ICICC-2024

7th International Conference on Innovative Computing and Communication

ORGANISED BY: SHAHEED SUKHDEV COLLEGE OF BUSINESS STUDIES, UNIVERSITY OF DELHI, NEW DELHI IN ASSOCIATION WITH NATIONAL INSTITUTE OF TECHNOLOGY, PATNA & UNIVERSITY OF VALLADOLID SPAIN On 16-17th FEBRUARY 2024.

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

SPECIAL SESSION ON

Multidisciplinary Aspects of Cyber Security

SESSION ORGANIZERS:

1. **Dr. Zahid, State University of New York Polytechnic Institute, Utica, USA, akhtarz@sunypoly.edu**
2. **Dr. Shivi Garg, J.C. Bose University of Science & Technology, YMCA, Faridabad, India, shivi1989@gmail.com , shivigarg@jcboseust.ac.in**
3. **Dr. Bhawna Narwal, Indira Gandhi Delhi Technical University for Women (IGDTUW), Delhi, India, bhawnanarwal@igdtuw.ac.in**

EDITORIAL BOARD: (Optional)

1. **Prof. A.K. Mohapatra, Indira Gandhi Delhi Technical University for Women (IGDTUW), Delhi, India,** akmohapatra@igdtuw.ac.in
2. **Dr. Mohona Ghosh, Indira Gandhi Delhi Technical University for Women (IGDTUW), Delhi, India,** mohonaghosh@igdtuw.ac.in
3. **Dr. Santosh Singh Rathore, IIITM Gwalior, India, santoshs@iiitm.ac.in**
4. **Dr. Sandeep Kumar, Indian Institute of Technology, Roorkee, India, sgargfec@iitr.ac.in**
5. **Dr. Niyati Baliyan, National Institute of Technology, Kurukshetra, India, niyatibaliyan@nitkkr.ac.in**

SESSION DESCRIPTION:

The unparalleled development of Information and Communication Technology (ICT) in recent years has melded our life into the digital realm as the Internet became our daily necessity. At large, it can be started that a disconnect between personal and professional life no longer exists. Unfortunately, this interoperable global infrastructure is vulnerable to the hallmark of modern-day cyber-attacks as opportunistic threat actors just require a crack in the armor to take advantage of the lapses in cyber hygiene and their resulting damaging effects originating from surprising sources and bearings. The amalgamation of ICT in different sectors whether large or small is in the crosshairs of cyber-attacks. Relentless, well-funded, financially and criminally motivated cyber criminals with no boundaries are continuously working harder to utilize all the latest technologies for posing security challenges in front of public and private sectors around the globe to undermine their credibility through the variety and volume of cyber threats. This swift growth in sophisticated and rampant adversaries and attacks against home and business users over the last few decades has given rise to the need for stronger security defense solutions from security practitioners and vendors. Indeed, it has given rise to a lot of questions about whether a multidisciplinary approach can avert data breaches for example by using automation techniques, employing Machine Learning algorithms, and technology such as open AI. As a matter of fact, this has been the tenable reason for the researchers to meet and look more closely into the research problems upfront the Cyber Security community. Through this special session contributions can be made in the field of Cyber Security in relation to the Internet of Things (IoT), Artificial Intelligence, Wireless Networks, Metaverse, and Cyber-Physcial Systems to name a few.

RECOMMENDED TOPICS:

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

- Using machine learning to build an Intrusion detection system to detect attacks on IoT
- Optimization in IoT using genetic algorithms
- Using machine learning with the Internet of Things (IoT)
- Defense against cyber threats in IoT
- Data privacy and protection using automation techniques
- Analyzing cryptography algorithms to ensure secure communication
- Designing a security system that aligns human behavior
- Threat intelligence
- Cloud Security
- Cyber-physical system security
- Malware analysis and detection
- Biometrics and user authentication
- Adversarial attacks and defenses
- Multi-modal authentication using Artificial Intelligence
- AI-based anti-spoofing techniques
- Real-time threat detection
- Designing an AI-based authentication system that prioritizes user experience
- Privacy-preserving authentication
- Adaptive authentication
- Adversarial machine learning
- Continuous authentication using AI
- Blockchain Technology for data safety and security
- Internet of Things (IoT), and Internet of Medical Things (IoMT) security

SUBMISSION PROCEDURE:

Researchers and practitioners are invited to submit papers for this special theme session on **[Attacks and Defenses in Cybersecurity, User Authentication, and Machine Learning]** ***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 the paper in this special session, please specify [**Session Name**] at the top (above paper title) of the first page of your paper.

*** * * * * ***