Hindawi
Security and Communication Networks
Volume 2022, Article ID 9851463, 3 pages
https://doi.org/10.1155/2022/9851463

Editorial

Security, Trust, and Privacy in Machine Learning-Based Internet of Things

Weizhi Meng,[1] **Wenjuan Li**,[2] **Jinguang Han**,[3] **and Chunhua Su**[4]

[1]*Technical University of Denmark, Kongens Lyngby, Denmark*
[2]*The Hong Kong Polytechnic University, Hong Kong, China*
[3]*Queen's University Belfast, Belfast, UK*
[4]*University of Aizu, Aizuwakamatsu, Japan*

Correspondence should be addressed to Weizhi Meng; weme@dtu.dk

Received 22 April 2022; Accepted 22 April 2022; Published 30 May 2022

Internet of Things (IoT) allows billions of devices in the physical world as well as virtual environments to exchange data with each other intelligently. The worldwide government Internet of Things (IoT) endpoint electronics and communications market will total $21.3 billion in 2022 [1]. For example, smartphones have become an important personal assistant and an indispensable part of people's everyday life and work. However, IoT security has also been a major concern in both academia and industry [2, 3]. The insider threat is one of the major threats to the IoT applications [4], where the attackers can enjoy the resources within the organization or network. For example, Passive Message Fingerprint Attacks (PMFA) [5], a type of insider attacks, can allow several internal nodes to collaborate and compromise a distributed intrusion detection system (DIDS). Hence, there is a need to deploy more suitable security mechanisms to safeguard the IoT and distributed environment, such as traffic filtration [3, 6], trust management [4, 7], and blockchain [8, 9].

Currently, machine learning technique is being widely applied to IoT in order to facilitate performance and efficiency, such as semisupervised learning [10, 11], reinforcement learning [12], and deep learning [13, 14]. For instance, semisupervised learning has been widely studied on how to enhance the detection of spam by leveraging both labeled and unlabeled data [15]. However, machine learning also suffers many issues, which may threaten the security, trust, and privacy of IoT environments. Among these issues, adversarial learning is one major threat, in which attackers may try to fool the learning algorithm with particular training examples and lead to a false result or an inaccurate machine learning model [16, 17].

This Special Issue will focus on cutting-edge research from both the academia and industry and aims to solicit original research and review articles with a particular emphasis on discussing the security, trust, and privacy challenges in machine learning-based IoT. The potential topics focus on the application of machine learning techniques to address security, privacy, and trust issues in IoT systems, networks, and beyond. All submissions have been reviewed by independent reviewers and have undergone several rounds of revisions before being accepted for publication in this Special Issue. After a rigorous review process, a total of 12 papers were finally accepted.

In the first contribution titled "An Unsupervised Learning-Based Network Threat Situation Assessment Model for Internet of Things", Yang et al. [18] presented an unsupervised learning-based network threat situation assessment model that could work in a multisource data IoT network. In the evaluation, they implemented the algorithm with Python and demonstrated that their approach could reach a stronger characterization ability for network threats.

In the second contribution titled "A Key Business Node Identification Model for Internet of Things Security", Xie et al. [19] introduced a key business node identification model for IoT networks, by providing an analysis of business continuity. It contains four major modules: data preparation module, data operation module, decision module, and

analysis module. The experimental results indicated that the proposed model can enhance the identification accuracy, with reasonable continuity risk assessment.

In the third contribution titled "A Privacy-Preserving Caching Scheme for Device-to-Device Communications", Zhong et al. [20] introduced a privacy-preserving device-to-device (D2D) caching scheme by defining the node importance as the weighted sum of the physical intimacy and request similarity between devices. In their comparison with Leave Copy Everywhere (LCE) and Most Popular Cache (MPC), the proposed scheme demonstrated better performance.

In the fourth contribution titled "Two-Party Secure Computation for Any Polynomial Function on Ciphertexts under Different Secret Keys", Jiang [21] introduced a scheme that can reduce the size of the ciphertext under a single key. In the fifth contribution titled "An Efficient Anonymous Communication Scheme to Protect the Privacy of the Source Node Location in the Internet of Things", Li et al. [22] introduced an efficient anonymous communication scheme to ensure privacy in two aspects: source node location and the workload.

In the next contribution titled "A Residual Learning-Based Network Intrusion Detection System", Man and Sun [23] designed a deep learning-based intrusion detection model based on residual learning. There are three parts: data preprocessing, model construction, and model evaluation. Their evaluation on UNSW-NB15 demonstrated that the proposed scheme can reach good performance due to the residual blocks.

In the next contribution titled "Machine Learning-Based Stealing Attack of the Temperature Monitoring System for the Energy Internet of Things", Li et al. [24] designed a platform of Energy Internet of Things (EIoT) for the temperature monitoring system. They then introduced a two-step model stealing attack that can use the stolen data to set a copycat network, which could leak the artificial intelligence models.

