NEW HORIZON COLLEGE OF ENGINEERING

IEEE NHCE STUDENT BRANCH

INSTITUTION'S INNOVATION COUNCIL (Ministry of Education Initiative)

IEEE Industrial Electronics Society ies New Horizon College of Engineering, IE13

IEEE IES Bangalore Chapter

Silver Jubilee Celebrations | Silver Summit

Distinguished Lecture

Research Opportunities in Generative AI Security: Attacks, Vulnerabilities, and Countermeasures

30th June 2026

10:00 AM - 12:30 PM

Online

Dr. Praveen R

Executive Committee Member for
IEEE Vehicular Technology Society
IEEE Sensor Council of IEEE Madras Section
Department of Computer Science and Engineering,
National Institute of Technology, Puducherry

Organising Committee

Dr. Vinoth Kumar K
Professor and Associate Head - R&D
Advisor IEEE IES NHCE SBC

Dr. Revathi V
Dean - R&D

Dr. Manjunatha
Principal

Organised by

Department of Research and Development

Dean
Department of Research and Development
NEW HORIZON COLLEGE OF ENGINEERING
New Horizon Knowledge Park, Bellandur Main Road,
Near Marathalli, Bengaluru - 560 103

NEW HORIZON COLLEGE OF ENGINEERING

Department of Research and Development

Event Report

Title	**Distinguished Lecture on Research Opportunities in Generative AI Security: Attacks, Vulnerabilities, and Countermeasures**	
Department	Research and Development	
Date	From: 30.06.2026	To: 30.06.2026
Time	From: 10:00 AM	To: 12:30 PM

Event Overview

As part of the **Silver Jubilee Celebrations – Silver Summit**, the Department of Research and Development, New Horizon College of Engineering, organized an online **Distinguished Lecture** on **"Research Opportunities in Generative AI Security: Attacks, Vulnerabilities, and Countermeasures"** on **30 June 2026**.

The lecture was delivered by **Dr. Praveen R**, Executive Committee Member, IEEE Vehicular Technology Society, IEEE Sensor Council – IEEE Madras Section, and Faculty, Department of Computer Science and Engineering, National Institute of Technology Puducherry.

The session was organized to provide participants with insights into emerging research challenges in Generative Artificial Intelligence (GenAI), focusing on security threats, vulnerabilities, adversarial attacks, privacy concerns, and effective countermeasures. The lecture also highlighted potential research directions and opportunities for academicians, researchers, and postgraduate students working in AI and Cybersecurity.

Objectives

- To introduce participants to the latest developments in Generative AI security.
- To understand various attack vectors and vulnerabilities associated with Large Language Models (LLMs) and Generative AI systems.
- To discuss existing and emerging countermeasures for secure AI deployment.
- To identify promising research opportunities in AI security and trustworthy AI.
- To encourage interdisciplinary research collaborations in AI and Cybersecurity.

Highlights of the Lecture

Dr. Praveen R delivered a highly informative and engaging session covering:

- Evolution of Generative AI technologies.
- Security risks associated with foundation models and Large Language Models.
- Prompt injection attacks and adversarial prompting.
- Data poisoning and model manipulation techniques.
- Privacy leakage and model inversion attacks.
- Jailbreaking techniques against Generative AI systems.
- Secure prompt engineering methodologies.
- AI governance, ethical considerations, and responsible AI practices.
- Future research opportunities in AI security, explainable AI, and trustworthy machine learning.
- Publication opportunities and collaborative research initiatives.

The lecture concluded with an interactive question-and-answer session where participants discussed current research problems, publication strategies, funding opportunities, and future collaboration prospects.

