REPORT

on

Faculty Development Program

on

"Stepping into Emerging Technologies with a Practical Approach: Cybersecurity and AI/ML"

(22 January 2025 to 27 January 2025)

K.R. MANGALAM UNIVERSITY, GURUGRAM

TABLE OF CONTENTS

Sr. No.	Contents	Page Number
1	Introduction including topic	
2	Report of the Session Conducted (Session wise - Day wise)	
3	Faculty Feedback	
4	Annexure I – Broacher	
5	Annexure II – Minute-to-Minute FDP Schedule	
6	Annexure III – Attendance	
7	Annexure IV – FDP Sample Certificate	
8	Annexure V – FDP Grade Certificate	
9	Annexure VI – FDP Feedback	
10	Annexure VII- Geo tagged Photographs	

REPORT ON FACULTY DEVELOPMENT PROGRAMME ON

"Stepping into Emerging Technologies with a Practical Approach: Cybersecurity and AI/ML"

1. Introduction

The Centre of Excellence -AI, School of Engineering and Technology, organized the Faculty Development Program (FDP) titled "Stepping into Emerging Technologies with a Practical Approach: Cybersecurity and AI/ML" aimed to provide faculty members with in-depth knowledge and practical exposure to the fields of cybersecurity and Artificial Intelligence/Machine Learning (AI/ML). In collaboration with E&ICT Academy, IIT Guwahati, the six-day program was structured to ensure a comprehensive learning experience through theoretical and hands-on sessions. The primary objective was to empower educators to integrate emerging technologies into their academic and research practices, bridging the gap between academia and industry.

There were total 48 external as well as internal participants. The schedule of the FDP has been enclosed.

2. Day-wise Report of the Sessions Conducted

Day 1: Inaugural Session & Fundamentals of Cybersecurity:

The inaugural session began with Saraswati Vandana followed by welcome remarks from dignitaries. Dr. Bibhudendra Acharya introduced the fundamentals of cybersecurity, covering principles, threats, and vulnerabilities. He discussed key domains such as network security, information security, and cloud security. He further explained the role of cryptography, lightweight cryptography, and secures communication protocols in cybersecurity.



Fig. 1: FDP Inaugural Session



Fig. 2: Participants addressed by Dr. Bibhudendra Acharya

Day 2: Fundamentals of AI/ML & Hands-on Practice Dr. Ajay Singh Raghuvanshi introduced AI/ML fundamentals, covering AI, ML, and DL basics, their differences, and applications in cybersecurity. He discussed supervised, unsupervised, and reinforcement learning paradigms with practical examples in cybersecurity. The session included a hands-on practice session and Quiz-1.



Fig. 3: AI/ML Fundamentals Session



Fig.4: Dr. Ajay Singh Raghuvanshi explaining supervised learning techniques

Day 3: Role of Image Techniques in Cybersecurity Dr. Bibhudendra Acharya explained image encryption, watermarking, and attack analysis techniques for ensuring data authenticity. He covered ethical and legal considerations in AI/ML for cybersecurity, including GDPR and CCPA regulations. The session concluded with practical exercises.



Fig.5: Session by Dr. Bibhudendra Acharya explaining anomaly detection

Day 4: Types of Cybersecurity Attacks and IDS

Dr. Ajay Singh Raghuvanshi explained various types of cybersecurity attacks such as DoS, DDoS, SQL Injection, and MITM. He elaborated on Intrusion Detection Systems (IDS), their types, and detection strategies.

Advanced topics, including neural networks and predictive models for cybersecurity, were covered by Dr. Ajay Singh Raghuvanshi. Practical sessions conducted by Mr. Ankit Singh allowed participants to build and train neural network models.The session concluded with hands-on practice and Quiz-2.



Fig. 6: Dr. Ajay Singh Raghuvanshi explaining predictive models

Day 5: Emerging Technologies in Cybersecurity using AI/ML

Dr. Bibhudendra Acharya and Dr. Ajay Singh Raghuvanshi covered automated threat hunting, malware classification, and vulnerability management. They introduced federated learning in cybersecurity and adversarial attacks. The session concluded with hands-on activities and a valedictory session.

The final day focused on integrating AI/ML technologies with real-world cybersecurity challenges. Dr. Ajay Singh Raghuvanshi discussed ethical considerations in AI-driven cybersecurity and introduced participants to cutting-edge tools and frameworks. Practical exercises led by Mr. Ankit Singh allowed attendees to implement end-to-end solutions for simulated cybersecurity scenarios. Ms. Nitishmita Kalita ensured smooth coordination throughout the day.



Fig. 7: FDP Participants

Valedictory Session The program concluded with participants sharing their experiences, followed by certificate distribution and concluding remarks by Deans.

3. Key Outcomes

Participants gained practical skills in applying AI/ML technologies to cybersecurity challenges. They expressed increased confidence in leveraging these tools for teaching and research purposes. The interactive sessions fostered a collaborative learning environment, encouraging knowledge-sharing among attendees. The program also highlighted the potential for further exploration of advanced topics such as blockchain, deep learning, and specialized tools for cybersecurity.

4. Conclusion and Further Scope

The FDP successfully achieved its objective of equipping faculty members with the knowledge and skills necessary to integrate emerging technologies into their professional roles. Participants recommended conducting advanced-level programs focusing on specific domains such as deep

learning, ethical AI, and advanced cybersecurity measures. This feedback underscores the ongoing demand for professional development opportunities in these rapidly evolving fields.

