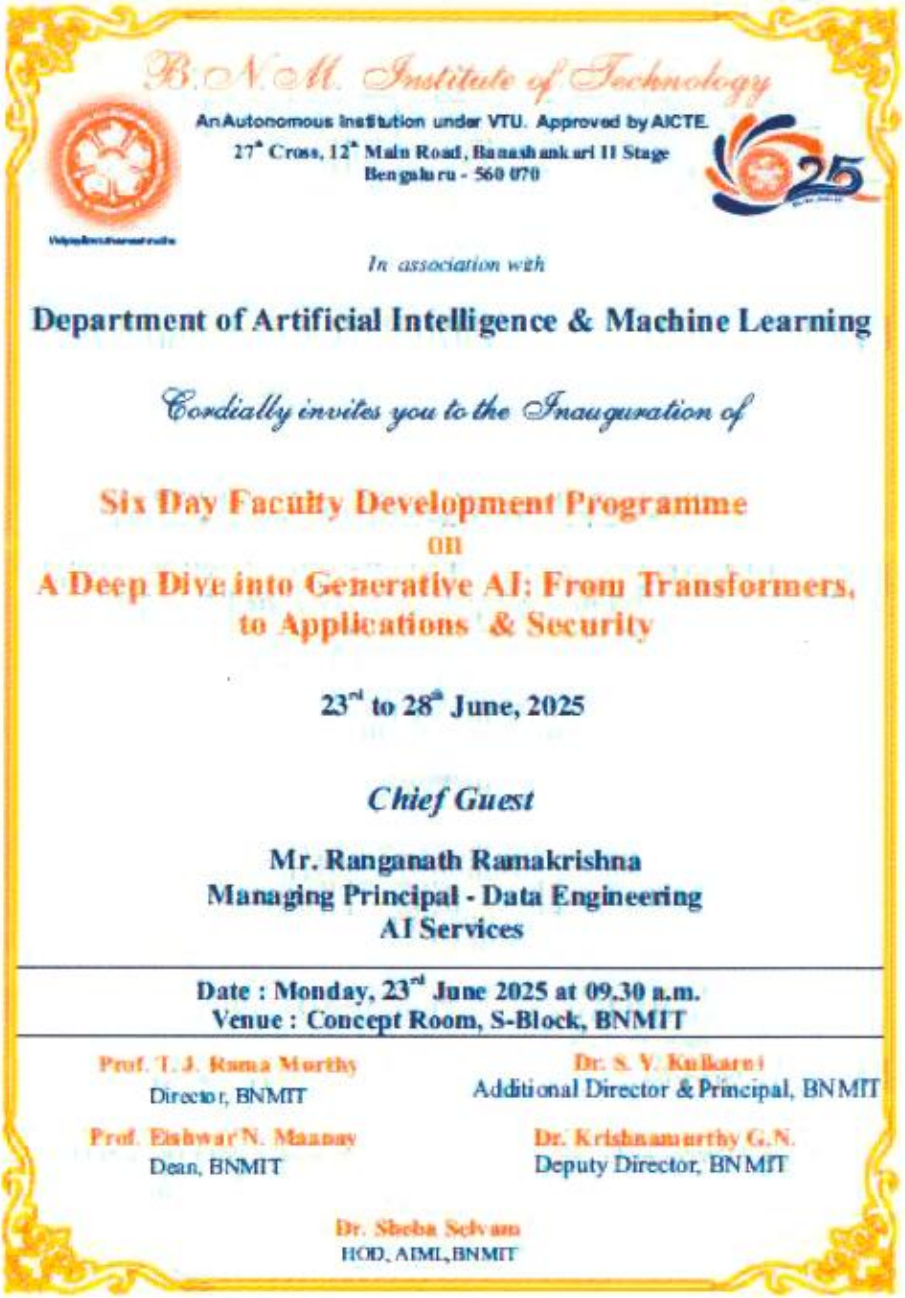
K.S. INSTITUTE OF TECHNOLOGY, BANGALORE

#14, Raghuvanahalli, Kanakapura Main Road, Bengaluru-5600109

DEPARTMENT OF ARTIFICIAL INTELLEGENCE AND MACHINE LEARNING

Report on Faculty Development Program on 23rd to 28th JUNE 2025 On

"A Deep Dive into Generative AI: From Transformers to Applications & Security"



