CfP: AI/ML for Cybersecurity: Challenges, Solutions, and Novel Ideas at SDM '21

Submitted by Anonymous on Tue, 02/09/2021 - 6:36pm

CALL FOR PAPERS

AI/ML for Cybersecurity: Challenges, Solutions, and Novel Ideas at SDM '21

https://sites.google.com/view/ai4cs-sdm2021

AI in the cyber domain has not attracted nearly as much attention as AI in other domains. However, cybersecurity not only presents a domain in which to test the limits of AI, it affords an opportunity to protect things we all rely on. In order to advance the state of the art in AI for cyber security, there must be a greater degree of cross-pollination between cybersecurity professionals, those AI researchers/practitioners working cybersecurity, and the greater AI community. A greater collaboration among these groups is likely to be mutually beneficial. Further, these joint efforts must also span across the government, industrial sector, and academia, in order to maximize returns on investment.

This speaks to the primary aim of this workshop, which is to build a wider community of interest in AI for cybersecurity. By fostering meaningful exchanges between these groups, we hope to create new synergies that can only come through building a mutual comprehensive awareness of the problem and solution spaces. By way of our invited speakers and direct outreach with all communities across the three sectors, we shall attain adequate representation of all groups at the workshop and achieve the goals we have set.

The program will include invited presentations, submitted talks, poster sessions, and panel discussions, all designed to promote cross-community dialogue and new collaboration opportunities. The proposal, which is for a full-day workshop, would divide the program along two sessions, each containing presentations and discussions of a particular subject matter or which are part of a broader theme.

The organizers will build a program whose content is highly technical and broadly appealing to the attendees of the main conference. The invited speakers will include those actively contributing to the state of the art of AI/ML and who can provide a unique perspective on the challenges, successes, and potential of AI/ML in cybersecurity. The organizers will seek talk proposals from the wider SIAM community on related topics, in order to ensure that the workshop is broadly appealing. The program will include two panel discussions and two poster

sessions to bring additional perspectives and facilitate conversations.

Topics of interest to the organizers include, but are by no means limited to the following.

- Challenges and opportunities in data mining for cybersecurity tasks.
- Autonomous and semi-autonomous reasoning/decision making and response for defensive cyber operations or other complex domains.
- Challenges and successes of automation (non-AI/ML) capabilities on intrusion detection systems (IDS).
- Challenges and benefits of augmenting cybersecurity operations, especially automated intrusion detection systems, with AI/ML capabilities.
- Data engineering challenges in AI for cybersecurity or other complex environments.
- Novel AI/ML techniques for cyber threat discovery.
- The impact of AI/ML generated information on human decision-making (i.e. human-machine teaming effectiveness) in complex environments, such as cyber defense systems.
- Applications of realistic human cognitive behavioral modeling of complex and multifaceted problems to appropriate tasks in cybersecurity.
- Application of multi-agent and distributed/decentralized AI solutions for collaboration and competition to cyber operations
- Leveraging evolutionary and/or genetic-based AI algorithms for improved cyber defense (e.g., threat modeling, anomaly detection, automated/adaptive response)
- Exploring requirements for explainable AI/ML algorithms in cybersecurity domain.
- Automated inference from compact knowledge representations.
- Mitigations for adversarial attacks on AI/ML algorithms deployed for complex problems, such as cyber operations.
- Suitability of AI/ML for cybersecurity command and control for complicated tasks.
- Unique challenges in development and sharing of benchmark cyber data sets and cyber simulation/emulation environments for testing and validating AI/ML techniques
- Novel techniques in AI/ML applied to complex, real-world problems, such as cybersecurity, with large, highly correlated data .
- Explorations of transfer-ability of solutions, or lessons learned, between complex, open-world problems in the cyber- and non-cyber domain.

Audience

The organizers envision the audience for this workshop to be those attendees with interests in applying data science, AI, and/or machine learning to complex and data-intensive problems. This will include those already working in cybersecurity, but those working in other domains. The organizers will publicize the workshop within the cybersecurity community, especially among government sponsors, to attain a broader representation of workshop participants and attendees. We expect this group would include those whom may not have attended a SIAM conference before.

Call For Papers (Deadline: March 1)

The organizers invite participants to submit short (max 4 pgs. excluding references and supplementary material) papers to the workshop. These may include traditional research papers, position papers, and those of a more visionary character. Papers will be evaluated primarily on their relevance to the workshop topics and ability to stimulate intellectual conversations and/or healthy debate. As appropriate for the kind of submission, papers will also be evaluated on their originality, technical quality, level of insight, clarity, and potential impact.

The organizers encourage submissions which cover or are related to the workshop topics, but will consider papers of broad interest to the AI and Cybersecurity communities. Submissions must be made through the Easy Chair platform.

Depending on the number of submissions, the organizers may accept papers for either oral presentations or as part of a virtual poster session. Accepted papers will appear in an arxiv proceedings for the workshop.

Papers must be submitted by 11:59 PM AOE on March 1. Notifications will be sent by March 15. Camera-ready submissions must be ready by April 15.

Organizers

- John Emanuello, Laboratory for Advanced Cybersecurity Research
- Kimberly Ferguson-Walter, Laboratory for Advanced Cybersecurity Research
- Erik Hemberg, Massachusetts Institute of Technology- CSAIL
- Una-May O'Reilly, Massachusetts Institute of Technology- CSAIL
- Ahmad Ridley, Laboratory for Advanced Cybersecurity Research
- Dennis Ross, Massachusetts Institute of Technology- Lincoln Laboratory
- Diane Staheli, Massachusetts Institute of Technology- Lincoln Laboratory
- William Streilein, Massachusetts Institute of Technology- Lincoln Laboratory

---

? JCST CFP: Special Section on Software Systems 2021 CfP: CSF 2021 ?

Calls for Papers
