

2024 IEEE CSR Workshop on Cyber Forensics and Advanced Threat Investigations in Emerging Technologies (CFATI)

Call for Papers

Important dates

Paper submission deadline:

June 3, 2024 AoE

Authors' notification:

July 3, 2024 AoE

Camera-ready submission:

July 14, 2024 AoE

Early registration deadline:

July 20, 2024 AoE

Workshop dates:

September 2–4, 2024

Workshop chairs

Chris Lane (UK)

Preeti Patel (UK)

Ahmed Elmesiry (UK)

Organizing committee

Hafiz Malik (US)

Gabriella Marcelja (CH)

Funminiyi Olajide (UK)

Elisa Chiapponi (FR)

Technical program committee

Karim Ouazzane (UK)

Sandra Fernando (UK)

Elaheh Homayounvala (UK)

Funminiyi Olajide (UK)

Elisa CHIAPPONI (FR)

Kanaka Durga Amaravathi (IN)

Ahmed Elmesiry (UK)

Mehdi Gheisari (IR)

Hafiz Malik (US)

Gabriella Marcelja (CH)

Yugal Pathak (IN)

Sharwari Solapure Sangli (IN)

Michael Spranger (DE)

Publicity chairs

Mona Abdelgayed (UK)

Contact us

a.elmesiry@londonmet.ac.uk

The increasing proliferation of information and communication technologies (ICT) in our lives, has facilitated connectivity growth between distinct parts of our world. Various types of data are continuously streaming across many boundaries in the world with different models, policies, and purposes. This data is usually analyzed or stored on edge or gateway devices, which have limited capabilities and are vulnerable to sophisticated attacks. Recent cyberattacks dangerously target a broad array of computing systems, varying from data centers and personal machines to mobile devices and industrial control systems. There is a growing need for new methodologies, tools, and techniques, capable of extracting, preserving, and analyzing different evidence trails in various networked systems and services. Additionally, there is also a growing need for research into new systems that are capable of analyzing network traffic, netflows, and systems logs. Satisfying these demands will aid in reconstructing the timeline of the cyber-crime/attack under investigation and, possibly, the identification of the potential actor(s). Cyber forensics and threat investigations have rapidly emerged as a new research field to provide the key elements for maintaining security, reliability, and trustworthiness of the next generation of emerging technologies. Moreover, new frameworks are required to collect and preserve potential evidential data in suitable and timely manners as well. To guarantee proper cyber-defenses and strategies against the expanding landscape of criminal activities as well as rapidly advancing emerging technologies.

The workshop is held in conjunction with the IEEE CSR 2024 conference as a **hybrid event**, during September 2–4, 2024. Prospective authors are encouraged to submit previously unpublished contributions from a broad range of topics, which include but are not limited to the following:

- › Forensics and threat investigations in P2P, cloud/edge, SDN/NFV, VPN, social nets
- › Forensics and threat investigations in IoT, smart tech. (car, home, city), e/m-health
- › Forensics and visualization of big data
- › Tools and services for cyber forensics and threat investigations
- › Attack detection, traceback, attribution in emerging technologies
- › Malware analysis and attribution
- › Methods for reconstruction of digital evidence in emerging technologies
- › Security and privacy in P2P, cloud/edge, SDN/NFV, VPN, social nets
- › Security and privacy in IoT, smart tech. (car, home, city)
- › Open source intelligence (OSINT)
- › Dark web Investigations
- › Digital evidence extraction/analysis using AI/ML and data mining
- › Data exfiltration from networked devices/services (e.g. cyber-physical systems, IoT)
- › Large-scale investigations and ML for the analysis of intelligence data sets and logs

Submissions that evaluate existing research results, by reproducing experiments, are welcomed.

The CSR CFATI workshop will accept high-quality research papers presenting strong theoretical contributions, applied research and innovation results obtained from funded cyber-security and resilience projects, and industrial papers that promote contributions on technology development and contemporary implementations.

Submitted manuscripts should not exceed 6 pages (plus 2 extra pages, being subject to overlength page charges) and should be of sufficient detail to be evaluated by expert reviewers in the field. Accepted papers will be submitted for inclusion into IEEE Xplore subject to meeting IEEE Xplore's scope and quality requirements. Detailed information about paper submission and guidelines for authors can be found at the workshop's website <https://www.ieee-csr.org/2024-csr-cfati/>.