Call for Contributions

1. Inform the Chair: with the title of your contribution
2. Submission URL:
https://www.iariasubmit.org/conferences/submit/newcontribution.php?event=SECURWARE+2024+Special
Please select Track Preference as **ECSTAI**
3. Note: *For 2024, all events will be held in a hybrid mode: on site or virtual choices (live, prerecorded videos, voiced presentation slides, and .pdf slides). We hope for better times allowing us to return to the traditional on site scientific events. However, we are ready to adapt any which way the conditions dictate.*

Special track

ECSTAI: Emerging Cyber Security Threats and AI

Chairs

Adj. Prof. Dr. Fatima Hussain, Toronto Metropolitan University, Toronto, Canada
fatima.hussain@rbc.com
Sr. Lect. Dr. Rasheed Hussain, University of Bristol, Bristol, UK
rasheed.hussain@bristol.ac.uk
Adj. Prof. Dr. Salah Sharieh, Toronto Metropolitan University, Toronto, Canada
salah.sharieh@rbc.com

along with

SECURWARE 2024: The Eighteenth International Conference on Emerging Security Information, Systems and Technologies
https://www.iaria.org/conferences2024/SECURWARE24.html
November 03 - 07, 2024 - Nice, France

. We cordially invite you to participate in the special track ECSTAI, in upcoming SECUREWARE 2024 conference which focuses on the latest advancements, challenges, and solutions in Cyber Security Threats and how AI is or can be leveraged to combat these threats and attacks.

Speculating on the future of cybersecurity is inherently challenging. Cyber threat landscape is ever evolving with new attacks and so are the techniques and tools for the defense. Due to concept of global cyber-physical continuum and digitization of data and channels, organizations are relying more on virtualization, cloud services, and software as a service, to name a few. Cloud vulnerabilities, social engineering, third-party exposure risks, and insider threats have gained a significant ground during the last decade. Defending against cyber threats is a critical and ongoing process that requires an informed, intelligent, proactive, and multifaceted approach. Enterprises constantly focus upon these threats to protect their systems, assets, clients and in turns reputation. It is worth mentioning that the advancement in technology is a double-edged sword where on one hand, it helps the organizations to focus on sophisticated security solutions but on the other hand it also favors the cyber attackers. One such example is the monumental advancements in the capabilities of the Artificial Intelligence (AI) that can be both used to protect against attack but at the same time used as a tool by cyber attackers to launch security attacks. Therefore, it is essentially important to investigate the role of AI in safeguarding against overarching security attacks in critical infrastructure. The current proliferation of Generative AI (Gen AI) further reinforces the need for cybersecurity professionals, practitioners, and academics, to investigate and harness the potential of Gen AI to be used as a cornerstone in combating security attacks.
This special track aims to bring together researchers, practitioners, and industry experts to discuss and share insights on emerging cyber security threats and how AI can be used at forefront for enhancing the security, privacy, and resilience of networks, systems and digital assets. This track will focus on enabling technologies and AI and their role in both offensive and defensive security ranging from simple security

attacks to Advanced Persistent Threats (APTs) in critical infrastructure. We encourage you to submit both long, short and idea papers. Also, demos and posters on current cyber security threats and AI solutions are welcome.

Subtopics for contributions include, but are not limited to:

- Emerging security threats and countermeasures
- Insider threat detection and mitigation
- Threat hunting and incident response techniques
- Third party management and governance
- Security gamification
- Security threats and human psychology
- Security agent augmentation using Gen AI
- Gen AI and legal aspects
- Smart automated security frameworks
- Gen AI enabled security frameworks
- Data quality and Gen AI
- Machine learning and AI applications in SaaS, Third Party Risk, Social Engineering etc.
- Gen AI, Adversarial Attacks and Privacy Issues
- Security and Privacy aspects in real-world applications such as; E-health, Financial Institutions etc.
- Advanced Persistence Threats (APTs) and AI
- Enabling technologies for security of critical infrastructure
- Offensive and proactive security measures for infrastructure security
- Digital Twins in cybersecurity
- Threat intelligence and Digital Twins
- Moving Target Defense (MTD) and infrastructure security
- AI-driven red and blue-teaming for infrastructure security

Contribution Types
- Regular papers [in the proceedings, digital library]
- Short papers (work in progress) [in the proceedings, digital library]
- Posters: two pages [in the proceedings, digital library]
- Posters: slide only [slide-deck posted on www.iaria.org]
- Presentations: slide only [slide-deck posted on www.iaria.org]
- Demos: two pages [posted on www.iaria.org]

Important Datelines
Inform the Chair or Coordinator: As soon as you decide to contribute
Submission: Sep 19, 2024
Notification: Oct 6, 2024
Registration: Oct 16, 2024
Camera-ready: Oct 16, 2024
Note: *The submission deadline is somewhat flexible, providing arrangements are made ahead of time with the chairs.*

Paper Format
- See: http://www.iaria.org/format.html
- Before submission, please check and comply with the editorial rules:
http://www.iaria.org/editorialrules.html

Publications
- Extended versions of selected papers will be published in IARIA Journals: http://www.iariajournals.org
- Print proceedings will be available via Curran Associates, Inc.: http://www.proceedings.com/9769.html
- Articles will be archived in the Open Access ThinkMind Digital Library: http://www.thinkmind.org

Paper Submission

https://www.iariasubmit.org/conferences/submit/newcontribution.php?event=SECURWARE+2024+Special
Please select Track Preference as **ECSTAI**

Registration
- Each accepted paper needs at least one full registration, before the camera-ready manuscript can be included in the proceedings.
- Registration fees are available at http://www.iaria.org/registration.html

Contact
Chair
Fatima Hussain fatima.hussain@rbc.com
Logistics (Steve McGuire), steve@iaria.org