Report on AI Security Summer Training Program – 2025

The Departments of Electrical & Electronics Engineering (EEE) and Information Technology (IT) at Maharaja Agrasen Institute of Technology (MAIT), in collaboration with CRAC Learning, successfully organized a six-week Summer Training Program on Artificial Intelligence Security. The program was held from June 23 to August 1, 2025, and aimed to equip students with practical skills and conceptual understanding in AI Security.

The hybrid-mode training program (online and offline) offered structured lab sessions, expert talks, and engaging assignments to provide students with immersive, real-world experience. The initiative emphasized the significance of secure AI systems in modern engineering and technology.

Key Highlights

• Duration: 6 Weeks (June 23 – August 1, 2025)

• Mode: Hybrid (Online and Offline)

• Organizer: EEE & IT Departments, MAIT

• Industry Partner: CRAC Learning, led by Ms. Swati Laxmi

• Format: Technical lectures, lab sessions, demo showcases, expert interactions, and certification

• Participants: 21 including 1 External Participant from Outside India

Summary of Weekly Themes

• Week 1: Introduction to Artificial Intelligence and Python Programming

• Week 2: Machine Learning Concepts and Model Development

• Week 3: Introduction to Cybersecurity and Network Threats

• Week 4: Adversarial Attacks, Malware Analysis, and Secure AI Techniques

• Week 5: Real-World Applications and Hands-on Projects

• Week 6: Final Demos, Project Presentations, and Certificate Distribution

Acknowledgements

We express our sincere gratitude to the esteemed leadership and faculty members whose guidance and support made this program a resounding success:

• Dr. Nand Kishor Garg – Founder Chairman

• Dr. Subodh Jindal

• Shri Rajneesh Gupta

• Prof. J.V. Desai

• Prof. S.S. Deswal

• Prof. Sachin Gupta

• Ms. Swati Laxmi – Founder, CRAC Learning

Program Coordinators:

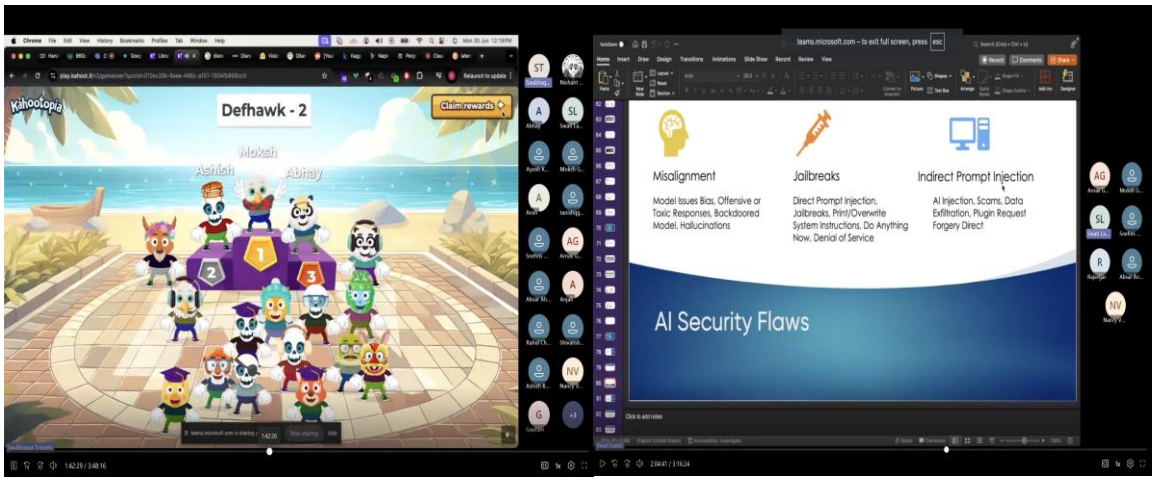
• Dr. Monika Gupta – Head of Department, EEE

• Prof. Amita Goel – Head of Department, IT

• Ms Monika Bhardwaj – Assistant Professor, EEE

• Dr Vasudha Bahl – Associate Professor, IT

The AI Security Summer Training Program – 2025 was a pioneering effort to foster future-ready engineers with a strong foundation in AI technologies and cybersecurity. The enthusiastic participation, expert mentorship, and successful outcomes of this initiative reflect the commitment of MAIT towards academic excellence and technological advancement.


Kahootopia
Defhawk - 2
Claim rewards
Moksh
Ashish
Abhay
Misalignment
Model Issues Bias, Offensive or Toxic Responses, Backdoored Model, Hallucinations
Jailbreaks
Direct Prompt Injection, Jailbreaks, Print/Overwrite System Instructions, Do Anything Now, Denial of Service
Indirect Prompt Injection
AI Injection, Scams, Data Exfiltration, Plugin Request Forgery Direct
AI Security Flaws