Outcome of the Programme

The distinguished lecture enabled participants to:

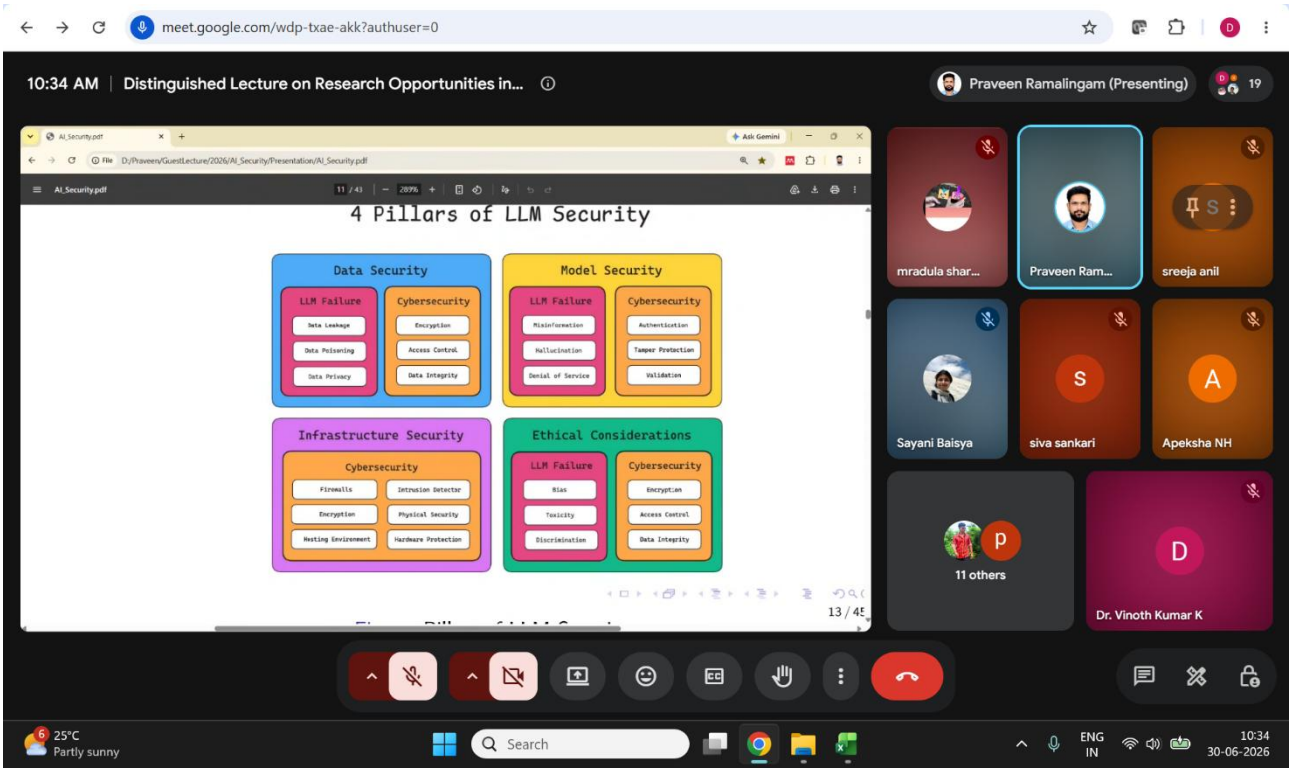
- Gain comprehensive knowledge of Generative AI security challenges.
- Understand real-world attack scenarios targeting AI models.
- Explore current research trends in trustworthy and secure AI.
- Identify potential interdisciplinary research topics.
- Enhance awareness of ethical AI development and deployment practices.
- Develop interest in collaborative research and IEEE professional activities.

