Journal of Network and Systems Management (2022) 30:39
https://doi.org/10.1007/s10922-022-09659-3

EDITORIAL

Special Issue on Cybersecurity Management in the Era of AI

Moayad Aloqaily[1] · **Salil Kanhere**[2] · **Paolo Bellavista**[3] · **Michele Nogueira**[4]

Accepted: 2 March 2022 / Published online: 18 March 2022

Fifth Generation (5G) and beyond cellular networks have revolutionized the communication architecture, providing connectivity for people, things, data, applications, transport, and cities in smart networked environments, at faster data rates, reduced latencies, and acceptable costs. The massive number of heterogeneous connected devices in such an open space has led to an increasing number of personal and ubiquitous intelligent systems associated with advancements in human–computer interaction (HCI), artificial intelligence (AI), computing and communication technologies. Such a vast deployment of connected smart technologies introduces new challenges to scalable system security and privacy, mainly for Cyber-physical Systems.

Cyber-physical means the integration of physical and computing domains as seen in many different areas such as medical, automotive, energy, and other critical systems. Cyber-physical systems are highly prone to cyber-attacks and other forms of security threats at the communication layer due to the hyperconnectivity of these systems. Some of today's emerging security threats are hard to detect using traditional security and privacy measures and techniques. Therefore, there is an urgent request for innovative solutions for achieving security and privacy in intelligent cyber-physical systems. Hence, cybersecurity management systems need to adapt to the changing cyber security threats autonomously with minimal user intervention to provide maximum protection against cyber-attacks, intrusions, malware, and various types of data breaches.

✉ Moayad Aloqaily
moayad.aloqaily@mbzuai.ac.ae

Salil Kanhere
Salil.Kanhere@unsw.edu.au

[1] Machine Learning Department, Mohamed Bin Zayed University of Artificial Intelligence (MBZUAI), Abu Dhabi, UAE

[2] UNSW Sydney, Sydney, Australia

[3] DISI, University of Bologna, Bologna, Italy

[4] Federal University of Parana, Curitiba, Brazil

Artificial Intelligence (AI) has a great potential to evolve cybersecurity and cyber threat detection. It has received significant interest lately. Many intelligent learning techniques, such as deep and reinforcement learning, are now being integrated into cybersecurity systems to provide more secure and robust privacy-preserving solutions for personal and ubiquitous systems. Such integration plays a vital role in providing enhanced security for intelligent autonomous systems and enables organizations to make crucial changes to their security landscape.

This Special Issue has targeted theoretical and applied cutting-edge research on standards, frameworks, models, and approaches on cybersecurity management in the era of AI and intelligent learning technologies. Notably, we have encouraged and stimulated original submissions on the most recent advances in security network and system management solutions using AI, with a particular interest in contributions from the industry. Therefore, the Special Issue has attracted manuscripts primarily with the following topics of interest:

- Cybersecurity management in cyber-physical systems using AI.
- Security, privacy, and trust issues in cyber-physical systems.
- Blockchain-enabled cyber-physical systems.
- Utilizing AI technologies for cyber investigation and threat intelligence.
- The integration of AI and Blockchain for security critical infrastructures.
- Design, optimization, and modeling of cybersecurity management systems.
- AI and ML for intrusion detection/prevention in sensitive environments.
- Advanced AI techniques to secure future Internet architectures/protocols.
- Trust management in cyber-physical networks and systems.
- Privacy management at edge of the network using machine learning.
- Trustworthy data collection and processing using intelligent learning techniques.
- Cybersecurity management of big data.
- AI-based cybersecurity techniques for IoT, IoE, IoH, and IoV.
- Cybersecurity of connected and autonomous vehicles.
- Cybersecurity and AI for digital twins.
- Management framework for intelligent secure networking.
- Cybersecurity management to protect organizations' sensitive data using intelligent learning techniques.
- AI-enabled digital investigation.

