Department of Computer Science & Engineering

Date: 10/08/2026

Submitted,

Sub: Report on Five-Day Online Faculty Development Programme (FDP) on "Cyber Security Using Artificial Intelligence" – Reg.

The Department of Computer Science and Engineering (CSE), Sri Sairam College of Engineering, Bangalore, conducted a **Five-Day Online Faculty Development Programme (FDP)** on **"Cyber Security Using Artificial Intelligence"** from **03.08.2026 to 07.08.2026** through online mode.

The programme aimed to enhance the knowledge and skills of faculty members, research scholars, and participants in the areas of Artificial Intelligence and Cyber Security. The FDP provided valuable insights into contemporary trends, emerging technologies, AI-based security tools, cyber threat analysis, secure machine learning practices, ethical AI and their applications in the field of cyber security.

The programme commenced with a welcome address by **Dr. Smitha J. A., Professor & HoD, Department of CSE**, followed by the introduction of the Resource Persons by Dr. Mahesh A., Professor, Department of CSE.

OBJECTIVES OF THE FDP

- To create awareness of the emerging role of Artificial Intelligence in cybersecurity.
- To understand current cyber threats and security challenges affecting AI-enabled systems.
- To introduce threat modeling approaches for AI systems and common attacks such as data poisoning, model inversion and model theft.
- To discuss AI governance, ethical AI, risk management and secure AI practices.

FDP COORDINATORS

Name	Designation
Dr. MAHESH A	Professor, Department of Computer Science and Engineering
Dr. KARTHIKA K	Associate Professor, Department of Computer Science and Engineering

Fwd
13/8/26

13/08/2026

Department of Computer Science & Engineering

PROGRAMME DETAILS

Day & Date	Resource Person	Designation / Organization	Session Topic
Day 1 03.08.2026	**Mr. P. B. Senthil Kumar**	Senior Software Engineer, CISCO, Bangalore	AI Governance, Ethical AI, Risk Management, Secure AI
Day 2 04.08.2026	**Mr. A. Venkateshmoorthy**	Cyber Security Analyst, Caterpillar, Bangalore	Threat Modeling for AI Systems, Data Poisoning, Model Inversion, Model Theft Attacks
Day 3 05.08.2026	**Mr. Santhosh Rajasekaran**	Founder, Masala Metrics, Bangalore	Adversarial Machine Learning, Defensive Techniques, Secure Model Training, Privacy-Preserving AI
Day 4 06.08.2026	**Mr. Adhiyan Chandrasekaran**	Senior Software Engineer, Tangoe, Bangalore	Introduction to AI, Machine Learning, Cybersecurity Fundamentals, AI Security Landscape
Day 5 07.08.2026	**Mr. Rakshit Rangarajan**	Software Engineer (Full-Stack Developer), BrandMuscle India Pvt. Ltd., Bangalore	Security in Data Science and Analytics Applications

Day 1(03.08.26) – AI Governance, Ethical AI, Risk Management and Secure AI

The first session introduced the broader relationship between Artificial Intelligence and cybersecurity. The resource person discussed the importance of AI governance, ethical use of AI, risk identification and management, and secure AI practices. Emphasis was placed on responsible development and deployment of AI systems and on addressing security and ethical risks throughout the AI lifecycle.

Department of Computer Science & Engineering

Day 2(04.08.26) – Threat Modeling for AI Systems

The second session focused on threat modeling for AI-based systems. Participants were introduced to security threats including data poisoning, model inversion and model theft attacks. The session highlighted the need to identify attack surfaces, understand possible adversarial actions and incorporate security controls into AI system design.

Day 3(05.08.26) – Adversarial Machine Learning and Privacy-Preserving AI

The third session explored adversarial machine learning and the ways in which attackers can manipulate or exploit machine-learning systems. Defensive techniques, secure model training and privacy-preserving approaches were discussed. The session helped participants understand the importance of building resilient AI models against adversarial threats.

Day 4(06.08.26) – AI, Machine Learning and the AI Security Landscape

The fourth session covered the fundamentals of Artificial Intelligence and Machine Learning in the context of cybersecurity. The resource person explained the evolving AI security landscape and discussed how AI technologies can both introduce new security risks and support cybersecurity operations.

Day 5(07.08.26) – Security in Data Science and Analytics Applications

The fifth session addressed security considerations in data science and analytics applications. The discussion emphasized protecting data, ensuring secure analytical workflows and recognizing security risks associated with data-driven applications. The session provided a practical perspective on integrating security into data science activities.