In the next contribution titled "An Efficient Communication Intrusion Detection Scheme in AMI Combining Feature Dimensionality Reduction and Improved LSTM", Lu and Tian [25] introduced a Stacked Autoencoder method to achieve feature dimensionality reduction for the high-dimensional features of data in Advanced Metering Infrastructure (AMI). In addition to using Attention Mechanism, their evaluation showed that better performance could be achieved based on two datasets: UNSW-NB15 and NSL-KDD.

In the next contribution titled "An Adaptive Communication-Efficient Federated Learning to Resist Gradient-Based Reconstruction Attacks", Li et al. [26] introduced an adaptive frequency-compression federated learning (AFC-FL) by adjusting the communication frequency and parameter compression. In the evaluation, they showed that the proposed model could reduce the workload significantly.

In the next contribution titled "A Hierarchical Approach for Advanced Persistent Threat Detection with Attention-Based Graph Neural Networks", Li et al. [27] introduced a hierarchical approach that is capable of effectively detecting APTs with attention-based Graph Neural Networks (GNNs). In the evaluation, they discussed that the proposed method could outperform some similar approaches.

In the next contribution titled "Towards a Statistical Model Checking Method for Safety-Critical Cyber-Physical System Verification", Xie et al. [28] constructed a cross-entropy optimization model in Safety-Critical Cyber-Physical System (SCCPS). Their experimental results indicated that the proposed method could reduce the standard deviation and corresponding errors by more than an order of magnitude.

In the final contribution titled "Cost-Sensitive Approach to Improve the HTTP Traffic Detection Performance on Imbalanced Data", Li et al. [29] introduced a character-level abstract feature extraction approach (cost-effective) to enhance the detection of the HTTP traffic under imbalanced data. In the evaluation, they demonstrated a higher detection rate as compared with two similar studies.

Conflicts of Interest

We declare no conflicts of interest.

Acknowledgments

We would like to take this opportunity to thank the Chief Editor Dr. Di Pietro and all staff from *Security and Communication Networks*, for supporting and guiding this Special Issue. We also thank all authors for their submissions and support and express our deepest gratitude to all the anonymous reviewers who devoted their time reviewing all the papers in this Special Issue. We believe that this Special Issue can provide useful hints on how to address security, privacy, and trust issues in machine learning-based IoT environments.

Weizhi Meng
Wenjuan Li
Jinguang Han
Chunhua Su

References

[1] Gartner report:, 2021, https://www.gartner.com/en/newsroom/press-releases/2021-06-30-gartner-global-government-iot-revenue-for-endpoint-electronics-and-communications-to-total-us-dollars-21-billion-in-2022.

[2] W. Li, W. Meng, and M. H. Au, "Enhancing Collaborative Intrusion Detection via Disagreement-Based Semi-Supervised Learning in IoT Environments," *Journal of Network and Computer Applications*, vol. 161, pp. 1–9, 2020.

[3] W. Meng, W. Li, and L. F. Kwok, "Towards Effective Trust-Based Packet Filtering in Collaborative Network Environments," *IEEE Transactions on Network and Service Management*, vol. 14, no. 1, pp. 233–245, 2017.

[4] W. Meng, K.-K. R. Choo, S. Furnell, A. V. Vasilakos, and C. W. Probst, "Towards Bayesian-Based Trust Management for Insider Attacks in Healthcare Software-Defined Networks," *IEEE Transactions on Network and Service Management*, vol. 15, no. 2, pp. 761–773, 2018.

[5] W. Li and W. Meng, "PMFA: Toward Passive Message Fingerprint Attacks on Challenge-Based Collaborative Intrusion Detection Networks," in *Proceedings of the 10th International Conference on Network and System Security (NSS 2016)*, pp. 433–449, Taipei, Taiwan, September 2016.

[6] W. Meng, "Intrusion Detection in the Era of IoT: Building Trust via Traffic Filtering and Sampling," *Computer*, vol. 51, no. 7, pp. 36–43, July 2018.

[7] A. Rezapour and W.-G. Tzeng, "A Robust Intrusion Detection Network Using Thresholdless Trust Management System with Incentive Design," *Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering*, vol. 255, no. 2, pp. 139–154, 2018.

[8] H. Liang, J. Wu, S. Mumtaz, J. Li, X. Lin, and M. Wen, "MBID: Micro-Blockchain-Based Geographical Dynamic Intrusion Detection for V2X," *IEEE Communications Magazine*, vol. 57, no. 10, pp. 77–83, 2019.

[9] O. Alkadi, N. Moustafa, and B. Turnbull, "A Review of Intrusion Detection and Blockchain Applications in the Cloud: Approaches, Challenges and Solutions," *IEEE Access*, vol. 8, pp. 104893–104917, 2020.

[10] R. Švihrová and C. Lettner, "A Semi-Supervised Approach for Network Intrusion Detection," in *Proceedings of the 15th International Conference on Availability, Reliability and Security*, vol. 93, pp. 1–6, Ireland, August 2020.

