ACM KDD AI4Cyber/MLHat: Workshop on AI-enabled Cybersecurity Analytics and Deployable Defense

Sagar Samtani†
Indiana University
Bloomington, IN, USA
ssamtani@iu.edu

Gang Wang
University of Illinois at
Urbana-Champaign, USA
gangw@illinois.edu

Ali Ahmadzadeh
Blue Hexagon
USA
ali@bluehexagon.ai

Arridhana Ciptadi
TruEra
USA
arridhana@gmail.com

Shanchieh Yang
RIT
Henrietta, New York, USA
Jay.Yang@rit.edu

Hsinchun Chen
University of Arizona
Tucson, Arizona, USA
hsinchun@arizona.edu

ABSTRACT

Federal funding agencies and industry entities are seeking innovative approaches to address the ever-growing cybersecurity crisis. Increasingly, numerous cybersecurity thought leaders are indicating that Artificial Intelligence (AI)-enabled analytics can help tackle key cybersecurity tasks and deploy defenses. This half-day workshop, co-located with ACM KDD, sought to attain significant research contributions to various aspects of AI-enabled analytics for cybersecurity applications and deployable defense solutions from academics and practitioners. This workshop was a joint workshop of the 2021 AI-enabled Cybersecurity Analytics and 2021 International Workshop on Deployable Machine Learning for Security Defense. As such, we developed an interdisciplinary Program Committee with significant experience in various aspects of AI, cybersecurity, and/or deployable defense.

CCS CONCEPTS

• Security and Privacy • Computing methodologies ~Artificial intelligence ~Knowledge representation and reasoning • Computing methodologies ~Machine learning ~ Machine Learning Approaches

KEYWORDS

Cybersecurity; artificial intelligence; analytics; deployable defense; machine learning

ACM Reference format:

Sagar Samtani, Gang Wang, Ali Ahmadzadeh, Arridhana Ciptadi, Shanchieh Yang, & Hsinchun Chen. 2022. ACM KDD AI4Cyber/MLHat: Workshop on AI-enabled Cybersecurity Analytics and Deployable Defense. In *Proceedings of 2022 ACM Conference Knowledge Discovery and Data Mining (KDD'22), August 14– 18, Washington DC, USA.* ACM, New York, NY, USA. 2 pages. https://doi.org/10.1145/3534678.3542894

KDD '22, August 14–18, 2022, Washington, DC, USA

ACM ISBN 978-1-4503-8332-5/21/08. https://doi.org/10.1145/3534678.3542894

1 Introduction and Workshop Objective

Despite the best efforts of academia, industry, and government, cyber-attacks are still rising at an unprecedented rate. Increasingly, many cybersecurity thought leaders are indicating that Artificial Intelligence (AI) can play a critical role in sifting through large quantities of cybersecurity data to derive valuable insights for cyber-analysts and help develop viable defense solutions [1]. To date, very promising research focused on developing AI-enabled analytics approaches for cyber threat intelligence, Security Operations Centers, disinformation and computational propaganda, and robustifying cyber-defenses [2]. However, significant opportunities remain to develop novel techniques based on the heterogeneity and velocity of cybersecurity data. Therefore, our objective for this co-convened workshop was to seek completed research papers, work in progress, and review articles from academics and practitioners on AI-enabled cybersecurity analytics and approaches for developing deployable defense solutions. Significant contributions to the half-day workshop were made in vulnerability management, malware analysis, and cybersecurity education.

2 Topics of Interest for the Workshop

This workshop sought to attain submissions about AI-enabled cybersecurity analytics [3] and deployable defense [4]. Therefore, areas of interest for this workshop included:

- Multi-lingual threat detection, key threat actor identification
- Network attack detection, classification, and analysis
- Large-scale and smart vulnerability assessment
- Real-time threat detection and categorization
- Real-time alert correlation for usable security
- Weakly supervised learning intrusion detection
- Adversarial attacks to automated cyber defense
- Automated vulnerability remediation
- Misinformation and disinformation
- Deep packet inspection
- Static and/or dynamic malware analysis and evasion
- Mapping threats to risk management frameworks
- Robustifying cyber-defense with deep reinforcement learning
- Automatic cybersecurity plan or report generation

- AI-enabled open-source software security
- Augmented intelligence for cybersecurity
- Model verdict explainability in security applications
- Privacy-preserving security data collection and sharing
- Concept drift detection and explanation
- Interactive machine learning for security
- Few-shot learning for security applications
- Resource-constrained machine learning

Similar to previous workshops, authors were encouraged to clearly summarize their data, algorithm details, performance metrics, statistical tests, and case studies in their submissions. Providing public releases of data and code was strongly encouraged to help facilitate scientific reproducibility.