Day 1: Monday, 23rd June 2025

Program Overview:

The first day of the Faculty Development Programme (FDP) commenced with **registration** at **9:30 AM**, followed by the **inaugural ceremony** at **10:00 AM**. The participants were welcomed with an opening speech, setting the stage for a week-long exploration of GEN AI from Transformers to Applications to Security

Session I: Keynote Address

Title: "Understanding Transformers: The Backbone of Large Language Models"

Resource Person. Dr. Shrirang Kulkarni, Associate Professor School of Computer Science Manipal Institute of Technology (MIT), Bengaluru,

Dr. Shrirang Kulkarni delivered an insightful talk on the potential of GEN AI. He covered Transformers revolutionized language AI by enabling **parallel, context-rich processing** via attention mechanisms. From powering ChatGPT, BERT, and GPT-4 to redefining fields from vision to biology, they've become the dominant architecture across AI. Despite resource demands and interpretability challenges, innovations continue—extending context length, efficiency, and reasoning capabilities.

Session II: Hands on Session on Transformers in LLM

Resource Person: Dr. Shrirang Kulkarni, Associate Professor School of Computer Science Manipal Institute of Technology (MIT), Bengaluru,

The session began with a conceptual explanation of the transformer model, detailing key mechanisms like self-attention, encoder-decoder architecture, and how transformers differ from RNNs and CNNs.: Participants engaged in practical exercises:

Hands-on Exercise

- Fine-tuning BERT for sentiment analysis.
- Running inference on text inputs using GPT-style models

Day 2: Tuesday, 24th June 2025

Session III:

Theme: Word Embeddings and Evaluation Benchmarks in Large Language Models: Concepts, Techniques, and Metrics"

Resource Person: Mr. Joel Data Scientist -AI Center of Data for Public Good IISC, Bengaluru

A session on Word Embeddings and Evaluation Benchmarks in Large Language Models (LLMs) was conducted to explore foundational concepts in language representation and the methodologies used to evaluate the effectiveness and performance of LLMs. The session was designed to blend theoretical insights with practical frameworks for understanding how models learn and represent language. The session was informative and well-structured, with a strong emphasis on both theory and practical utility. Participants appreciated the clarity of explanations and the relevance of the hands-on components. Several expressed interest in deeper dives into model interpretability and bias mitigation strategies in future sessions.

Session IV: Hands on Session on"Prompt Engineering, Building LLM Ontology, Name Entity Recognition"

Resource Person: Mr. Joel Data Scientist -ICenter of Data for Public Good IISC, Bengaluru

A comprehensive hands-on session was conducted on Prompt Engineering, Building LLM Ontologies, and Named Entity Recognition (NER) to equip participants with practical skills and foundational knowledge in working with Large Language Models (LLMs). The session focused on how LLMs can be guided effectively through prompts, structured through ontologies, and applied in information extraction tasks.

Hands-on Activities:

- Using OpenAI's GPT or similar LLMs via API or playgrounds
- Designing prompts for summarization, translation, sentiment analysis, and question answering
- Prompt refinement and performance comparison

Day 3: Wednesday, 25th June 2025

Session V

Theme: "Gen AI to generate Image"

Resource Person: Dr. Shreekant Jere Decision Science Practitioner Associate Manager, Accenture AI

Session on "Generative AI to Generate Images" was organized to introduce participants to the capabilities of generative artificial intelligence in visual content creation. The session covered fundamental concepts of generative models, with a focus on how advanced AI systems can create realistic, creative, or synthetic images from text prompts or other data input. Speaker also covered topics like., Ethical and Responsible Use

- Deepfakes, misinformation, and copyright concerns
- Use of watermarks and attribution
- Respecting community guidelines and model usage policies

Session VI: End to End Video Summarization with Gen AI: Leveraging Phi data and Gemini LLM lore Topic

Resource Person: Dr. Shreekant Jere Decision Science Practitioner Associate Manager, Accenture AI

Participants expressed enthusiasm about the hands-on experience and were amazed by the creative potential of AI image generation. Many appreciated the opportunity to experiment with live tools and better understand how text can be translated into powerful visual outputs.

