CALL FOR PAPERS

IEEE International Conference on Cyber Warfare and Security (ICCWS)

31st Mar - 2nd April, 2020

Air University E-9 Islamabad, Pakistan

Cyber Security is a rapidly growing global challenge with new sophisticated zero-day attacks costing economies billion of dollars annually. Cyber attacks may particularly affect the developed world, but developing countries are also at higher risk due to the lack of expertise and shortage of security professionals with adequate skills and experience to effectively combat the rising threats. There is a persistent need for initiatives that can produce skilled resources and carry out Research and Development (R&D) activities in the specialized areas of Cyber Security. National Centre for Cyber Security (NCCS) is an R&D initiative of Government of Pakistan to promote research and human resource development in the fields of Cyber Security. NCCS in technical co-sponsorship and joint collaboration with IEEE Islamabad Section (R-10) is organizing a three days conference event, i.e. ICCWS-2020; to invite researchers and practitioners around the World to share their original research ideas and experiences related to the state-of-the-art as well as the emerging areas of Cyber Security. ICCWS-2020 will include high-quality and focused technical program on Cyber Security with keynote talks from prominent industry and academia experts. The conference will also feature an attractive Lab-to-Market Event aimed at industry practitioners, vendors and local start-up companies.

MAIN TOPICS OF INTERESTS:

Submissions are solicited in the following areas and others closely related topics:

- Networks and infrastructure security
- Hardware and systems security
- Operating systems and software security
- Embedded systems, IoT and Cyber Physical Systems (CPS) security
- Web, Big data and Cloud security
- Edge/Fog computing and data centre security
- Information security and data provenance
- Cyber warfare
- Information assurance
- Cryptology, cryptanalysis and security analysis of cryptographic primitives and protocols
- Prevention, detection and investigation of APTs, Botnets, DDoS and other cyber attacks
- Anti-malware techniques: detection, analysis, and prevention
- Security and privacy of systems based on Machine Learning and Artificial Intelligence

- Artificial Intelligence aided security and privacy concerns
- (Adversarial) Machine learning and cyber deception
- (Anti-) Reverse engineering, side channels and physical attacks
- Protection of Digital Services
- Digital forensics, social media, networks, computer and mobile forensics
- Automated security analysis of protocols, source code and binaries
- Measurements and monitoring of human behaviour in cyberspace
- Security, Privacy, and Trust in Digital Payments and Crypto-currencies
- Security and privacy issues in Blockchain
- Security, privacy and resilience in critical infrastructures
- Testing, auditing and evaluation of security architectures and models
- 5G Security issues and architectural requirements with privacy considerations
- Energy efficient security in IoT and CPS
- Security for future Internet architectures and designs
- Authentication, Identification, Authorization and Biometrics
- Cybercrime defense (anti-phishing, anti-blackmailing, anti-fraud, etc.) techniques
- Legal Aspects of Cyber Security (Cyber Laws and Regulations)

IMPORTANT DATES:

Paper Submission Deadline: 31st January 2020
Notification of Acceptance: 29th February 2020
Camera Ready Submission: 22nd March 2020

HOW TO SUBMIT THE PAPER:

Please submit your papers at: https://easychair.org/conferences/?conf=iccs2020