ICICC-2024

5th International Conference on Innovative Computing and Communication

Organized by Shaheed Sukhdev College of Business Studies, New Delhi, India
On 16-17 February 2024

************** CALL FOR PAPERS ***************

SPECIAL SESSION ON
Artificial Intelligence in Cyber Security

SESSION ORGANIZERS:

1. **Dr. Shivi Garg, J.C. Bose University of Science & Technology, YMCA, Faridabad, India, shivi1989@gmail.com/ shivigarg@jcboseust.ac.in**
2. **Dr. Saumya Bansal, Bharati Vidyapeeth's Institute of Computer Applications and Management (BVICAM), New Delhi, India, saumya.bansal@bvicam.in**

EDITORIAL BOARD: (Optional)

1. **Dr. Chandresh Kumar Maurya, Indian Institute of Technology, Indore, India, chandresh@iiti.ac.in**
2. **Dr. Santosh Singh Rathore, IIITM Gwalior, India, santoshs@iiitm.ac.in**
3. **Dr. Sandeep Kumar, Indian Institute of Technology, Roorkee, India, sgargfec@iitr.ac.in**
4. **Dr. Niyati Baliyan, National Institute of Technology, Kurukshetra, India, niyatibaliyan@nitkkr.ac.in**
5. **Dr. Mohona Ghosh, Indira Gandhi Delhi Technical University for Women, Delhi, India, mohonaghosh@igdtuw.ac.in**
6. **Dr. Pravin Chandra, University School of Information, Communication & Technology, Delhi, India, pchandra@ipu.ac.in**

SESSION DESCRIPTION:

The cyber security techniques have gone through a rapid development in today's internet connected world. With the wide application of the booming technologies such as the Internet of things (IoT) and cloud computing, huge amount of data is generated and collected. While the data can be used to better serve the corresponding business needs, it also poses big challenges for the cyber security and privacy protection. It becomes difficult to discover the malicious behavior among the big data in real time. Thus, this gives rise to the cyber security solutions which are driven by AI-based technologies, such as machine learning, statistical inference, big data analysis, and deep learning.

AI-driven cyber security analytics has already found its applications in the next generation firewall, automatic intrusion detection system, encrypted traffic identification, malicious software detection and so on. Researchers are now assisted by the AI-driven solution to optimize the algorithm design and reduce the cryptanalysis effort. Also, automatic data protection solution based on the deep learning technology starts to appear in academia. On the other hand, individual's privacy is under threat given the AI-based systems. The rise of AI-enabled cyberattacks is expected to cause an explosion of network penetrations, personal data thefts, and an epidemic-level spread of intelligent computer viruses. This brings the concern to defend AI-driven attacks by using AI-driven techniques, which could possibly lead to an AI arms race. AI-driven security solution is among the fastest growing fields which bring together researchers from multiple areas such as machine learning, statistics, big data analytics, network, and cryptography to fight against the advanced cyber security threats.

This special session is focused on the cutting-edge research from both academia and industry, with a particular emphasis on the new tools, techniques, concepts, and applications concerning the AI-driven cyber security analytics and privacy protection.

RECOMMENDED TOPICS:

Topics to be discussed in this special session include (but are not limited to) the following:

- Machine learning attacks and defenses
- Deep learning for enhancing security and privacy
- Reliability and safety of deep learning architectures
- Adversarial examples: attacks and defenses
- Privacy issues in ML
- AI model stealing and defenses
- AI Hardware Attacks
- Robustness to hardware attacks on ML
- ML for information security
- Brain-inspired computing attacks and defenses
- Mobile software's malware analysis with deep learning
- Applications of machine learning in network security and privacy
- Automated design of cryptographic primitives
- Automated and intelligent cryptanalysis
- Automated Vulnerability Assessment/ Penetration Testing
- Cloud computing and social media security and privacy
- Cybercrime and cyberwar
- Intrusion detection/prevention systems
- Intelligent encrypted traffic identification
- Malware (Virus, Worms, Trojans, Backdoors) analysis

- Multiparty/multiagent access control
- Privacy and personal information protection

SUBMISSION PROCEDURE:

Researchers and practitioners are invited to submit papers for this special theme session on **[session name]** ***on or before*** **[30th October 2023]**. All submissions must be original and may not be under review by another publication. INTERESTED AUTHORS SHOULD CONSULT THE CONFERENCE'S GUIDELINES FOR MANUSCRIPT SUBMISSIONS at http://icicc-conf.com/paper_submission.html. All submitted papers will be reviewed on a double-blind, peer review basis.

NOTE: While submitting paper in this special session, please specify [**Session Name**] at the top (above paper title) of the first page of your paper.

* * * * * *