various application areas: malware classification, intrusion detection systems, image watermarking, color image watermarking, the battlefield target aggregation behavior recognition model, IP cameras, IoT security, service function chains, indoor positioning systems, and cryptoanalysis.

2. Symmetry-Adapted Machine Learning for Information Security

Symmetry-Adapted Machine Learning for Information Security delivers successfully accepted submissions [1–12] in this Special Issue of *Symmetry*. Proposals for several innovative paradigms, novel architectural designs, and frameworks with symmetry-adapted machine learning are covered in this particular issue. All the accepted articles deliver recent developments in information security based on different dimensions: malware classification, intrusion detection systems, image watermarking, color image watermarking, the battlefield target aggregation behavior recognition model, IP cameras, IoT security, service function chains, indoor positioning systems, and cryptoanalysis.

Phuc et al. [1] propose a new attack method for the BM123-64 structure based on related-key attacks. The study addresses the security weaknesses found in ciphers based on data-dependent operations implemented in lightweight targets and rapid transformation. The study results show related-key amplified boomerang attacks on a full eight rounds of BM123-64 in distinctive designs with effective complexity results.

Kang et al. [2] present an indoor location tracking system with enhanced performance by improving unstable RSSI signals collected from BLE beacons. The error range of results obtained from the RSSI values was reduced by applying a filtering algorithm based on the average filter. The evaluation of the proposed tracking method exhibits stable performance at distances less than 7 m. However, performance degradation occurs when the distance between the beacon and the device exceeds 7 m.

The vast increase in connected devices in today's networks, and their management, information security, and complexity, are significant challenges that need to be addressed. Sun et al. [3] propose a Q-learning framework hybrid module using reinforcement learning to resolve the service chain function deployment problem in networks. Simulation-based experiment results show that the proposed algorithm is superior in performance compared to CG and Viterbi when processing service requests.

Sang et al. [4] introduce the flexible job-shop scheduling problem with parallel machines in each workstation for dynamic manufacturing systems. They propose an algorithm based on the Genetic Algorithm with two-dimensional chromosomes. Experimental analysis of the algorithm using meta-heuristic data shows an improvement of the solution by 1.34% for different dimensions of the problem, such as machine failure and bottleneck machines.

The widespread implementation of IoT devices has witnessed large-scale attacks affecting personal information leakage, Denial of Service attacks attacks, and privacy violations. Lee at al. [5] present a symmetry protocol for the efficient operation of IP cameras in the IoT environment. The authentication protocol is intended to serve in heterogeneous networks as a lightweight security solution. Performance analysis demonstrates that the protocol is lighter than existing client-side based authentication technologies, resulting in a secure and a lower energy-consuming solution.

Khan et al. [6] propose a scalable and hybrid intrusion detection system (IDS) based on a two-stage ID system using Spark machine learning and a convolutional LSTM network (Conv-LSTM). The first stage implements an anomaly detection module using Spark. The second stage performs as a misuse detection module using Conv-LSTM, addressing both global and local latent threat signatures. The IDS is evaluated using the ISCX-UNB dataset with 97.29% accuracy in identifying network misuses.

Jiang et al. [7] introduces a novel 3D-CNN model to improve the identification accuracy of battlefield target aggregation operation while maintaining the low computational cost of spatio-temporal depth neural networks. A 3D convolution two-stream model based on multi-scale feature fusion further improved the multi-fiber system reducing the computational complexity of the network. Experimental results show that the 3D-CNN model increases the efficiency of existing CNN networks for aggregate behavior recognition.

Yu et al. [8] present a robust color image watermarking algorithm for the copyright protection of color images. The algorithm is based on all phase discrete cosine biorthogonal transform (APDCBT) and shuffled singular value decomposition (SSVD). The algorithm's security and robustness are improved using SSVD and the Fibonacci transform at the watermark pre-processing stage. The experimental results show that the algorithm is resistant to attacks such as Gaussian noise, salt and pepper noise, JPEG compression, and scaling attacks.

Kim et al. [9] propose a model using multiple ε-greedy buffers in off-policy deep RL to enhance research for better generalization. Multiple random ε-greedy buffers are utilized to enhance explorations towards a near-perfect generalization. Experimental results show compatibility with discrete actions and continuous control symmetrically, resulting in improved accuracy in real-time online learning for verifying whether the network is normal or abnormal.

