

## **PakSec: International symposium on security in next generation computing technologies**

In conjunction with SpaCCS 2023

December 21 - 24, 2023, Wuhan, China

### **CALL FOR PAPERS**

This year, PakSec will be held in conjunction with the 16<sup>th</sup> IEEE International Conference on Security, Privacy, and Anonymity in Computation, Communication, and Storage (SpaCCS 2023) in Wuhan, China, on December 21 - 24, 2023.

Next generation computing technologies comprising artificial intelligence, blockchain, internet of things, big data, cyber-physical systems, next generation mobile networks, augmented and virtual reality etc. are being regarded in the evolutionary phase that will eventually revolutionize the digital landscape of the globe. The aim is to have seamless transition from humans to machines, however, there has been an increasing trend of cyber-attacks. These threats originate due to various intentions ranging from personal or national interests. Nevertheless, whatever is the intent, future computing technologies are becoming digital battleground, and there is dire need to contribute to these emerging domains. In this context, PakSec aims at complementing SpaCCS topics by providing specialized, in-depth focus on the cyber security issues in next generation computing technologies.

The focus of PakSec is on high quality research papers about state of the art in a wide range of next generation technologies:

- Security, privacy and trust in emerging AI and machine learning technologies
- Security, privacy and trust in Edge/Fog/Cloud computing
- Security, privacy and trust in AI/IoT
- Security, privacy and trust in next generation VANETS
- Security, privacy and trust in next generation web 3.0
- Security, privacy and trust in metaverse
- Security, privacy and trust in protocols for next generation networks
- Security, privacy and trust in intrusion detection system for future computing

**Proceedings:** Accepted and presented papers will be submitted to the IEEE for indexing. Best papers, after further revisions, will be invited for possible publication in the special issues:

**Submission and Publication Information:** All papers need to be submitted electronically through the submission website using PDF format. Submitted papers must be clearly presented in English, not substantially overlap with papers that have been published or that are simultaneously submitted to a journal or a conference with proceedings.

Papers will be selected based on their originality, significance, relevance, and clarity of presentation assessed by at least two reviewers. Submission of a paper should be regarded as a commitment that, should the paper be accepted, at least one of the authors will register and attend the conference to present the work. PakSec-2023 reserves the right to exclude a paper from distribution after the conference (e.g., removal from the digital library and indexing services), if the paper is not presented at the conference.

A submission is limited to 6 pages in workshop or short papers in the IEEE Computer Society Proceedings Format. A submission can have at most 4 additional pages with the pages overlength charge if accepted. Papers must be clearly presented in English, including tables, figures, references and appendices.

## **IMPORTANT DATES**

Paper submission deadline: August 15, 2023

Author notification: September 25, 2023

Camera-Ready paper due: October 20, 2023

Symposium Date: December 21 - 24, 2023

### **Workshop Chairs:**

Mukhtaj Khan,  
PhD, Professor,  
The University of Haripur, Pakistan,  
[mukhtaj.khan@uoh.edu.pk](mailto:mukhtaj.khan@uoh.edu.pk)

Ateeq ur Rehman  
PhD, Associate Professor,  
The University of Haripur, Pakistan,  
[ateeq@uoh.edu.pk](mailto:ateeq@uoh.edu.pk)

Muhammad Faizan Khan  
PhD, Postdoc Fellow  
Guangzhou University, China  
[faizan@gzhu.edu.cn](mailto:faizan@gzhu.edu.cn)