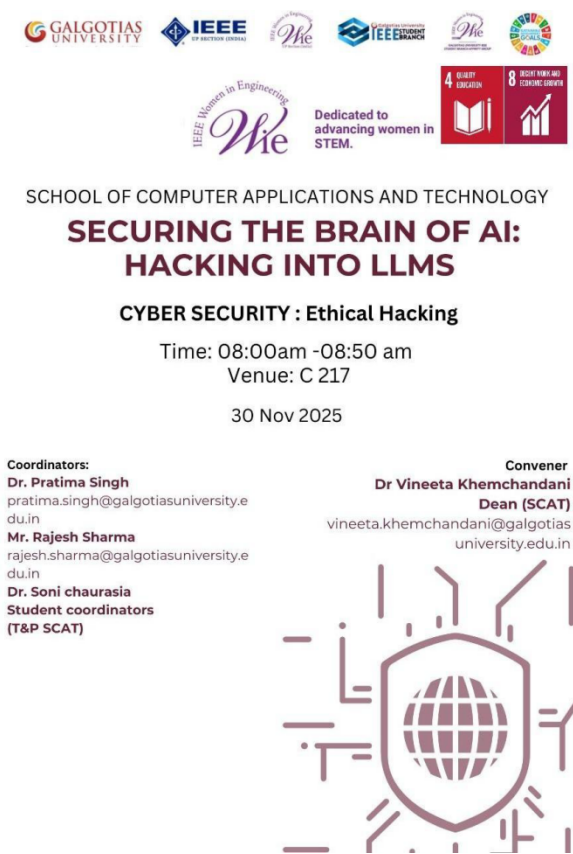


Event Report 2025 - 26

Title of Activity*	Securing the Brain of AI: Hacking into LLMs
Organized by (School/Centre Name)*	Training & Placement Team, School of Computer Applications and Technology (SCAT), Galgotias University
Program Theme*	Cyber Security / Ethical Hacking
Date*	30th November 2025
Time*	08:00 AM - 08:50 AM
Duration of the event* (If more than one day kindly fill the table available at the end of this form)	50 Minutes (Single Session)
Poster*	 SCHOOL OF COMPUTER APPLICATIONS AND TECHNOLOGY SECURING THE BRAIN OF AI: HACKING INTO LLMs CYBER SECURITY : Ethical Hacking Time: 08:00am -08:50 am Venue: C 217 30 Nov 2025 Coordinators: Dr. Pratima Singh pratima.singh@galgotiasuniversity.edu.in Mr. Rajesh Sharma rajesh.sharma@galgotiasuniversity.edu.in Dr. Soni chaurasia Student coordinators (T&P SCAT) Convener Dr Vineeta Khemchandani Dean (SCAT) vineeta.khemchandani@galgotiasuniversity.edu.in
Venue* (Block and Room No.)	C-217, Galgotias University
SDG Attained* (Mention SDG number/s)	SDG 8 - Decent Work and Economic Growth
YouTube/Facebook Link: (if live steamed or video posted on FB/YT)	NA
Social media link* (promoting in any one Facebook/Instagram/WhatsApp/Twitter is mandatory)	https://chat.whatsapp.com/J8qgxniP1DZI CgzUZ3dk9E

No. of Students* (only no. to be written, list in excel or word should be maintain at department level as proof for any further requirement)	
No. of Faculty* (only no. to be written , list in excel or word should be maintain at department level as proof for any further requirement)	3
No. of External Participants (students + faculty) [write NA if not applicable]	NIL
(Geotag) Photograph-1*	
(Geotag) Photograph-2	
Description (min 250 to max 800 words)*	The School of Computer Applications and Technology, Galgotias University, successfully organized an expert session titled “Securing the Brain of AI: Hacking into LLMs” on 30th November 2025 under the theme Cyber Security: Ethical Hacking. The session was designed to create awareness among students about emerging security challenges in Artificial Intelligence systems, particularly Large Language Models (LLMs), which are increasingly being adopted across various industries. The primary objective of the session was to enhance students’ understanding of AI vulnerabilities, ethical hacking techniques, and secure AI system design. The session aimed to familiarize students with real-world threats affecting AI models and emphasize the importance of responsible and secure AI development. The event began with an introductory address by the faculty coordinators, followed by detailed presentations by the resource persons. The session provided deep insights into the

	internal functioning of LLMs and explained how attackers exploit weaknesses through techniques such as prompt injection, jailbreaking, adversarial attacks, and unauthorized output generation. Practical examples were demonstrated to help students understand how insecure AI systems can lead to data leakage, misinformation, privacy violations, and system-level compromises. Special emphasis was laid on the ethical aspects of hacking, highlighting the difference between malicious exploitation and responsible security testing. The speakers discussed the growing global importance of AI security, particularly in critical domains such as healthcare, finance, education, and enterprise systems, where AI failures can have serious consequences. The session was highly interactive, with students actively participating in discussions related to AI safety, cybersecurity career paths, secure model development, and best practices for responsible AI usage. The event aligned well with current industry requirements and introduced students to the rapidly emerging domain of AI Security and Ethical Hacking, thereby enhancing their technical awareness and industry readiness. Outcomes of the Event Students gained awareness of security challenges in AI and LLMs Understanding of ethical hacking techniques used in AI systems Exposure to real-world AI vulnerabilities and attack scenarios Increased interest in cybersecurity and AI security career pathways Enhanced understanding of responsible and secure AI development
Details of Keynote speaker/ Special Guest (<i>Name, Institute/ Company name, Designation, contact no.</i>)	Dr. Pratima Singh Mr. Rajesh Sharma Dr. Soni Chaurasia
Student Coordinators	
Attendance Sheet* (Physical attendance is mandatory to submit with signature of attendees)	

Report Submitted by* (<i>write faculty coordinator name, contact number</i>)	Dr. Pratima Singh Mr. Rajesh Sharma Dr. Soni Chaurasia
---	--

Fields marked with '' are mandatory*

Fill the information if the event is for more than 1 day

	Session – 1	Session-2	Session-3	Session-4
Date				
Time				
Key Speaker				
Venue				