Title: *AI-Driven Cybersecurity: Innovations, Challenges, and Future Directions*

Session Description:

As digital transformation accelerates, cybersecurity has become a critical concern for enterprises, governments, and individuals. The integration of Artificial Intelligence (AI), Machine Learning (ML), and Deep Learning (DL) in cybersecurity has led to the development of autonomous threat detection systems, intelligent security analytics, and real-time response mechanisms. However, alongside these advancements, cyber threats have also evolved, leveraging AI for sophisticated attacks such as adversarial ML, AI-powered malware, and deepfake-based social engineering.

This special session will focus on cutting-edge research and practical applications of AI in cybersecurity, discussing innovations, challenges, and future directions. It aims to bring together researchers, academicians, and industry professionals to share their insights and latest findings in AI-driven security strategies, ethical AI, and the role of AI in combating emerging cyber threats.

Topics of Interest (but not limited to):

- **AI-Powered Threat Detection:**
  - Machine Learning for anomaly detection and intrusion prevention
  - Deep Learning models for malware analysis and classification
  - AI-based behavioral profiling for fraud detection
- **Adversarial Machine Learning in Cybersecurity:**
  - Techniques for evading AI-based security solutions
  - Defense mechanisms against adversarial AI attacks
  - Explainable AI (XAI) in cybersecurity
- **Blockchain and AI for Secure Computing:**
  - AI-enhanced blockchain security solutions
  - Decentralized identity management and authentication
  - Smart contract security with AI
- **Cybersecurity in IoT and Edge Computing:**
  - AI-driven security frameworks for IoT devices
  - Edge AI for real-time threat mitigation
  - Secure federated learning in distributed environments
- **Digital Forensics and AI:**
  - AI-assisted forensic analysis of cyber incidents
  - Deepfake detection and AI-driven misinformation countermeasures
  - AI-powered network traffic analysis for forensic investigations
- **Privacy-Preserving AI and Secure Data Analytics:**
  - Differential privacy in AI models
  - AI-based techniques for secure multi-party computation
  - Privacy-preserving federated learning
- **AI and Human-Centric Cybersecurity:**
  - AI-driven phishing detection and social engineering prevention
  - User authentication and biometrics with AI
  - AI-powered security awareness training

Session Objectives:

- To explore AI's role in enhancing cybersecurity frameworks and threat intelligence.
- To discuss the challenges and solutions in AI-based security mechanisms.
- To present real-world applications of AI in cybersecurity across industries.
- To foster collaborations between AI researchers and cybersecurity professionals.

Target Audience:

This session is designed for AI researchers, cybersecurity experts, data scientists, industry professionals, government agencies, and academicians working at the intersection of AI and security.

Session Chair:

Dr. Keshav Kaushik
(Center for Cyber Security and Cryptology, Sharda School of Computer Science & Engineering, Sharda University, Greater Noida, India)
Email ID: officialkeshavkaushik@gmail.com