. Hands-on Demonstration

- Live walkthrough of generating images from text using:
- OpenAI's DALL·E (via ChatGPT or API)
- Crafting effective prompts: descriptive language, style hints, modifiers
- Modifying and refining outputs based on user feedback and prompt tweaks

Day 4: Thursday, 26th June 2025:

Session VII: Industrial visit To LTI Mindtree, Bengaluru

Resource Person: Mr. Ranganath Sharma, Managing Principal -Data Engineering AI Services LTI Mindtree

Industrial visit to LTI Mindtree in Bengaluru isn't just a one-off event—it's a window into: How large IT consultancies operate end-to-end. Participants explored various technologies being used in AI industry. Participants gained exposure to the company's extensive service portfolio—including Agile methodologies, Analytics & Information Management, Application Dev & Maintenance, Enterprise & Infrastructure solutions, Testing, Digital Engineering, and Platform-based offerings The visit is typically anchored by HR leads and senior technical architects offering direct Q&A opportunities about hiring, training, and project culture.

1. Deep Insight into LTI Mindtree's Core Services
2. Exposure to Emerging Tech in Actio
3. Direct Engagement with Industry Leaders
4. Bridging Classroom Knowledge with Industry Practice
5. Networking & Mentorship Prospects

Such visits often open doors for future interactions—think internship opportunities, mentorship from technical experts, or panel discussions guiding career paths

Day 5: Friday, 27th June 2025

Session VIII: "Open AI, RAG, Serving LLMs Locally "

Resource Person: Mr. Arun, Data Scientist I- Center of Data for Public Good IISC, Bengaluru

Participants gained knowledge about Open AI, RAG and LLM. OpenAI is a leading AI research and deployment company focused on developing safe and useful artificial general intelligence (AGI). Founded in 2015, OpenAI is known for creating cutting-edge language models, including:GPT-3.5 and GPT-4: Generative pre-trained transformers capable of natural language understanding and generation.GPT-4o (2024): A multimodal model with real-time vision, audio, and text capabilities.ChatGPT: A user-facing application that leverages OpenAI's models, widely adopted for productivity, coding, writing, and creative tasks.API & Platform Tools: OpenAI offers its models via API and integrations (e.g., Microsoft Copilot, ChatGPT Team/Enterprise).

Session IX: Hands-On Topic "Agentic AI, Anthropic Model Content Protocol (MCP), Langchain "

This session introduced the principles of Agentic AI and real-world use cases.Demonstrate how Anthropic's Model Content Protocol (MCP) can be applied for content safety and compliance.Build an agentic workflow using LangChain, with LLM tool use and dynamic decision-making.Explored responsible deployment of AI using safety checks and RAG integration.

- ◈ Part 1: Build a Simple LangChain Agent
- ◈ Part 2: Introduce Retrieval-Augmented Generation (RAG)
- ◈ Part 3: Simulate Anthropic's MCP (Model Content Protocol)

Results & Outcomes

- ☑ Successfully built tool-using agents that respond intelligently
- ☑ Added RAG layer to provide grounded answers
- ☑ Simulated content moderation using LLM filters (MCP principles)
- ☑ Discussed practical agent deployments and limitations

Day 6: Saturday, 28th June 2025

Session X: Exploring LLM Vulnerabilities

Resource Person: Mr. Gajendra Deshpande Managing Director, Theta Dynamics Private Limited

Large Language Models (LLMs) like GPT-4, Claude, Gemini, and open-source models (e.g., LLaMA, Mistral) are increasingly integrated into real-world applications—from customer support and legal automation to healthcare and finance. However, LLMs can exhibit vulnerabilities that may be exploited for harmful purposes, misused unintentionally, or result in compliance breaches