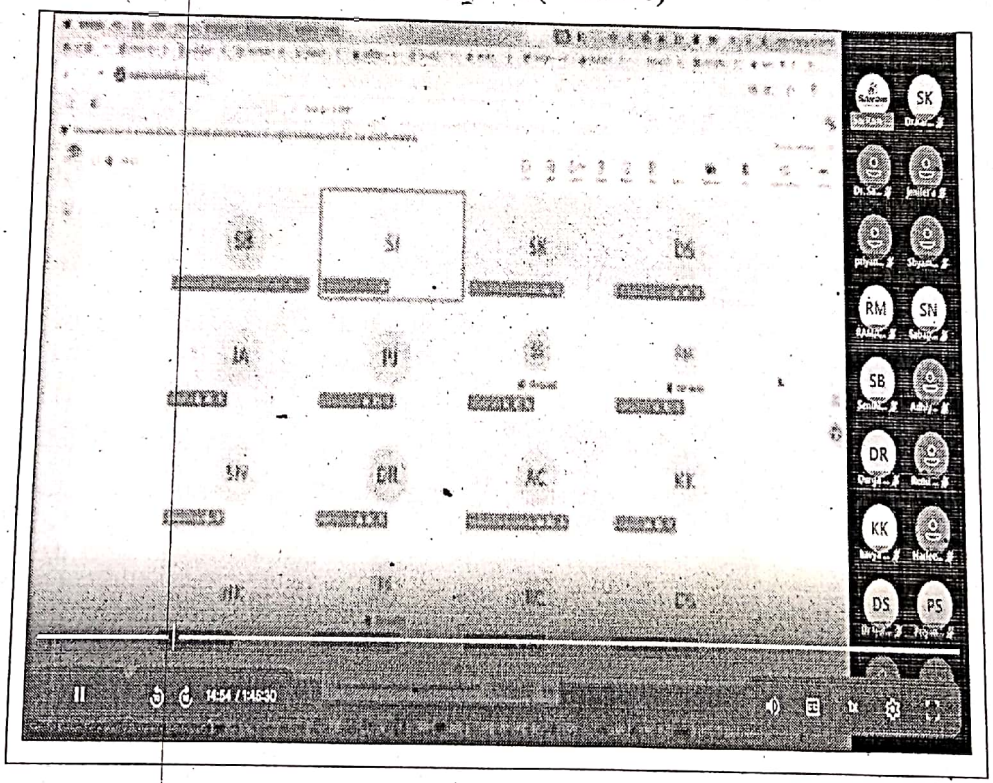
The Five-Day Faculty Development Programme provided participants with a comprehensive understanding of the evolving cybersecurity landscape in AI-enabled environments. Participants gained familiarity with AI governance, ethical AI principles, and AI risk management, while also learning about major attacks against AI systems, including data poisoning, model inversion, and model theft. The programme enhanced their awareness of adversarial machine learning techniques and methods for improving model robustness. Participants also developed an understanding of the significance of secure model training and privacy-preserving AI, along with an overview of key AI security challenges and opportunities in practical applications. Participant feedback and learning assessment were incorporated as integral components of the programme. Participants were encouraged to provide feedback on the quality and relevance of the sessions, effectiveness of the resource persons, technical delivery, and overall organization of the FDP.

Department of Computer Science & Engineering

A post-programme quiz was also conducted to reinforce and assess the learning gained during the five-day programme. Certificates were issued to eligible participants who fulfilled the prescribed participation and assessment requirements of the programme.

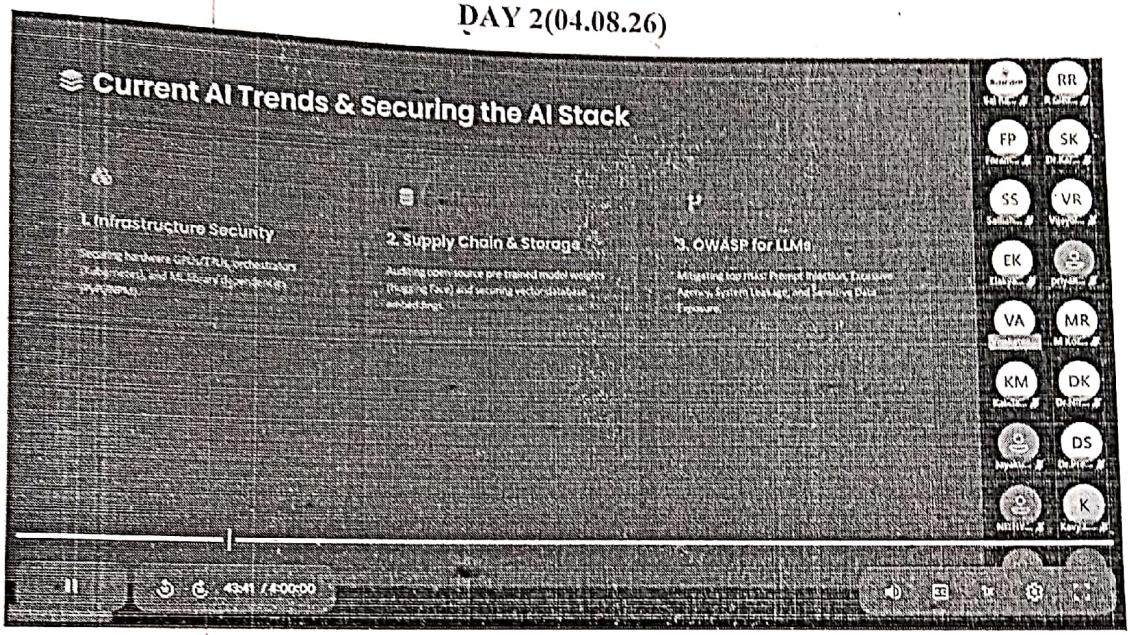
The Five-Day FDP on **"Cyber Security Using Artificial Intelligence"** proved to be a valuable learning experience for all participants. The programme successfully met its objectives by equipping faculty members with the latest knowledge, practical skills and insights into **Artificial Intelligence and Cyber Security**. The programme concluded at around **8:00 PM on 07.08.2026** with participant feedback, followed by a **vote of thanks by Dr. Smitha J. A.**, who acknowledged the valuable contributions and efforts of the organizing team, resource persons and participants in making the programme a successful one.

