A Report on Expert Talk on "AI in Cyber Security"
Organized by Department of CSE-Artificial Intelligence & Machine Learning
on 22.12.2025


Report Submitted by: Mr. BSH. Shayeez Ahamed, Assistant Professor, Department of CSE (AI and ML)
Resource Person Details: Mr. Charan Gudivada, CEO, Woollemia Infosec, Bengaluru
Participants: II Year CSE (AI and ML) – 120 Students
Venue: Seminar Hall - A
Mode of Conduct: Offline

Department of Computer Science and Engineering (AI and ML) organized an Expert Talk on "AI in Cyber Security" on 22.12.2025 (Monday).

Welcome Address:
The event commenced at 10:00 AM with a warm and engaging welcome address to all by Mr. BSH. Shayeez Ahamed, Asst. Professor, Department of CSE (AI and ML), Madanapalle Institute of Technology & Science (MITS), Madanapalle. The events' primary goal of the expert talk was to create awareness and build practical understanding among students about the critical role of Artificial Intelligence in modern cybersecurity, by exposing them to real-world cyber threats, AI-driven security solutions, industry tools, and emerging career opportunities.


Keynote Address

Dr. S. Padma, Associate Professor & Head, Department of CSE (AI and ML), Madanapalle Institute of Technology & Science (MITS), Madanapalle welcomed the student with her keynote address and highlighted the importance of such initiatives in shaping students' futures and appreciated their active participation. She advised students to cultivate innovation by adopting emerging technologies that cater to present industry demands. Furthermore, she emphasized continuous learning and skill development as key factors in building sustainable and successful professional careers.

Dr. P. Ramanathan, Principal, MITS, Madanapalle addressed the gathering and emphasized the importance of the session, The Principal encouraged students to actively participate in the expert session, interact with the speaker, and make the best use of the opportunity to clarify their doubts and gain in-depth knowledge. He motivated students to focus on these areas to enhance their employability and achieve success in competitive domains.

Resource Person Lecture:
Mr. Charan Gudivada, CEO, Woollemia Infosec, Bengaluru, shared his insights related to expert talk on AI in Cyber Security for II CSE (AI and ML) students.

He discussed the following points in the event
He focused on the growing role of Artificial Intelligence in modern cybersecurity, highlighting how AI-driven tools and techniques are transforming threat detection, vulnerability assessment, incident response, and security operations.

Reality of Cybersecurity Today
Mr. Charan explained about the rapid growth of cloud computing, mobile applications, APIs, and AI tools has significantly increased the attack surface. Attackers are now using automation and AI, making traditional manual security approaches insufficient. Cybersecurity is no longer limited to IT departments but has become a business and national security concern.
Why AI Became Critical in Cybersecurity
He highlighted that AI does not replace human experts, but instead augments human capabilities. AI plays a crucial role across multiple cybersecurity domains such as:

- **Vulnerability Assessment & Penetration Testing (VAPT)**
- **Security Operations Center (SOC) & SIEM**
- **Threat Intelligence**
- **Incident Response**

Later he emphasized that AI touches every cybersecurity role, not just a single job profile.

Role of AI in Ethical Hacking:
The expert demonstrated how AI assists ethical hackers by:

- **Identifying vulnerabilities faster**
- **Simulating real-world attack scenarios**
- **Prioritizing exploitable vulnerabilities**
- **Reducing false positives**

AI-assisted tools such as Burp Suite, Pentera, and Horizon3.ai help in intelligent scanning, while human experts validate findings and prepare risk-based reports.
AI in SOC & SIEM Operations
The talk explained challenges faced by Security Operations Centers such as:

- **Thousands of alerts per day**
- **Alert fatigue**
- **Limited skilled analysts**

AI-based SIEM solutions like Microsoft Sentinel, Splunk, and IBM QRadar use log correlation, behavior analysis (UEBA), and alert noise reduction techniques—reducing false alerts by up to 70% and enabling faster incident triage.

AI in Phishing and Social Engineering Detection

The resource person emphasized that over 90% of cyber breaches start with phishing attacks. AI-generated phishing emails and AI-based voice cloning have made attacks more convincing. AI-based solutions help by:

- **Email behavior analysis**
- **Voice anomaly detection**
- **Abnormal login behavior detection**

Tools like Microsoft Defender and Proofpoint were discussed as effective AI-driven security solutions.

AI for Threat Detection and Incident Response

AI enables organizations to:

- **Detect unknown and advanced attacks**
- **Identify lateral movement within networks**
- **Predict attacker intent**
- **Automate responses using SOAR platforms**

Security tools such as CrowdStrike and Darktrace help reduce breach detection time from hours to minutes and lower breach costs by more than 50% through early detection.

Key Takeaways

The session concluded with important guidance for students aspiring to build a career in cybersecurity:

- **Strong fundamentals in networking, operating systems, and security**
- **Hands-on experience with real-time tools and labs**
- **Understanding how AI supports security decision-making**
- **Thinking like a defender, attacker, and analyst**

The expert stressed that AI will not replace cybersecurity professionals, but professionals who combine security expertise with AI knowledge will lead the future.

Vote of thanks

The event formally concluded with a Vote of Thanks delivered by Mr. BSH. Shayeez Ahamed, Assistant Professor, Department of CSE (AI and ML), MITS. He expressed his sincere gratitude to the resource person for taking the time to share his expertise and valuable insights with the students. He also extended his thanks to the Management, the Principal, and the Head of the Department for their constant encouragement and support in successfully conducting the Expert Talk.

Outcomes:

At the end of Presentation, Students will be able to

1. **Students gained practical insights into AI-driven cybersecurity.**
2. **Students gained Awareness about industry tools and real-world attack scenarios.**
3. **Students enhanced their understanding skills towards career paths in cyber security.**
4. **Strengthened academia–industry interaction through expert engagement.**

UN-SDG Mapping:

SDG 4 – Quality Education
SDG 8 – Decent Work and Economic Growth
SDG 9 – Industry, Innovation, and Infrastructure
SDG 16 – Peace, Justice and Strong Institutions
SDG 17 – Partnerships for the Goals