Categories of LLM Vulnerabilities

A. Prompt Injection Attacks

B. Hallucinations

C. Jailbreaking

D. Training Data Leakage

E. Data Exfiltration via Output

F. Insecure Tool Use in Agents

Session XI: Hands on Generative AI & Agentic App Security

With the rise of Generative AI and Agentic Applications (apps powered by autonomous agents), organizations are increasingly exposed to new security risks and attack vectors. These systems can generate text, code, images, and even take autonomous actions across tools, APIs, and systems — making AI-driven apps powerful but also high-risk. Participants are able to

- Understand the threat landscape for generative AI systems and autonomous agents.
- Explore real-world vulnerabilities including prompt injection, unsafe tool use, and data leakage.
- Implement defensive coding and hardening techniques in AI-driven apps using hands-on labs.
- Learn how to test, monitor, and secure agentic workflows using practical examples

Security Best Practices Covered

- Input/output sanitization for all user and document inputs
- Zero-trust architecture for tools and retrieved content
- Tool invocation with policy enforcement
- Use of content moderation layers (OpenAI Moderation API, Claude's MCP)

Summary of the Program:

Program The primary aim of this FDP is to provide participants with a comprehensive understanding of cutting-edge AI technologies. It covers foundational concepts such as Transformers and tokenization, along with advanced topics like image generation and video summarization in GenAI, evaluation benchmarks, prompt engineering, and security in LLMs. Through expert-led sessions, attendees will gain insights into optimizing AI performance, enhancing security measures, and applying these concepts in real-world scenarios, empowering them to integrate modern AI advancements into research and academia effectively

Program Outcomes of FDP:

1.Demonstrate a Comprehensive Understanding of Transformers-Explain the architecture, working principles, and applications of transformer-based models in natural language processing (NLP).

2.Apply Tokenization Techniques in LLMs – Utilize various tokenization methods to preprocess text data effectively for large language models.

3.Implement image generation and video summarization in GenAI – Develop and deploy GenAI- for automated video summarization, enhancing content extraction and analysis.

4.Evaluate LLM Performance Using Benchmarks – Analyse and compare the efficiency of LLMs using standard evaluation frameworks and key performance indicators

5. Optimize AI Outputs through Prompt Engineering –Design and experiment with different prompt engineering techniques to improve the accuracy and relevance of model-generated responses.

6.Enhance Security and Mitigate Risks in LLMs – Identify potential security threats, implement protective measures,and ensure ethical and responsible use of large language models.

This FDP will empower faculty members with the latest advancements in LLMs, enabling them to integrate cutting-edge AI techniques into research, teaching, and industry applications.

It gives me immense pleasure to thank our **KSIT Management, Principal Dr. Dilip Kumar K and HOD of AIML Dept, Dr. Suresh M.B** for providing me an opportunity to attend such FDP program and hence to update my professional growth.

B. N. M. Institute of Technology

An Autonomous Institution under VTU, Approved by AICTE

Certificate of Participation

This is to Certify that Mr/Ms /Mrs Dr Sahana Salagare

of K S Institute of Technology has attended six day Faculty Development Programme on " A Deep Dive Into Generative AI: From Transformers to Applications and Security" organized by Department of Artificial Intelligence and Machine Learning, BNMIT during 23rd to 28th June 2025.

Dr. Sudha Subbiah | Dr. Krishnamurthy G. N. | Dr. S. Y. Kulkarni | Prof. T. J. Rammurthy

Participant:

Dr. SAHANA SALAGARE

Assistant Professor

Dept of AI & ML

KSIT, Bengaluru

HOD

Dr. Suresh M. B

Dept of AI &ML

KSIT, Bengaluru

Head of the Department
Artificial Intelligence & Machine Learning
K.S. Institute of Technology
Bengaluru - 560 109

Principal

Dr. Dilip Kumar K

KSIT, Bengaluru