Khanam et al. [10] approach the challenge of proof of ownership of multimedia data exposing users to significant threats emerging from transmission channel attacks over distributed computing infrastructures. An efficient blind symmetric image watermarking method using singular value decomposition (SVD) and fast Walsh–Hadamard transform (FWHT) is discussed for ownership protection. Simulation-based results demonstrate that the proposed scheme shows high robustness against attacks with the NC being numerically one compared with existing methods, which give between 0.7991 and 0.9999.

Sarnovsky et al. [11] propose a hierarchical intrusion detection system (IDS) based on the original symmetrical combination of machine learning and a knowledge-based approach for the improved detection of new types of attacks on the network. A severity prediction model is applied, and the network operator is provided when data is low for a new attack type. The performance of the proposed knowledge-based hierarchical IDS for both precision and recall is 0.998, and 0.001 for FAR. The IDS perform better than in existing studies of network intrusion detection systems.

Kwon et al. [12] propose two malware classification methods to protect systems from attacks on their security. The symmetrical covariance matrix is used in both methods: malware classification using SimHash (MCSP), and malware classification using SimHash and linear transform (MCSLT). The performance is measured in terms of accuracy and F- score using a micro-average and a weighted macro-average. MCSP shows a maximum efficiency of 98.74% and average accuracy at 98.58% for 3-g smash encoding.

3. Conclusions

This editorial discussed information security using symmetry-adapted machine learning in ICT systems. Several mechanisms have been presented for defense against security attacks. The proposed schemes include various techniques such as malware classification, intrusion detection systems, image watermarking, and color image watermarking.

Special thanks go to the Editor-in-Chief of *Symmetry*, as well as to all the editorial teams for their invaluable support throughout the preparation and publication of this Special Issue. In addition, we thank the external reviewers for their invaluable help in reviewing the papers.

Funding: This research received no external funding.

Conflicts of Interest: The author declares no conflict of interest.

References

1. Phuc, T.; Lee, C. Cryptanalysis on SDDO-Based BM123-64 Designs Suitable for Various IoT Application Targets. *Symmetry* **2018**, *10*, 353. [CrossRef]
2. Kang, J.; Seo, J.; Won, Y. Ephemeral ID Beacon-Based Improved Indoor Positioning System. *Symmetry* **2018**, *11*, 622. [CrossRef]
3. Sun, J.; Huang, G.; Sun, G.; Yu, H.; Sangaiah, A.; Chang, V. A Q-Learning-Based Approach for Deploying Dynamic Service Function Chains. *Symmetry* **2018**, *10*, 646. [CrossRef]
4. Sangaiah, A.; Suraki, M.; Sadeghilalimi, M.; Bozorgi, S.; Hosseinabadi, A.; Wang, J. A New Meta-Heuristic Algorithm for Solving the Flexible Dynamic Job-Shop Problem with Parallel Machines. *Symmetry* **2019**, *11*, 165. [CrossRef]
5. Lee, J.; Kang, J.; Jun, M.; Han, J. Design of a Symmetry Protocol for the Efficient Operation of IP Cameras in the IoT Environment. *Symmetry* **2019**, *11*, 361. [CrossRef]
6. Khan, M.A.; Karim, M.; Kim, Y. A Scalable and Hybrid Intrusion Detection System Based on Convolutional-LSTM Network. *Symmetry* **2019**, *11*, 583. [CrossRef]
7. Jiang, H.; Pan, Y.; Zhang, J.; Yang, H. Battlefield Target Aggregation Behavior Recognition Model Based on Multi-Scale Feature Fusion. *Symmetry* **2019**, *11*, 761. [CrossRef]
8. Yu, X.; Wang, C.; Zhou, X. A Robust Color Image Watermarking Algorithm Based on APDCBT and SSVD. *Symmetry* **2019**, *11*, 1227. [CrossRef]
9. Kim, C.; Park, J. Exploration with Multiple Random ε-Buffers in Off-Policy Deep Reinforcement Learning. *Symmetry* **2019**, *11*, 1352. [CrossRef]
10. Khanam, T.; Dhar, P.K.; Kowsar, S.; Kim, J.M. SVD-Based Image Watermarking Using the Fast Walsh-Hadamard Transform, Key Mapping, and Coefficient Ordering for Ownership Protection. *Symmetry* **2020**, *12*, 52. [CrossRef]
11. Sarnovsky, M.; Paralic, J. Hierarchical intrusion detection using machine learning and knowledge model. *Symmetry* **2020**, *12*, 203. [CrossRef]
12. Kwon, Y.M.; An, J.J.; Lim, M.J.; Cho, S.; Gal, W.M. Malware Classification Using Simhash Encoding and PCA (MCSP). *Symmetry* **2020**, *12*, 830. [CrossRef]