Poster of the FDP:

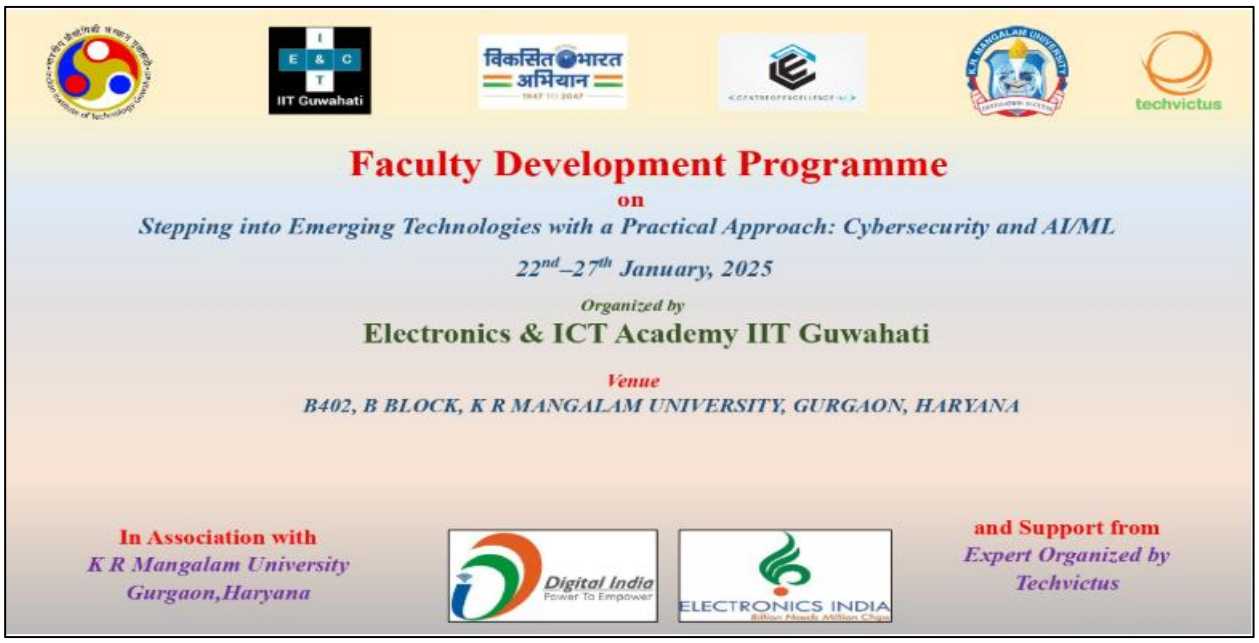


Fig. 8: Poster

Sample Certificates:

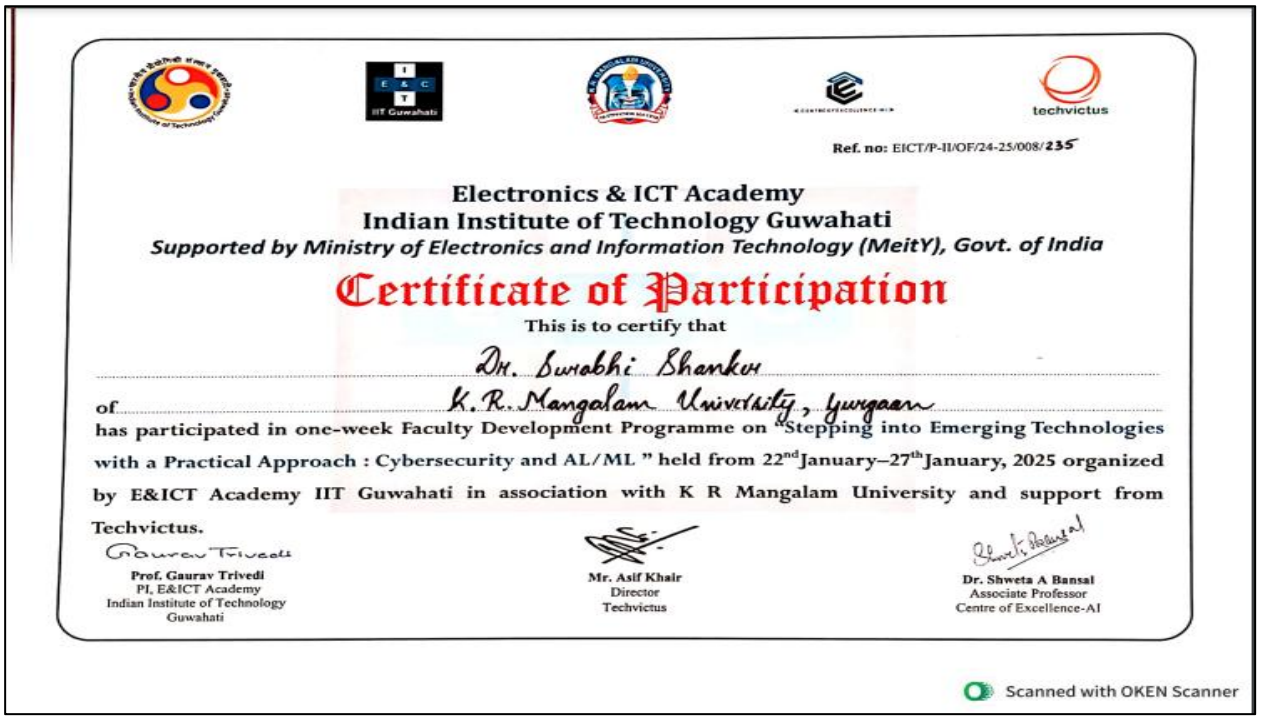


Fig. 9: Sample Certificate