3 Summary of Program Committee Members

We composed an inter-disciplinary Program Committee (PC) with significant expertise in various aspects of AI-enabled Cybersecurity Analytics and deployable defense. The PC spans both academics and practitioners. The PC members are as follows (in alphabetical order): Benjamin Ampel (University of Arizona), Hyrum Anderson (Microsoft), Mehdi Ansari (Blue Hexagon), Victor Benjamin (Arizona State University), Yidong Chair (Hefei University of Technology), Shuo Deng (Blue Hexagon), Wenbo Guo (PSU/Purdue), Apoorva Joshi (Elastic), Sven Krasser (CrowdStrike), Ben Lazarine (Indiana University), Yunji Liang (Northwestern Polytechnical University), Xiaojing Liao Indiana University, Sudip Mittal (Mississippi State University), Feargus Pendlebury (Meta/UCL), Brian Pendleton (Deloitte), Fabio Pierazzi (King's College London), Ed Raff (Booz Allen Hamilton), Ethan Rudd (Mandiant), Iris Safaka (Open Systems), Steven Ullman (University of Arizona), Binghui Wang (Illinois Institute of Technology), Ziming Zhao (University of Buffalo), Lina Zhou (UNC Charlotte), and Hongyi Zhu (UT San Antonio).

4 Background of the Workshop Organizers

The workshop organizers have extensive expertise in numerous AI for Cybersecurity analytics-related topics and lead other highly-visible AI for Cybersecurity initiatives. Each organizer's biography appears below:

- **Dr. Sagar Samtani** is an Assistant Professor and Grant Thornton Scholar of Operations and Decision Technologies at Indiana University. Dr. Samtani's research on CTI for Dark Web analytics and scientific cyberinfrastructure security have been funded by the NSF SaTC, CICI, and CRII programs. Dr. Samtani has published 50+ articles at *MIS Quarterly*, *Journal of MIS*, *ACM TOPS*, IEEE S&P, IEEE ICDM, and others.
- **Dr. Gang Wang** is an Assistant Professor of Computer Science at the University of Illinois at Urbana-Champaign. He obtained his Ph.D. from UC Santa Barbara in 2016. His research interests are Security and Privacy, and Data Mining. He is a recipient of the NSF CAREER Award (2018). His projects have been covered by media outlets such as The New York Times, Boston Globe, CNN, and ACM TechNews.
- **Dr. Ali Ahmadzadeh** is the head of the Blue Hexagon Labs. Ali leads the effort to develop state-of-the-art cybersecurity threat detection using advanced deep learning. Dr. Ahmadzadeh has more than 20 patents, and he has published in top-tier journals and conferences in communication networks and computer security. He received his Ph.D. from the University of Waterloo.
- **Dr. Arridhana Ciptadi** is a Principal Engineer at TruEra. He obtained his Ph.D. in Computer Science from Georgia Tech in 2016. His research interests are deep learning, adversarial machine learning, and cybersecurity. His work has been published in top-tier venues. His projects have been covered by media outlets such as MIT Technology Review.
- **Dr. Shanchieh (Jay) Yang** is a Professor in Computer Engineering and the Director of Global Outreach for the Global Cybersecurity Institute at Rochester Institute of Technology. His research focuses on advancing machine learning, modeling, and simulation for predictive cyber intelligence and anticipatory cyber defense. He has worked on 20+ sponsored research projects and has published 70+ peer-reviewed papers.
- **Dr. Hsinchun Chen** is a Regents' Professor of Management Information Systems at the University of Arizona. Dr. Chen is the founder and director of the Artificial Intelligence Lab, an internationally recognized research lab renowned for its research on AI cybersecurity. Dr. Chen has received over $50M of federal funding and has published 900+ papers in highly visible IEEE, ACM, and information systems venues. He is a Fellow of the IEEE, ACM, and AAAS.

ACKNOWLEDGMENTS

This workshop is based upon work funded by DGE-2038483 (SaTC-EDU), DGE-1946537 (SFS), and CNS-1850362 (CRII SaTC). We thank the authors for their contributions. We extend our appreciation to We would also like to thank each Program Committee Member for reviewing the submitted papers.

REFERENCES

[1] Elisa Bertino, Murat Kantarcioglu, Cuneyt Gurcan Akcora, Sagar Samtani, Sudip Mittal, Maanak Gupta. 2021. AI for Security and Security for AI. In *Proceedings of the 11th. ACM Conference on Data and Application Security and Privacy (CODASPY)*. ACM Press, New York, NY, 226-236. DOI: https://doi.org/10.1145/3422337.3450357

[2] Sagar Samtani, Murat Kantarcioglu, and Hsinchun Chen. 2020. Trailblazing the Artificial Intelligence for Cybersecurity Discipline. ACM Trans. Manag. Inf. Syst. 11, 4 (December 2020), 1–19. DOI: https://doi.org/10.1145/3430360

[3] Sagar Samtani, Shanchieh Yang, Hsinchun Chen. 2021. *Proceedings of the 27th ACM SIGKDD Conference on Knowledge Discovery and Data Mining (SIGKDD)*. ACM Press, New York, NY, 4153-4154. DOI: https://doi.org/10.1145/3447548.3469450

[4] Gang Wang, Arridhana Ciptadi, Ali Ahmadzadeh. 2021. *Proceedings of the 27th ACM SIGKDD Conference on Knowledge Discovery and Data Mining (SIGKDD)*. ACM Press, New York, NY, 4161-4162. DOI: https://doi.org/10.1145/3447548.3469463