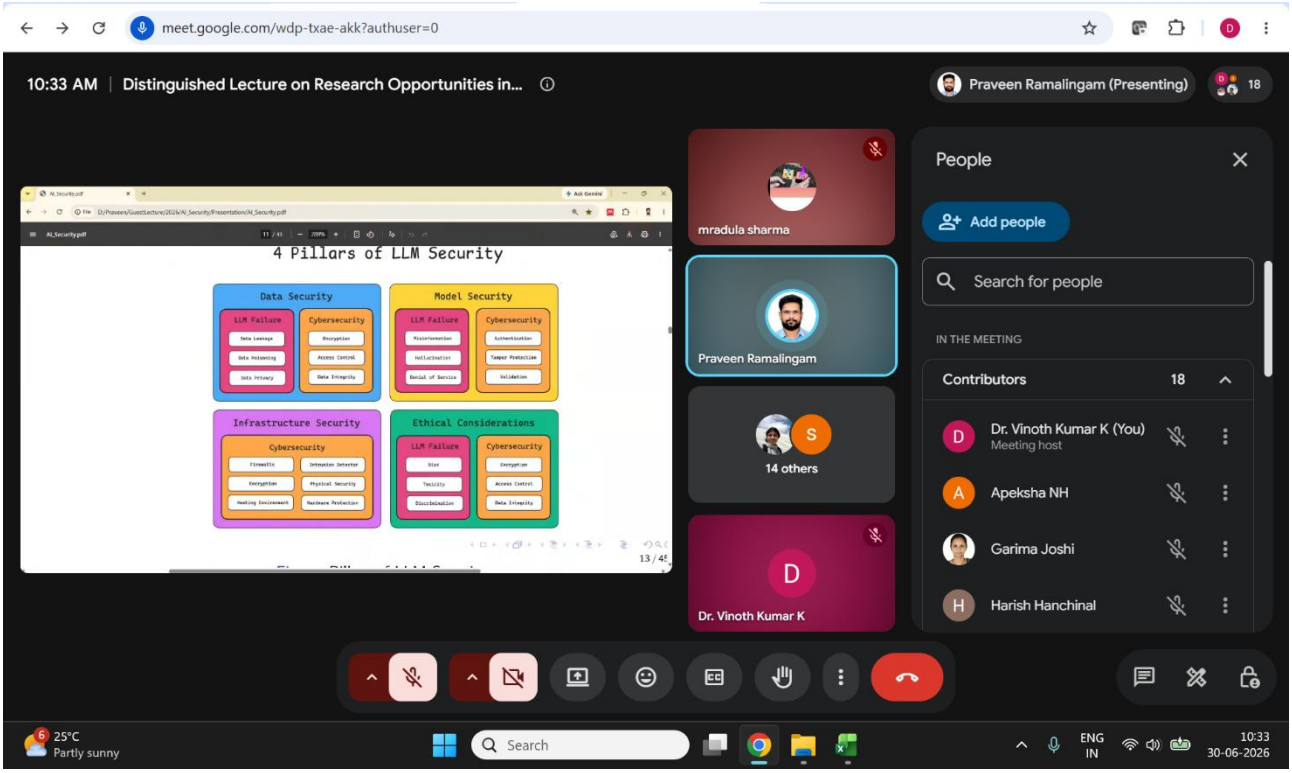
Participants

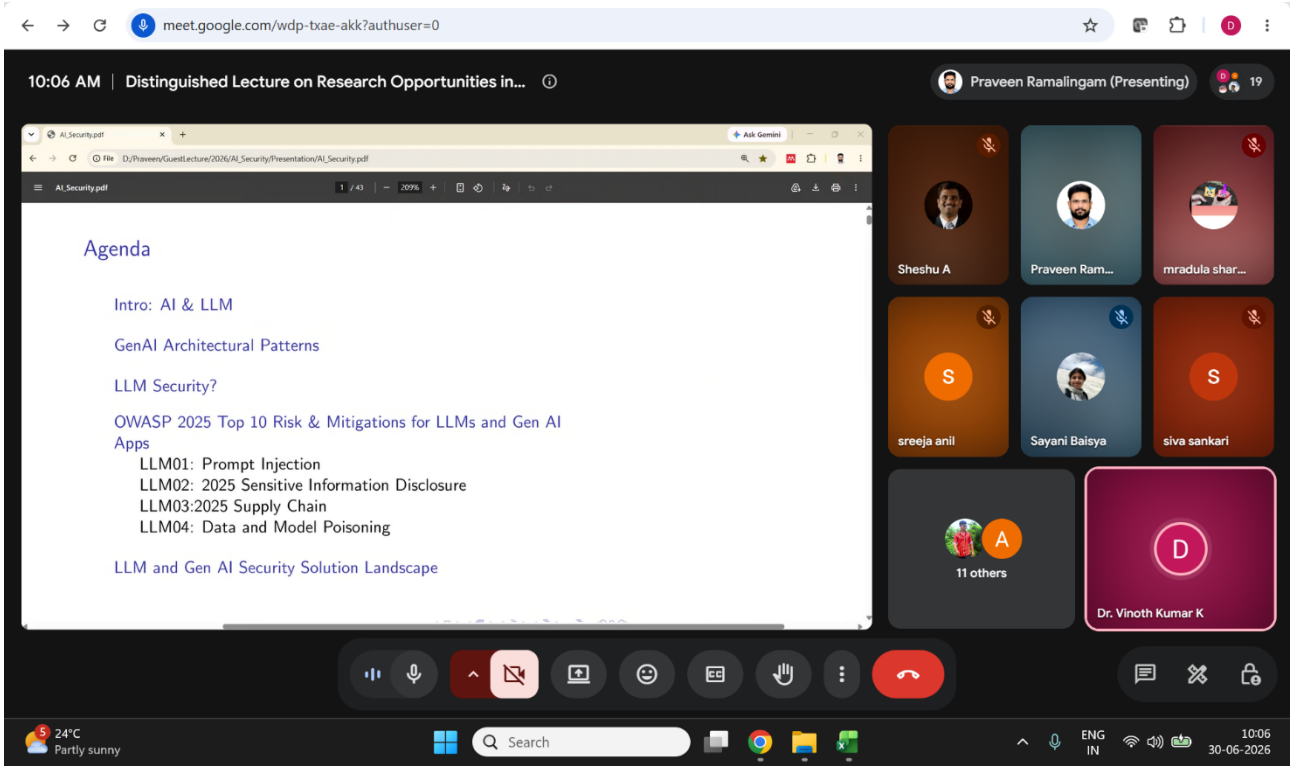
The online session witnessed enthusiastic participation from:
39 Faculty members participants actively interacted with the speaker during the discussion session, making the programme highly engaging and beneficial.

