# Call for Papers

## Track 7 – Security, Privacy, and Content Protection

### Track Chairs:

Shamik Sengupta, University of Nevada, Reno, USA (email: ssengupta@unr.edu)
Kiho Lim, William Paterson University of New Jersey, USA (email: limk2@wpunj.edu)

### Scope and Motivation:

IEEE CCNC 2024 Security, Privacy, and Content Protection Track is dedicated to exploring and discussing the most recent advancements and state-of-the-art technical solutions in the dynamic and ever-evolving field of cybersecurity and privacy protection. As technology advances, the need to address emerging threats and safeguard sensitive information becomes increasingly critical. This track encourages the submission of high-quality research contributions that push the boundaries of knowledge and demonstrate significant advancements in the field. It seeks to showcase cutting-edge research that addresses emerging threats, tackles existing security and privacy challenges, and presents novel solutions that can be deployed in real-world scenarios.

### Main Topics of Interest:

The scope of this track covers practical and theoretical submissions describing novel contributions on a wide range of topics, including:

- Anonymity and privacy-enhancing technologies
- Applied cryptography for network, information, and cyber security
- Authentication, authorization, and auditing for content protection
- Blockchain security and privacy
- Botnet analysis and detection
- Computer and network forensics
- Consumer-friendly and usable security and privacy tools
- Control of personal data & privacy protection
- Digital rights management & copyright protection
- Exploit writing, mitigation bypass techniques
- Firewalls and intrusion detection
- Internet measurements for network security and security monitoring
- Malware detection and recovery
- Network infrastructure security
- Personal, portable, and wearable device security
- Privacy-preserving mechanisms for distributed computing
- Privacy-preserving mechanisms for autonomous systems
- Phishing and spam detection and defense
- Reputation and trust management mechanisms
- Security and privacy in WiFi and Home Networks
- Security and privacy in cellular and mobile networks
- Security and privacy in cloud and edge computing
- Security and privacy in crowdsourcing
- Security and privacy in emerging wireless technologies and applications (e.g., short-range communications, personal/body-area networks, mmWave communications, smart/connected vehicles, UAS, etc.)
- Security and privacy in IoT, industrial IoT, smart cities, smart and connected health, and RFID systems
- Security and privacy in social networks
- Security and privacy in software-defined networking and content-centric networking
- Security and privacy in spontaneous networking
- Web, e-commerce, m-commerce, and e-mail security
- Worm and malware detection and defense