These topics and the aim of this Special Issue are timely for the research communities as well as the cybersecurity industry. The peer-review process has provided a valuable contribution to the emerging field of management of cybersecurity using AI. The review process was thorough, and after several rounds of peer-reviews, twenty articles have been accepted. The article selection was merely based on the scientific quality of the submitted papers, suitability to the Special Issue, and contribution. Various topics related to the AI for cybersecurity were solicited, as follows.

In the modern Software Defined Networking (SDN) paradigm, controllers are sensitive points of failures in the whole network architecture and may represent a key target of malicious cyberattacks. The article titled "Machine-Learning-enabled

DDoS attacks detection in P4 programmable networks", by F. Musumeci et al., investigates the potential of Artificial Intelligence combined with data plane programmability, enabled by P4 language, to perform real-time attack detection directly in network switches and with marginal involvement of SDN controllers.

It is evident that the IoT paradigm is the next frontier in technology and engineering; cybersecurity poses a major challenge for it, and deep learning may well be the single best solution for the unique characteristics of the problem. On these grounds, the article entitled "Deep Learning in IoT Intrusion Detection" sheds light on the deep learning methods which have been proposed for intrusion detection, specifically targeting IoT environments, offering an exhaustive, detailed exposition of all the research that has been conducted in this area.

Numerous machine learning techniques for intrusion detection have been proposed over the last decade but are rarely deployed in operation systems, most possibly due to the lack of generalization power of the newly developed models. The article entitled "Towards Model Generalization for Intrusion Detection: Unsupervised Machine Learning Techniques" by Verkerken et al. assesses the generalization strength of four unsupervised machine learning models for intrusion detection using a novel inter-dataset evaluation strategy. This enables the research community to estimate and further improve the generalization strength of future developments.

The inclusion of information and communication technology (ICT) tools in the smart grid paradigm has increased its vulnerability to cyber-attacks. An attack on the electricity market operation in the smart grid aims at causing unethical loss or profit to a particular power utility or consumer. The article "An Ensemble Classifier Based Scheme for Detection of False Data Attacks Aiming at Disruption of Electricity Market Operation" by Jena et al. proposes an ensemble classifier-based approach to detect any manipulation of sensor information carried out by the intruder, with the intention of disrupting the electricity market.

Classifying Android malware has become increasingly important due to its significant threat and the potential financial loss for businesses and governments. The article entitled "Effective and Efficient Hybrid Android Malware Classification Using Pseudo-Label Stacked Auto-Encoder" by Mahdavifar et al. proposes an effective and efficient Android malware category classification approach based on a semi-supervised deep neural network, namely Pseudo-Label Stacked Auto-Encoder (PLSAE). It is a hybrid approach that integrates both static and dynamic analysis of malware to utilize the strengths of both types of features. The semi-supervised technique benefits from the unsupervised pre-training using Stacked Auto-Encoder (SAE) that helps in better generalization. Furthermore, it eliminates the need for numerous labeled instances, which is very expensive to acquire for malware analysis.

The demand for intelligent intrusion detection approaches using Machine Learning (ML) techniques is significantly increasing due to the widespread of distributed heterogeneous devices. The article entitled "An Intelligent Tree-based Intrusion Detection Model for Cyber Security" by Al-Omari et al. proposes an intelligent intrusion detection model based on the concept of Decision Trees to detect and predict cyber-attacks efficiently and reduce the complexity of the computation process considering the ranking of the security features compared to other traditional machine learning techniques.

The volume and complexity of cyber-attacks have grown near exponentially, which leaves cybersecurity analysts overwhelmed when navigating through countless daily Intrusion Detection Systems (IDS) threat alerts. The article entitled “FAIXID: A Framework for Enhancing AI Explainability of Intrusion Detection Results Using Data Cleaning Techniques” by Liu et al. proposes an integrated framework that incorporates Explainable Artificial Intelligence (XAI) and data cleaning techniques to improve the explainability and understandability of intrusion detection alerts, thereby assisting cybersecurity analysts in making more informed decisions.

