INTERNATIONAL CONFERENCE ON

Data-Driven Insights for National Security (DINS-2026)

Exploring AI and Statistical Frontiers in India's Socio-Cultural Landscape

(30th – 31st March 2026)

DINS-2026 Special Session on

"From AI Products to AI Defense: Building Cyber-Resilient Systems for the Future"

Aims and scope of the session:

This session shows how the principles used to build secure and trustworthy AI products can be directly applied to create advanced AI driven cyber defenses. It focuses on designing AI systems that are secure from the ground up, resilient under attack, and capable of detecting, predicting, and responding to threats in real time. By connecting practical AI product building experience with real cybersecurity needs, the session highlights how strong data pipelines, protected models, adversarial-aware design, and automated threat intelligence form the foundation of next generation security architecture. Attendees will learn how to engineer AI systems that not only survive attacks but actively reinforce overall security, leading to adaptive, self-healing, and future ready digital defenses.

Topics of interest:

1. Secure-by-Design AI Systems.
2. AI Driven Threat Detection & RealTime Anomaly Monitoring.
3. Adversarial Defense and Model Protection.
4. Automated Threat Intelligence and Response.
5. Building Resilient, Self-Healing Cyber Systems.

Special session organizers:

1. **Nikhila Racha**

   Software Engineer - Senior Consultant, Visa

   nikhilareddy58@gmail.com, +1 4258645536