DAY 1(03.08.26)

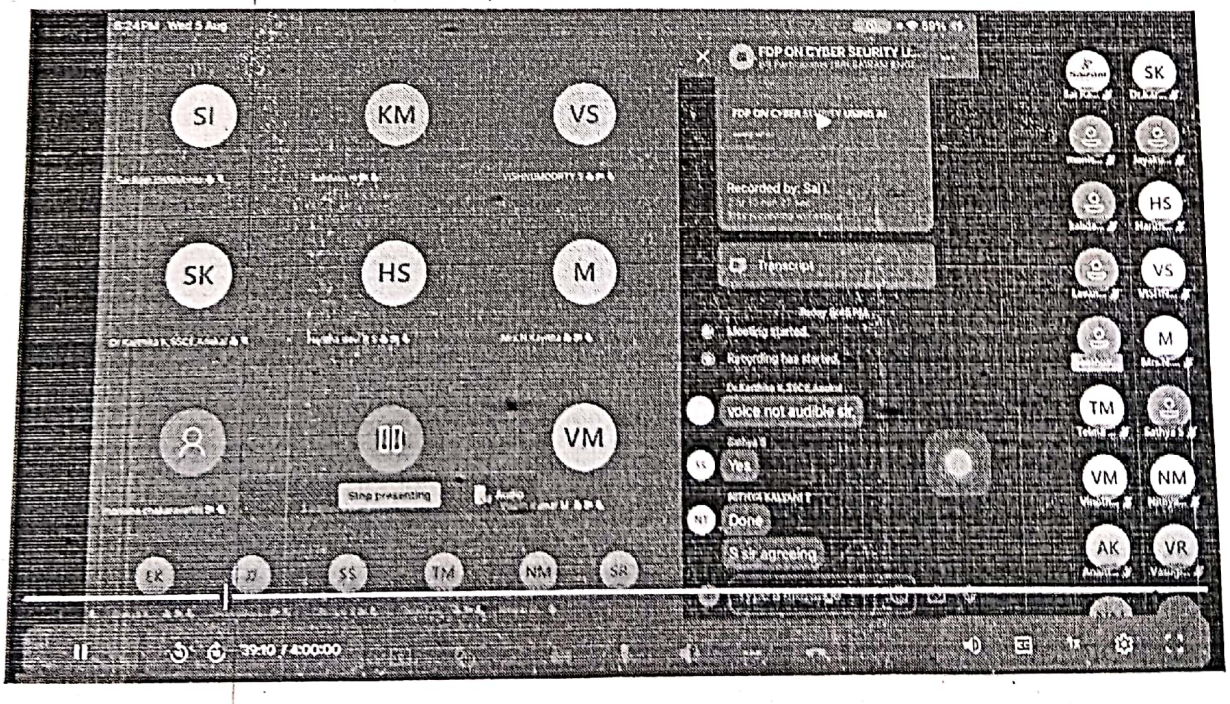


Department of Computer Science & Engineering

DAY 2(04.08.26)