[11] Y. Zong and G. Huang, "Application of Artificial Fish Swarm Optimization Semi-Supervised Kernel Fuzzy Clustering Algorithm in Network Intrusion," *Journal of Intelligent and Fuzzy Systems*, vol. 39, no. 2, pp. 1619–1626, 2020.

[12] Y. Jiang, K. Zhang, Y. Qian, and L. Zhou, "Reinforcement Learning-Based Query Optimization in Differentially Private IoT Data Publishing," *IEEE Internet of Things Journal*, vol. 8, no. 14, pp. 11163–11176, 2021.

[13] C. Wu and W. Li, "Enhancing Intrusion Detection with Feature Selection and Neural Network," *International Journal of Intelligent Systems*, vol. 36, no. 7, pp. 3087–3105, 2021.

[14] N. Gupta, V. Jindal, and P. Bedi, "CSE-IDS: Using Cost-Sensitive Deep learning and Ensemble Algorithms to Handle Class Imbalance in Network-Based Intrusion Detection Systems," *Computers & Security*, vol. 112, Article ID 102499, 2022.

[15] S. Hershkop and S. J. Stolfo, "Combining email Models for False Positive Reduction," in *Proceedings of the eleventh ACM SIGKDD international conference on Knowledge discovery in data mining-KDD '05*, pp. 98–107, Chicago IL USA, August 2005.

[16] A. Abusnaina, A. Khormali, H. Alasmary, J. Park, A. Anwar, and A. Mohaisen, "Adversarial Learning Attacks on Graph-Based IoT Malware Detection Systems," *ICDCS*, in *Proceedings of the 2019 IEEE 39th International Conference on Distributed Computing Systems*, pp. 1296–1305, Dallas, TX, USA, July 2019.

[17] A. Singh and B. Sikdar, "Adversarial Attack and Defence Strategies for Deep-Learning-Based IoT Device Classification Techniques," *IEEE Internet of Things Journal*, vol. 9, no. 4, pp. 2602–2613, 2022.

[18] H. Yang, R. Zeng, F. Wang, G. Xu, and J. Zhang, "An Unsupervised Learning-Based Network Threat Situation Assessment Model for Internet of Things," *Security and Communication Networks*, vol. 2020, Article ID 6656066, 11 pages, 2020.

[19] L. Xie, H. Ni, H. Yang, and J. Zhang, "A Key Business Node Identification Model for Internet of Things Security," *Security and Communication Networks*, vol. 2020, pp. 1–11, Article ID 6654283, 2020.

[20] Y. Zhong, Z. Li, and L. Liao, "A Privacy-Preserving Caching Scheme for Device-to-Device Communications," *Security and Communication Networks*, vol. 2021, Article ID 6696149, 8 pages, 2021.

[21] B. Jiang, "Two-Party Secure Computation for Any Polynomial Function on Ciphertexts under Different Secret Keys," *Security and Communication Networks*, vol. 2021, pp. 1–6695304, 2021.

[22] F. Li, P. Ren, G. Yang et al., "An Efficient Anonymous Communication Scheme to Protect the Privacy of the Source Node Location in the Internet of Things," *Security and Communication Networks*, vol. 2021, Article ID 6670847, 16 pages, 2021.

[23] J. Man and G. Sun, "A Residual Learning-Based Network Intrusion Detection System," *Security and Communication Networks*, vol. 2021, Article ID 5593435, 9 pages, 2021.

[24] Q. Li, L. Zhang, R. Zhou, Y. Xia, W. Gao, and Y. Tai, "Machine Learning-Based Stealing Attack of the Temperature Monitoring System for the Energy Internet of Things," *Security and Communication Networks*, vol. 2021, Article ID 6661954, 8 pages, 2021.

[25] G. Lu and X. Tian, "An Efficient Communication Intrusion Detection Scheme in AMI Combining Feature Dimensionality Reduction and Improved LSTM," *Security and Communication Networks*, vol. 2021, Article ID 6631075, 21 pages, 2021.

[26] Y. Li, Y. Li, H. Xu, and S. Ren, "An Adaptive Communication-Efficient Federated Learning to Resist Gradient-Based Reconstruction Attacks," *Security and Communication Networks*, vol. 2021, Article ID 9919030, 16 pages, 2021.

[27] Z. Li, X. Cheng, L. Sun, J. Zhang, and B. Chen, "A Hierarchical Approach for Advanced Persistent Threat Detection with Attention-Based Graph Neural Networks," *Security and Communication Networks*, vol. 2021, Article ID 9961342, 14 pages, 2021.

[28] J. Xie, W. Tan, B. Fang, and Z. Huang, "Towards a Statistical Model Checking Method for Safety-Critical Cyber-Physical System Verification," *Security and Communication Networks*, vol. 2021, Article ID 5536722, 12 pages, 2021.

[29] W. Li, S. Sun, S. Zhang, H. Zhang, and Y. Shi, "Cost-Sensitive Approach to Improve the HTTP Traffic Detection Performance on Imbalanced Data," *Security and Communication Networks*, vol. 2021, Article ID 6674325, 11 pages, 2021.