J.B. INSTITUTE OF ENGINEERING & TECHNOLOGY

(UGC AUTONOMOUS)
Accredited by NBA & NAAC
Bhaskar Nagar, Moinabad Mandal, R.R. District, Hyderabad -500075

REPORT ON

MIC-driven Activity "AI for Atmanirbhar Bharat: HEI Pre-Summit Engagements"

Theme:

Safe and Trusted AI

Topic:

Advanced Defensive Strategies Against Adversarial Machine Learning Atacks in Critical Infrastructure Application

Technical event Organized By

Electronics and Computer Engineering Department

Date: 31st January 2026

Venue: Room No. 406, ECM, Admin Block, JB Institute of Engineering & Technology

Mode: Offline

Faculty Coordinators: Mrs. Kiran Pakmode, Assistant Professor, ECM

TABLE OF CONTENTS

1. INTRODUCTION

The seminar on " Advanced Defensive Strategies Against Adversarial Machine Learning Attacks in Critical Infrastructure Application " was organized to create awareness among students about the growing environmental impact of large-scale AI systems. With the rapid expansion of deep learning models, energy consumption and carbon emissions have become major concerns. The session emphasized sustainable AI practices and responsible model design.

2. OBJECTIVES

- Raise awareness of adversarial ML threats in critical infrastructure.
- Explain common attack vectors (evasion, poisoning, adversarial inputs).
- Present advanced defensive strategies and resilience frameworks.
- Share best practices, case studies, and industry standards.
- Encourage collaboration among researchers, practitioners, and policymakers.
- Inspire innovation in trustworthy and robust AI systems.

3. EVENT REPORT

DR. Akheel Mohammed, Associate Professor, AIML Department delivered an insightful session on Advanced Defensive Strategies Against Adversarial Machine Learning Attacks in Critical Infrastructure Applications focuses on strengthening the resilience of AI systems that power essential services such as energy, healthcare, transportation, and finance. It begins by outlining the threat landscape, where adversarial attacks like evasion, poisoning, and model manipulation can compromise reliability and safety. The discussion then moves to advanced defensive approaches, including robust training methods, anomaly detection, adversarial input filtering, and resilience frameworks designed for mission-critical environments. Case studies and industry standards are highlighted to provide practical insights into secure ML deployment. The session emphasizes collaboration among researchers, practitioners, and policymakers to build collective defense strategies, while also encouraging innovation in trustworthy, transparent, and robust AI systems to ensure the long-term security of critical infrastructure.

4. SPEAKER PROFILE

DR. Akheel Mohammed, Associate Professor, AIML Department with extensive experience in Artificial Intelligence and Data Science. His research interests include an ensemble of evolutionary algorithms Based data analytic tools for distributed big data systems in Cloud environment

5. PARTICIPANTS

2nd year and 3rd year students participated.

6. OUTCOMES& KEY HIGHLIGHTS

- Gain awareness of adversarial ML risks in critical infrastructure.
- Identify and understand key attack methods (evasion, poisoning, manipulation).
- Learn advanced defensive strategies and resilience techniques.
- Apply best practices and standards for secure ML deployment.
- Analyze case studies to connect theory with real-world applications.
- Strengthen collaboration across research, industry, and policy domains.
- Develop capacity to innovate trustworthy and robust AI systems.

7. FEEDBACK

□ **Gowthami (II Year, ECM):** - The defensive strategies discussed were practical and relevant for future research and industry use

□ **Mohan (III Year, ECM):** The session gave us clear insights into how adversarial ML attacks can disrupt critical infrastructure.

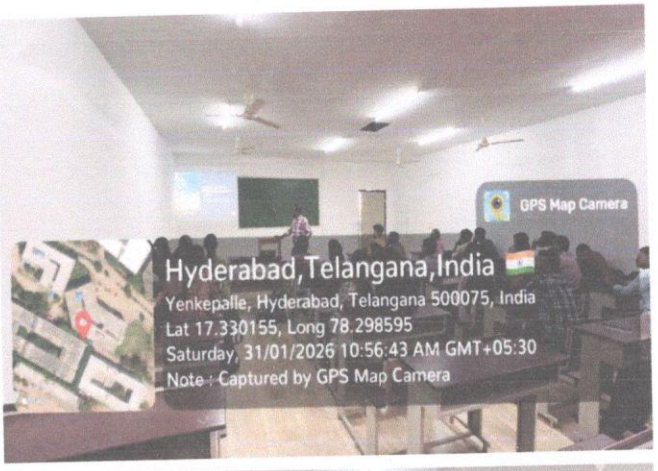
□ **Likhita (III Year, ECM):** - The session inspired us to think about innovative approaches for building robust and trustworthy AI systems.

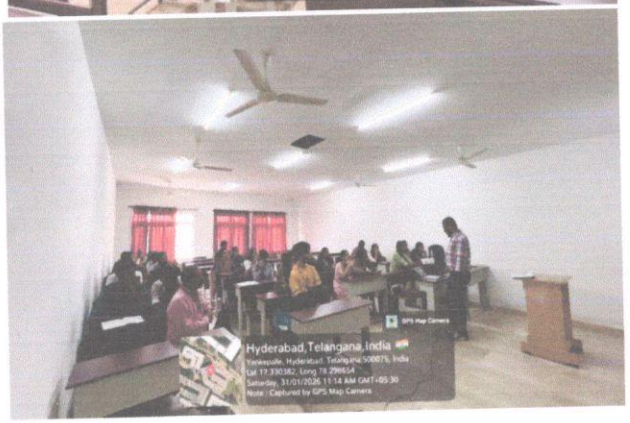
□ **Sashank (III Year, ECM):** Overall, it was engaging, informative, and strengthened our understanding of AI security in mission-critical contexts.

8. CONCLUSION

The session on Advanced Defensive Strategies Against Adversarial Machine Learning Attacks in Critical Infrastructure Applications underscores the urgent need to safeguard AI systems that power essential services. By examining the threat landscape, exploring advanced defensive mechanisms, and learning from real-world case studies, participants gain a holistic understanding of both the risks and the solutions. The discussion highlights that technical defenses alone are not enough—collaboration across research, industry, and policy domains is vital to building resilient systems. Ultimately, the session concludes with a call to action: to innovate and implement trustworthy, transparent, and robust AI strategies that ensure the security and reliability of critical infrastructure in the face of evolving adversarial threats.

9. EVENT PHOTO GALLERY





Head of the Department
Dept. of ECM
J.B Institute of Engineering & Technology
Bhaskar Nagar, Yenkapally (V)
Moinabad (M), R.R. Dist.- 500 075