Due to the extensive and high-dimensional availability of transactional data in cyber-physical systems, previous approaches relying on frequent item sets (FIs) as features suffer from dimensionality, sparsity, and privacy issues. The article entitled “A Federated Learning Approach to Frequent Itemset Mining in Cyber-Physical Systems” by Ahmed et al. developed an embedding model based on federated learning for transaction classification. The model considers transaction data as a collection of frequent item sets. Then, the model can be used to train low-dimensional continuous vectors while preserving the contextual association between frequent item sets. Extensive experimental studies on many high-dimensional transaction datasets to validate the constructed models with an attention-based mechanism and federated learning are then conducted and from the results, the developed model can support and improve the decision boundaries by lowering the global loss function while maintaining security and privacy.

Password generation and strength estimation have been trivial tasks. However, it remains a concern for users due to their readily available personally identifiable information. The article entitled “PassMon: A Technique for Password Generation and Strength Estimation” by Murmu et al. evaluates passwords doing prediction using SVM by learning over leaked passwords and guessing the difficulty to guess the password using LSTM. Further, the article suggests three password design methods to create memorable and reasonably strong passwords by taking user personal information and adding randomness based on functional patterns.

Fog computing allows computing to be placed at the edge of the network closer to the user. Lately, it has been gaining interest worldwide and so are its security issues. The article entitled “Human Immune-Based Intrusion Detection and Prevention System for Fog Computing” by Aliyu et al. proposes a human immune-based intrusion detection and prevention system that reduces the overhead on the fog nodes by distributing detection amongst the nodes in the fog layer. The system also uses specialized fog nodes called IDS nodes to improve the accuracy of the system.

5G expects to support a multi-tenant business model in which users may rent or buy service, resource, and infrastructure capabilities across multiple domains to cover feasible peak workloads with security and trustworthiness. The article entitled “Design of a Security and Trust Framework for 5G Multi-domain Scenarios” by Jorquera Valero et al. proposes a novel approach for increasing the security and trust levels of the 5G infrastructure, shared by diverse multi-tenant network slices. In addition, this article not only designs a security and trust framework but also builds it to validate zero trust principles in distributed multi-stakeholder environments, following the security and trust approach by the H2020 5GZORRO.

How to design an efficient security-aware routing protocol that can adapt its operating parameters based on the unique characteristics of the cognitive radio (CR) operating RF environment is critical in dynamic full-duplex (FD)-based CR networks (CRNs). The article entitled "Intelligent Secure Networking in In-band Full-duplex Dynamic Access Networks: Spectrum Management and Routing Protocol" by Bany Salameh et al. proposes a security-aware intelligent routing protocol that aims at mitigating the effects of jamming attacks on in-band FD (IBFD) CRNs. This protocol considers the unique characteristics of the CRN environment while being IBFD-aware. Specifically, it considers the primary user's channel-availability time, channel quality and jamming strategy.

Malicious websites are a primary means of carrying out cyber-attacks. In particular, malicious Uniform Resource Locators (URLs) embedded in social media posts have been used as weapons for luring Internet users into downloading and executing malicious content leading to compromised systems. The article entitled "URLdeepDetect: A Deep Learning Approach for Detecting Malicious URLs Using Semantic Vector Models" proposes a hybrid deep-learning approach named URLdeepDetect for time-of-click URL analysis and classification to detect malicious URLs.

Malicious IoT devices are major concerns that threaten the security of IoT applications. The article entitled "Building an Intelligent Global IoT Reputation and Malicious Devices Detecting System" by Yaseen and Jararweh proposes an intelligent reputation system for IoT devices using edge computing and cloud computing infrastructures. The proposed system can be used to mitigate the effect of malicious and malfunction IoT devices and enhance the effectiveness of IoT-based systems such as smart cities.