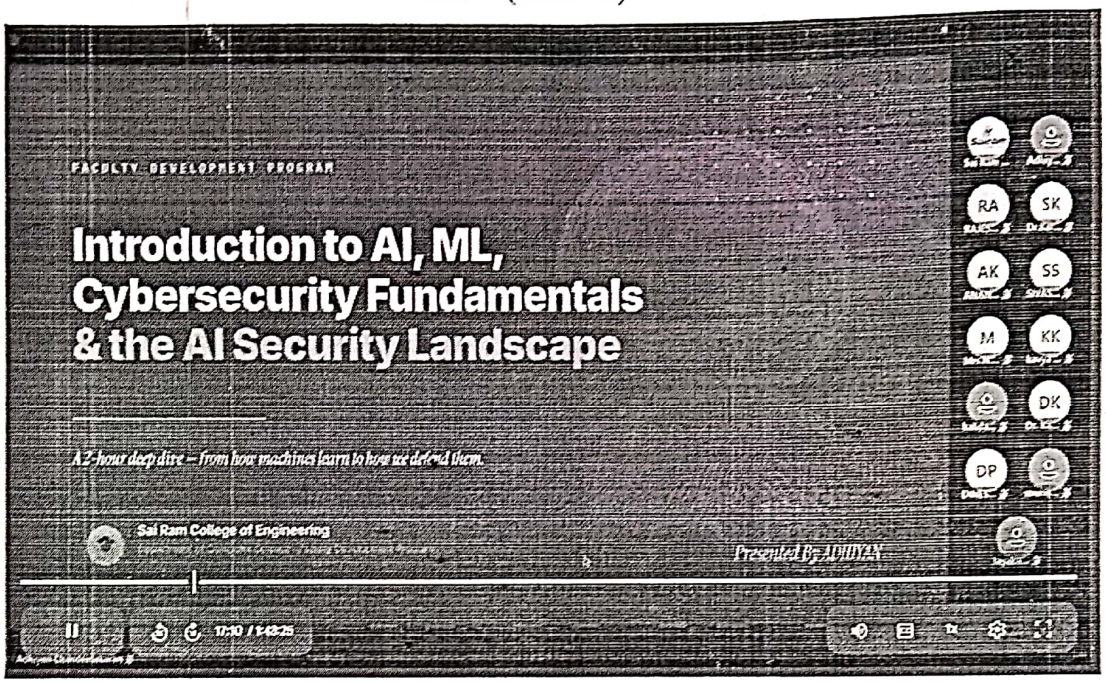


DAY 3(05.08.26)

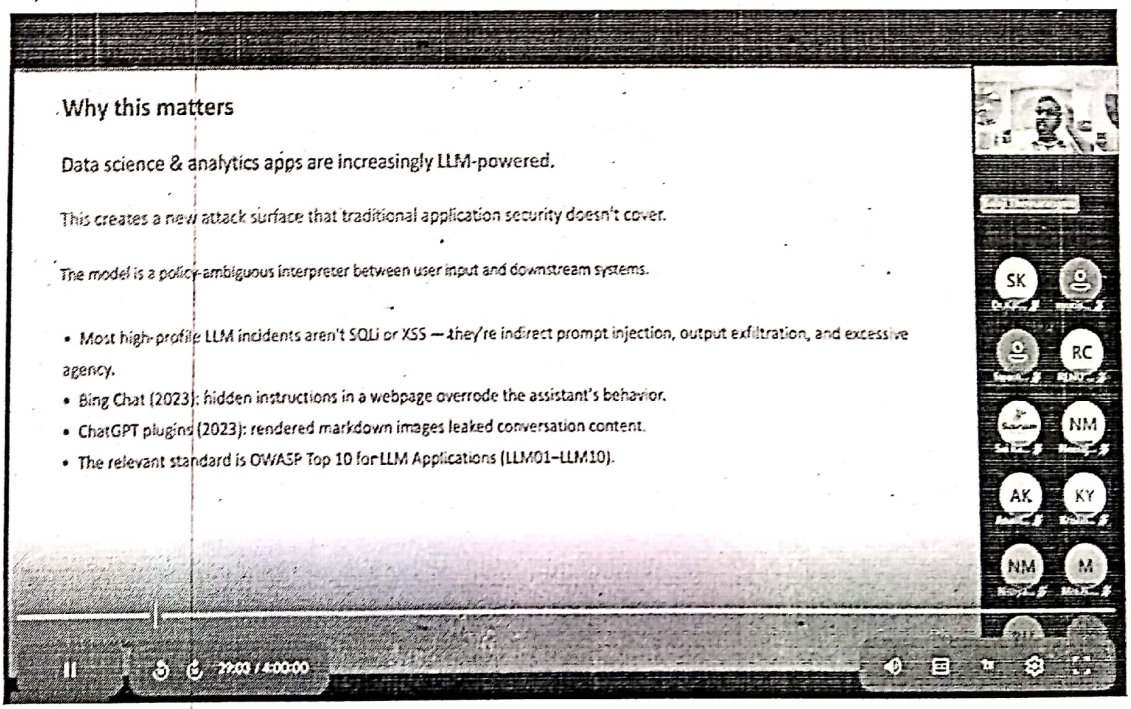


Department of Computer Science & Engineering

DAY 4(06.08.26)



DAY 5(07.08.26)



11/8/26

13/08/2026