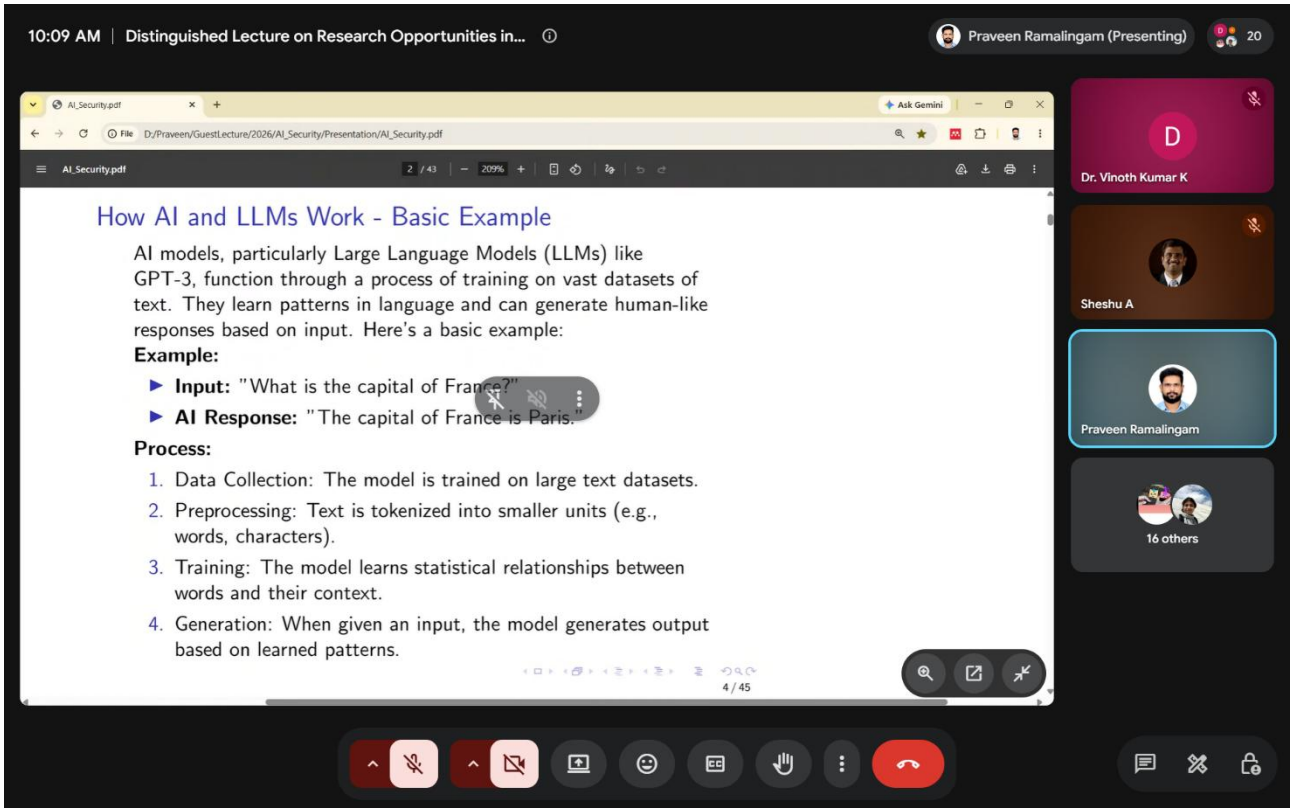
Conclusion

The Distinguished Lecture successfully achieved its objectives by providing valuable insights into the rapidly evolving domain of Generative AI Security. The expert session by Dr. Praveen R enhanced participants' understanding of emerging threats, vulnerabilities, and research opportunities while emphasizing the importance of developing secure, ethical, and trustworthy AI systems. The programme served as an excellent platform for knowledge sharing and inspired faculty members, researchers, and students to pursue innovative research in Artificial Intelligence and Cybersecurity as part of New Horizon College of Engineering's Silver Jubilee initiatives.




meet.google.com/wdp-txae-akk?authuser=0
10:33 AM | Distinguished Lecture on Research Opportunities in...
Praveen Ramalingam (Presenting)
18
4 Pillars of LLM Security
Data Security
LLM Failure
Cybersecurity
Model Security
Infrastructure Security
Ethical Considerations
mradula sharma
Praveen Ramalingam
14 others
Dr. Vinoth Kumar K
People
Add people
Search for people
IN THE MEETING
Contributors 18
Dr. Vinoth Kumar K (You)
Meeting host
Apeksha NH
Garima Joshi
Harish Hanchinal
25°C
Partly sunny
Search
ENG
IN
10:33
30-06-2026





Dean
Department of Research and Development
NEW HORIZON COLLEGE OF ENGINEERING
New Horizon Knowledge Park, Bellandur Main Road,
Near Marathalli, Bengaluru – 560 103

Participant Details of Distinguished Lecture on Research Opportunities in Generative AI Security: Attacks, Vulnerabilities, and Countermeasures dated on 30.06.2026