Timely and accurate cyber treat intelligence is crucial to cyber security professionals, services, and cyber defense products. The article entitled "A Deep Learning Approach for Classifying Vulnerability Descriptions Using Self Attention Based Neural Network" by Vishnu et al. proposes an artificial intelligence-based system that automates the process of classifying vulnerability descriptions to eliminate human errors and reduce manual effort involved in verification of descriptions from existing vulnerability databases such as CVE and NVD, which are widely adopted within the cyber security industry.

Automated surveillance systems aid in ensuring safety and security of life and property in smart cities. Recent developments in adversarial machine learning-based attacks could circumvent and trick such systems and render them ineffective. The article entitled "A Novel Lightweight Defense Method Against Adversarial Patches-Based Attacks on Automated Vehicle Make and Model Recognition Systems" by Siddiqui and Boukerche studies the impact of adversarial patches on an automated surveillance system that is designed for vehicle make and model recognition and proposes a lightweight defense method that detects adversarial patches and mitigates their effect with a minimal overhead.

The Internet of Things (IoT) security is critical due to potential malicious threats and the diversity of the connectivity. Devices can protect themselves and detect threats with the Intrusion Detection System (IDS). The paper by Otoum and Nayak proposes a model (known as "AS-IDS") that combines two approaches of the IDSs:

"anomaly-based and signature-based approaches to detect known and unknown attacks in IoT networks.".

Improper publication of trajectory data may jeopardize the privacy of moving objects, so trajectories ought to be anonymized before making them accessible to the public. The article entitled "Personalized Privacy-Preserving Publication of Trajectory Data by Generalization and Distortion of Moving Points" by Mahdavifar et al. proposes a novel clustering-based approach for privacy-preserving publication of trajectory data with the aim of anonymizing trajectories to some extent so that an adversary having some background knowledge cannot uniquely identify a specific trajectory, but with a maximum probability inversely proportional to the privacy protection requirement of the moving object that produced it.

Smart home systems are implemented on the top of connected sensors that act as data acquisition tools. However, such sensors are vulnerable to identity theft in which intruders can recognize residence activities by learning how these sensors are functioning. The article entitled "Cybersecurity of Smart Home Systems: Sensor Identity Protection" by Yazan Alshboul et al. proposes a protection technique that prevents intruders from identifying the functionality of working sensors. The proposed 3-phase technique guarantees keeping the identity of sensors hidden from outsiders.

A vehicular Botnet is one of the most dangerous cyber threats that can target connected vehicles, in which an attacker can compromise the onboard computer and take full control of the vehicle. The paper "AntibotV: A Multilevel Behaviour-Based Framework for Botnets Detection in Vehicular Networks" by Rahal et al. proposes a multilevel behaviour-based framework for botnet detection in vehicular networks. AntibotV monitors the vehicle's interaction with the outside world by analyzing network traffic. It also monitors activity inside the vehicle to detect suspicious operations that may be related to malicious bot activity. The multi-level monitoring aims to counter vehicular botnets at all levels.

Moayad Aloqaily (S-12, M-17, SM-21) received the Ph.D. degree in CE from the University of Ottawa, Canada, in 2016. He was an Instructor with the SYSC Department, Carleton University, Canada, in 2017. From 2018–2019, he was an assistant professor with American University of Middle East (AUM), Kuwait. From 2019–2021, he was the Cybersecurity Program Director and an assistant professor with the Faculty of Engineering, Al Ain University, UAE. He is the Managing Director of xAnalytics Inc., Canada, since 2019. He is currently with the Machine Learning Department, Mohamed Bin Zayed University of Artificial Intelligence (MBZUAI), UAE. His current research interests include the applications of AI and ML, connected and autonomous vehicles, blockchain solutions, and sustainable energy and data management. Dr. Aloqaily has chaired and co-chaired many IEEE conferences and workshops. He has served as a guest editor in many journals, including IEEE Wireless Communications Magazine, IEEE Network, and Computer Network. He is an Associate Editor of IEEE Wireless Communications, IEEE Networking Letters, Ad Hoc Networks, Journal of Network and Systems Management, Simulation Modelling Practice and Theory, Cluster Computing, Security and Privacy, and IEEE Access. He has also been appointed as the Co-Editor-in-Chief of IEEE CommSoft TC eLetter in 2020. He started his Special Interest Groups on Blockchain and Application as well as Internet of Unmanned Aerial Networks. He is an IEEE Senior Member, ACM Member and a Professional Engineer Ontario (P.Eng.). https://scholar.google.com/citations?user=AuAQVVEAAAAJ&hl=en&oi=ao.

