BigCyber 2021

Workshop Chairs: Dr. Karuna Pande Joshi, Rajeev Agrawal, Sudip Mittal

Time in EST	Title	Presenter/Author
9:00 – 10:00 AM	Keynote	
10:00 – 10:20 AM	Evaluating Model Robustness to Adversarial Samples in Network Intrusion Detection (S20201)	Madeleine Schneider, David Aspinall, and Nathaniel Bastian
10:20 – 10:40 AM	Efficient and Privacy-Preserving Collaborative Intrusion Detection Using Additive Secret Sharing and Differential Privacy (S20202)	Laylon Mokry, Paul Slife, Patrick Bishop, Jose Quiroz, Cooper Guzzi, Zhiyuan Chen, Adina Crainiceanu, and Don Needham
10:40 – 11 AM	Cybersecurity Knowledge Graph Improvement with Graph Neural Networks (S20206)	Soham Dasgupta, Aritran Piplai, Priyanka Ranade, and Anupam Joshi
11 – 11:20 AM	Machine Learning Approaches for Authorship Attribution using Source Code Stylometry (S20204)	Sophia Frankel and Krishnendu Ghosh
11:20 – 11:40 AM	A Systematic Literature Review of Data Privacy Solutions for Smart Meter Technologies (S20208)	Jan Gross, Johannes Breitenbach, Waldemar Granson, Daniel Japs, Ardi Reci, Aaron Koengeter, and Ricardo Buettner
11:40 – 12 Noon	CyBERT: Contextualized Embeddings for the Cybersecurity Domain (S20207)	Priyanka Ranade, Aritran Piplai, Anupam Joshi, and Tim Finin
12 – 12:20 PM	Colab Cloud Based Portable and Shareable Hands-on Labware for Machine Learning to Cybersecurity (S20203)	Dan Lo, Hossain Shahriar, Kai Qian, Michael Whitman, and Fan Wu
12:20 – 12:40 PM	Combating Fake Cyber Threat Intelligence using Provenance in Cybersecurity Knowledge Graphs (S20205)	Shaswata Mitra, Aritran Piplai, Sudip Mittal, and Anupam Joshi
12:40 – 1 PM	Identifying Protection Motivation Theory Factors that Influence Smartphone Security Measures (BigD222)	Marvin Schneider and Shawon Rahman
1 – 1:20 PM	Detection of Newly Registered Malicious Domains through Passive DNS (BigD339)	Marcos Rogrio Silveira, Leandro Marcos da Silva, Adriano Mauro Cansian, and Hugo Koji Kobayashi
1:20 – 1:40 PM	Detection of Malicious Webpages Using Deep Learning (BigD395)	Amit Kumar Singh and Navneet Goyal
1:40 – 2 PM	Tolerating Adversarial Attacks and Byzantine Faults in Distributed Machine Learning (BigD455)	Yusen Wu, Hao Chen, Xin Wang, Chao Liu, Phuong Nguyen, and Yelena Yesha
	Closing Remarks	