S.No	Timestamp	Name of the Participant	Designation	Department	Name of the Institution	Topic Coverage in the Session	Effectiveness in Delivering the Lecture	The learning materials were presented in clear and organized manner.	The experts/presenters were well prepared	The experts/presenters responded to queries of participants satisfactorily	Adequate time was provided for activities	Overall rating of the event
1	6-30-2026 11:40:13	Sukhmanpreet Kaur	Assistant Professor	CSE	NHCE	5	5	5	5	5	5	5
2	6-30-2026 11:41:01	Mradula	Sr Asst Professor	CSE-2	NHCE	5	5	5	5	5	5	5
3	6-30-2026 11:41:35	Vijayashree H P	Sr. Assistant Professor	CSE 2	NHCE	4	4	4	4	4	4	4
4	6-30-2026 11:41:48	Sayani Baisya	AP	CSE 2	NHCE	5	5	5	5	5	5	5
5	6-30-2026 11:42:06	Ramesh Prasad R	Professor of Practice	AIML	NHCE	5	4	5	5	5	3	5
6	6-30-2026 11:42:42	Dr. Neelima Ravindran K	Assistant Professor	MBA	NHCE	5	5	5	5	5	5	5
7	6-30-2026 11:43:24	Harish R Hanchinal	Sr.Assistant Professor	Electronics & Communication Engg.	NHCE	4	4	4	4	4	4	4
8	6-30-2026 11:43:48	Mrs. Padmavathi C Ainapure	Assistant Professor	Computer Science and Engineering	NHCE	5	5	5	5	5	5	5
9	6-30-2026 11:44:21	Garima Joshi	Asst Professor	CSE2	NHCE	4	5	5	5	5	4	5
10	6-30-2026 11:44:32	Dr. DIVYA SHARMA	Associate Professor	CSE	NHCE	5	5	5	5	5	5	5
11	6-30-2026 11:44:37	Manojkumar	Assistant professor	AIML	NHCE	5	5	5	5	5	5	5
12	6-30-2026 11:45:09	V Lakshmi Durga	Sr Assistant professor	CSE	NHCE	5	5	5	5	4	4	5
13	6-30-2026 11:45:20	Dr. D. Roja Ramani	Associate Professor	Computer Science and Engineering	NHCE	5	5	5	5	5	5	5
14	6-30-2026 11:45:31	Chempavathy B	enior Assistant Professo	Computer Science and Engineering	NHCE	5	5	5	5	5	5	5
15	6-30-2026 11:45:37	Saranya S	Assistant Professor	Computer science and Engineering	NHCE	5	5	4	4	5	5	5
16	6-30-2026 11:47:29	Dr Soja Rani S	Associate Professor	CSE	NHCE	5	5	5	5	5	5	5
17	6-30-2026 11:48:26	Dr. SOWMYA HK	Associate Professor	Artificial Intelligence and Machine Learning	NHCE	5	5	5	5	5	5	5
18	6-30-2026 11:48:44	Divyanshi Chhabra	Assistant Professor	CSE 1	NHCE	4	4	4	4	4	4	4
19	6-30-2026 11:49:56	Dr.sreoshi Dasgupta	Associate Professor	MBA	NHCE	5	5	5	5	5	5	5
20	6-30-2026 11:50:33	Dr J.Karthiyayini	Associate Professor	Information Science and Engineering	NHCE	5	5	4	5	5	5	5
21	6-30-2026 11:50:46	Sukanya N S	Associate Professor	MCA	NHCE	4	5	4	5	4	4	5
22	6-30-2026 11:51:00	B NITHYA	Associate Professor	MCA	NHCE	4	4	4	4	4	4	4
23	6-30-2026 11:51:07	Salna Joy	Sr Assistant Professor	CSE1	NHCE	5	5	5	5	5	5	5
24	6-30-2026 11:53:16	Archana Das	Assistant Professor	Information Science and Engineering	NHCE	5	5	5	5	5	5	5
25	6-30-2026 11:53:32	Rama Bansidhar Dan	enior Assistant Profess	ISE	NHCE	5	5	5	5	5	5	5
26	6-30-2026 11:53:52	Vanthana	Assistant Professor	ISE	NHCE	5	5	5	5	5	5	5
27	6-30-2026 11:54:37	Dr. Priya Thomas	Associate Professor	MCA	NHCE	5	5	5	5	5	5	5
28	6-30-2026 12:02:45	Shruthi G R	Sr. Asst. Professor	Information Science and Engineering	NHCE	4	4	4	4	4	4	4
29	6-30-2026 12:08:31	Dr.Rajlakshmi Ghatkamble	Associate Professor	ISE	NHCE	4	4	4	4	4	4	4
30	6-30-2026 12:12:25	DR.PRIYAMEET KAUR KEER	Professor	MBA	NHCE	5	5	5	5	5	5	5
31	6-30-2026 12:16:16	N Mithili Devi	Associate Professor	MCA	NHCE	5	5	5	5	5	5	5
32	6-30-2026 12:19:43	Dr. Srividhya G	enior Assistant Professo	Computer science and Engineering	NHCE	5	5	5	5	5	5	5
33	6-30-2026 12:58:51	S P Sreeja	Sr. Assistant Professor	MCA	NHCE	4	4	4	5	4	4	4
34	6-30-2026 13:03:10	Dr. Ramachandra Naik	Associate Professor	Applied Sciences	NHCE	5	5	5	5	5	5	5
35	6-30-2026 13:03:51	Dr.Jimsha K Mathew	Associate professor	AIML	NHCE	5	5	5	5	5	5	5
36	6-30-2026 13:16:14	Dr. Madhumohana Raju A B	Associate Professor	Applied Sciences	NHCE	5	5	5	5	5	5	5
37	6-30-2026 13:17:13	A.Kalaivani	enior Assistant Professo	MCA	NHCE	4	4	4	4	4	4	4
38	6-30-2026 13:19:00	Dr. R SUGANYA	Associate Professor	CSE(DATA SCIENCE)	NHCE	5	5	5	5	5	5	5
39	6-30-2026 13:26:03	BHASKAR S V	Sr AP	CSE	NHCE	4	4	4	4	4	4	4