cerc 2025

The 7th International
Cybersecurity Education and Research Conference
"Intelligent Cyber Defense for a Safer Digital World"
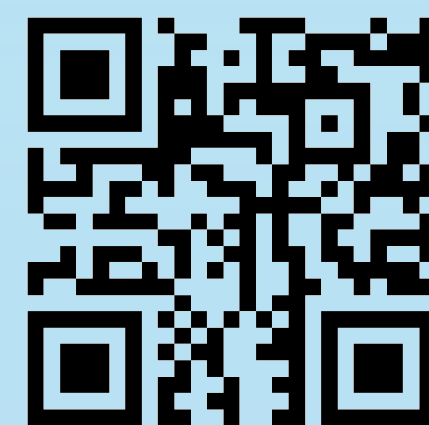
Technically Co-located with the

7th International Conference on Blockchain
Computing and Applications (BCCA 2025)

CALL FOR PAPERS

Paper Submission Deadline: August 15, 2025

https://cerc.kw/

15-16 October 2025 | KCST, Kuwait

CERC Background:

Cybersecurity Education and Research Conference (CERC) is a joint venture between Kuwait and the UK. CERC2025 supports the Kuwait-UK Memorandum of Understanding on Cyber Security signed in 2018, which points to (amongst other areas) engagement in both education and research. The conference has established traditions and is organized by the Kuwait College of Science and Technology (KCST), in partnership with the UK government, led by the British Embassy in Kuwait, and the UK Science & Innovation Network (SIN) and other organizations.

GENERAL INFORMATION

CERC 2025 is a premier international event for researchers, industry professionals, and academics dedicated to advancing cybersecurity through innovative cyber education and research. The conference will address the growing challenges and opportunities in cybersecurity across multiple domains, including secure infrastructures, intelligent threat detection, privacy-preserving systems, and cyber-resilience in emerging technologies such as IoT, AI, and blockchain. CERC 2025 aims to foster collaboration between academia and industry to shape the future of cybersecurity education, policy, and technological innovation. CERC2025 supports the Kuwait-UK Memorandum of Understanding on Cyber Security signed in 2018, which points to (amongst other areas) engagement in both education and research. The conference has established traditions and is organized by the Kuwait College of Science and Technology (KCST), in partnership with the UK government, led by the British Embassy in Kuwait, and the UK Science & Innovation Network (SIN) and other organizations. The two-day event will feature plenary sessions, technical paper presentations, and invited industrial and special sessions, offering participants a comprehensive overview of current trends and breakthroughs in cybersecurity. Accepted technical papers presented in the conference will be published at the IEEE Xplore Digital Library, which is indexed in all major indexing agencies, and selected high-quality papers may be invited for extended versions in special journal issues. You are invited to submit original research and innovative ideas in all areas of cybersecurity education, systems, applications, and emerging solutions.

Areas of focus will include:

o AI-Driven Cybersecurity
o Next-Generation Network Security
o IoT and Connected Systems Security
o Cryptography and Privacy
o Cybersecurity in Critical Infrastructure

RELATED TOPICS

Potential topics in this conference include, but are not limited to:
I. Technology and Systems
- AI and Machine Learning for Cyber Threat Detection and Response
- Cybersecurity for Next-Generation Networks (5G/6G, OpenRAN, CloudRAN)
- Security and Privacy in IoT, Smart Devices, and Edge Computing
- Blockchain and Quantum-Safe Cryptography for Secure Systems\
- Big Data Analytics and Threat Intelligence in Cybersecurity
- Cybersecurity for Critical Infrastructures and Smart Grids
- Secure Autonomous Systems, UAVs, and Vehicular Networks
- Network Security Architecture and Zero Trust Models
- Internet of Things (IoT) Security and Privacy
- Quantum-Safe Cryptography and Post-Quantum Security

II. Social and People
- Human-Centered Cybersecurity Design and Usability
- User Experience and Interaction with Security Systems
- Cyber Hygiene and Digital Literacy for End Users
- Psychological and Behavioral Aspects of Cybersecurity Awareness
- Security Education, Training, and Workforce Development
- Cultural Dimensions and Trust in Cybersecurity Practices
- Cyberbullying, Online Harassment, and Protection Mechanisms

III. Policies, Compliance, and Regulation
- Development and Enforcement of Security Policies in Organizations
- Operational Experience and Case Studies in Cybersecurity and Privacy
- Cybersecurity in Critical Infrastructure (e.g., Oil & Gas, Utilities, Transportation)
- Risk Assessment, Incident Response, and Business Continuity Planning
- Regulatory Compliance (e.g., GDPR, HIPAA, NIST, ISO Standards)
- Data Sovereignty, Governance, and Cross-Border Data Protection
- Legal and Ethical Dimensions of Cybersecurity and Surveillance
- National Cybersecurity Strategies and Public Policy

SUBMISSIONS

CERC 2025 invites the submission of original, unpublished research work that is not currently under review elsewhere.

- Full Paper: ~ 6 pages
- Short Paper: 3 pages
- Posters

Papers must be submitted through EDAS system via the conference website.

Detailed formatting and submission instructions will be available on the conference website (https://cerc.kw).

All papers must be submitted electronically, in PDF format, and uploaded to EDAS.

PRESENTATION

The accepted papers will be presented in an oral session. All accepted papers will appear in the CERC 2025 proceedings only if at least one of the authors registers for the conference to present the paper.

BEST PAPER AWARDS

CERC 2025 will present the Best Paper Awards to the authors of selected outstanding papers.

IMPORTANT DATES

- Paper Submission Deadline: 15 August 2025
- Notification of Acceptance: 15 September 2025
- Camera Ready Deadline: 20 September 2025
- Author Registration Deadline: 20 September 2025

Contact: info@cerc.kw

British Embassy Kuwait

KUWAIT COLLEGE OF SCIENCE & TECHNOLOGY
كلية الكويت للعلوم والتكنولوجيا

CARDIFF UNIVERSITY
PRIFYSGOL CAERDYDD

UK Science & Innovation Network

BCCA

IEEE Xplore® Digital Library

الجمعية الكويتية لتقنية المعلومات
Kuwait Information Technology Society