

Machine Learning and Cyber Threat Intelligence and Analytics: An Overview and Introduction to the Mini-Track

Kim-Kwang Raymond Choo
University of Texas at San Antonio
raymond.choo@fulbrightmail.org

Ali Dehghantanha
University of Guelph
adehghan@uoguelph.ca

Glenn Dietrich
University of Texas at San Antonio
Glenn.Dietrich@utsa.edu

Abstract

In this editorial, we will introduce the two papers accepted for presentation and inclusion in the 'Machine Learning and Cyber Threat Intelligence and Analytics' mini-track.

1. Introduction

As we noted in our previous editorial [1], cyber security remains an important policy and national security agenda items in technologically advanced nations such as Australia, Canada, New Zealand, United Kingdom, and United States. This trend has not changed since our mini-track was first introduced in HICSS 2018 [2]–[4].

In this year, we accepted two papers, as described below.

- (1) Universal Spam Detection using Transfer Learning of BERT Model, by Vijay Srinivas Tida and Sonya HY Hsu
- (2) Walk This Way: Footwear Recognition Using Images & Neural Networks, by Valentin Gazeau, William Glisson, Cihan Varol and Qingzhong Liu

In addition to the topics discussed in these two accepted papers, the following topics remain of relevance and importance to our cyber and national security conversation:

- Blockchain and its application in cyber security
- Detection and analysis of advanced threat actors tactics, techniques and procedures
- Application of machine / deep learning tools and techniques in cyber threat intelligence
- Theories and models for detection and analysis of advanced persistent threats
- Automated and smart tools for collection, preservation and analysis of digital evidences

- Threat intelligence techniques for constructing, detecting, and reacting to advanced intrusion campaigns
- Applying machine / deep learning tools and techniques for malware analysis and fighting against malicious cyber activities (e.g., cyber crime)
- Intelligent incident response tools, techniques and procedures for contemporary technologies, such as cloud and cyber-physical systems
- Intelligent analysis of different types of data collected from different layers of network security solutions
- Threat intelligence in cyber security domain utilizing big data solutions such as Hadoop
- Intelligent methods to manage, share, and receive logs and data relevant to variety of adversary groups
- Interpretation of cyber threat and forensic data utilizing intelligent data analysis techniques
- Infer intelligence of existing cyber security data generated by different monitoring and defense solutions
- Automated and intelligent methods for adversary profiling
- Automated integration of analyzed data within incident response and cyber forensics capabilities

References

(All URLs valid as of October 11, 2021)

- [1] Kim-Kwang Raymond Choo, Ali Dehghantanha, Glenn Dietrich. Introduction to the Minitrack on Machine Learning and Cyber Threat Intelligence and Analytics. In Proceedings of 54th Hawaii International Conference on System Sciences (HICSS 2021). Available on <http://hdl.handle.net/10125/71476>
- [2] Kim-Kwang Raymond Choo and Ali Dehghantanha. Introduction to the Minitrack on Machine Learning and Cyber Threat Intelligence and Analytics. In Proceedings of 53rd Hawaii International Conference on System Sciences (HICSS 2020). Available on <http://hdl.handle.net/10125/64530>

- [3] Kim-Kwang Raymond Choo and Ali Dehghantanha 2019. Introduction to the Minitrack on Cyber Threat Intelligence and Analytics. In Proceedings of 52nd Hawaii International Conference on System Sciences (HICSS 2019). Available on <http://hdl.handle.net/10125/60373>
- [4] Kim-Kwang Raymond Choo and Ali Dehghantanha 2018. Introduction to the Minitrack on Cyber Threat Intelligence and Analytics. In Proceedings of 51st Hawaii International Conference on System Sciences (HICSS 2018). Available on <https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1672&context=hicss-51>

center and network management. The curriculum now includes 20 classes related to cyber security. He founded and was the first director of the Center for Infrastructure Assurance and Security (CIAS) at UTSA. His research interests include intrusion detection and security on the smart grid and data correlation and visualization. He has published in leading journals such as Decision Support Systems, Communications of the Association for Information Systems (CAIS), MISQ Executive, and IEEE Transactions on Engineering Management. Prior to joining UTSA, he worked in private industry building information systems for the government. Dr. Dietrich is a Certified Information Systems Security Professional (CISSP).

Mini-Track Chairs Biography

Kim-Kwang Raymond Choo holds the Cloud Technology Endowed Professorship at The University of Texas at San Antonio (UTSA). He is the founding co-Editor-in-Chief of ACM Distributed Ledger Technologies: Research & Practice, and founding Chair of IEEE TEMS Technical Committee on Blockchain and Distributed Ledger Technologies. He is an ACM Distinguished Speaker and IEEE Computer Society Distinguished Visitor (2021–2023), and a Web of Science's Highly Cited Researcher in the field of Cross-Field - 2020. In 2015, he and his team won the Digital Forensics Research Challenge organized by Germany's University of Erlangen-Nuremberg. He is the recipient of the 2019 IEEE Technical Committee on Scalable Computing Award for Excellence in Scalable Computing (Middle Career Researcher).

Ali Dehghantanha is an academic-entrepreneur in cybersecurity and a Canada Research Chair in Cybersecurity and Threat Intelligence. He is the director of Cyber Science Lab - a research lab dedicated to advance research and training in cybersecurity - and the director of the Master of Cybersecurity and Threat Intelligence program at the University of Guelph, ON, Canada.

Glenn Dietrich received his Ph.D. from The University of Texas at Austin, and he is currently the Professor of Information Systems and Cyber Security at The University of Texas at San Antonio (UTSA). He started the information assurance (IA) program in the College of Business at UTSA, developing an undergraduate degree in IA as well as a concentration at the master's level. He has also been responsible for developing minors in information assurance, technology management, digital forensics and data