Salil Kanhere received the M.S. and Ph.D. degrees from Drexel University, Philadelphia, USA. He is a Professor in the School of Computer Science and Engineering at UNSW Sydney, Australia. His research interests include the Internet of Things, cyber-physical systems, blockchain, pervasive computing, cybersecurity, and applied machine learning. Salil is also affiliated with CISRO's Data61 and the Cybersecurity Cooperative Research Centre. He is a Senior Member of the IEEE and ACM, an ACM Distinguished Speaker, and an IEEE Computer Society Distinguished Visitor. He has received the Friedrich Wilhelm Bessel Research Award (2020) and the Humboldt Research Fellowship (2014), both from the Alexander von Humboldt Foundation in Germany. He has held visiting positions at I2R Singapore, Technical University Darmstadt, University of Zurich, and Graz University of Technology. He serves as the Editor in Chief of the Ad Hoc Networks Journal and as an Associate Editor of IEEE Transactions on Network and Service Management, Computer Communications, and Pervasive and Mobile Computing. He has been involved in the organization of many IEEE/ACM international conferences. He co-authored a book titled Blockchain for Cyber-physical Systems which was published by Artech House in 2020. https://scholar.google.com/citations?user=sgqmaPMAAAAJ&hl=en.

Paolo Bellavista is a Professor of Distributed and Mobile Systems at Dept. Computer Science and Engineering (DISI), Alma Mater Studiorum University of Bologna. His primary research interests and areas relate to middleware for mobile computing, Internet-of-Things platforms, efficient integrations of sensors-edge-cloud, edge/fog computing, mobile pervasive applications for Industry 4.0 and smart cities/communities. He has been visiting professor at Sorbonne Universités Paris and University College London. In addition to national/EU project participation (he is currently the scientific coordinator of the H2020 IoTwins project—https://www.iotwins.eu/) and publication activities, he is Editor-in-Chief of the MDPI Computers Journal (2017-), Associate Editor-in-Chief of IEEE Communication Surveys and Tutorials (2019-), and member of the Editorial Boards of ACM Computing Surveys (2020-), IEEE Transactions on Network and Service Management (2011-), Elsevier Pervasive and Mobile Computing Journal (2010-), and Elsevier Journal on Network and Computing Applications (2015-). https://scholar.google.com/citations?user=vVSZ4rUAAAAJ&hl=it.

Michele Nogueira is an Associate Professor at the Department of Computer Science, Federal University of Minas Gerais, Brazil. She is a CNPq Research Fellow, Brazil. D.Sc. in Computer Science, UPMC—Sorbonne Universités/LIP6, Paris, France. In 2009, I was a Postdoctoral Scholar at Telecom ParisTech (before: École Nationale Supérieure des Telecommunications—ENST), Paris, France, and a Visiting Researcher at the Broadband Networking Laboratory (BWN-Lab), Georgia Institute of Technology (GeorgiaTech), Atlanta, USA, at the beginning of the same year. In 2012, she was an Invited Researcher at the Laboratoire de Recherche en Informatique, Université Paris Sud, Orsay, France. She serves as Associate Technical Editor for the IEEE Communications Surveys and Tutorials and is a member of the Institute of Electrical and Electronics Engineers (IEEE) and Association for Computing Machinery (ACM). https://scholar.google.com/citations?user=1CfmgaAAAAAJ&hl=it.