MVJ COLLEGE OF ENGINEERING
Since 1982
Engineering A Better Tomorrow

An Autonomous Institute

Guest Lecture from the Department of Computer Science & Engineering

Affiliated to Visvesvaraya Technological University, Belagavi Approved By AICTE, New Delhi.
Recognized by UGC with 2(f) & 12(B) status
Accredited by NBA and NAAC.

A Report on Guest lecture on "AI AND CYBER SECURITY: A DOUBLE EDGED SWORD"

Date of the event	09.08.2024
Title of the Event	**Guest lecture on "AI AND CYBER SECURITY: A DOUBLE EDGED SWORD"**
Organized by	Dept of Computer Science and Engineering MVJCE, Bangalore

The Department of Computer Science and Engineering organized an event entitled. The event was Guest seminar on "AI AND CYBER SECURITY: A DOUBLE EDGED SWORD" conducted in "MVJ AUDITORIUM". The event started at 9:30 am and concluded at 11.30 pm. Total 200 students from all the 4th & 6th semesters of Dept. of Computer Science and Engineering, Computer Science and Design, and Artificial Intelligence and Machine Learning has participated in this event.

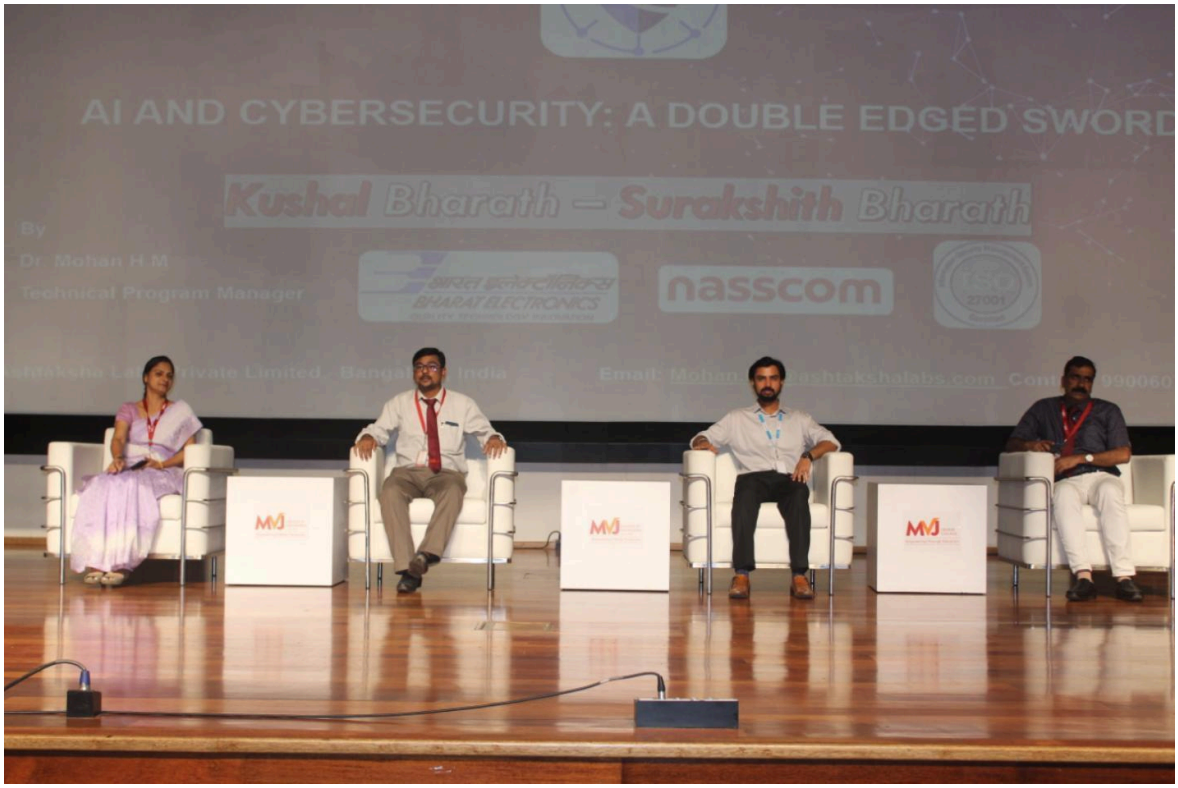
Chief guest Dr. Mohan H M

He is a Results-driven Technical Project Manager with 12+ years of experience, combining technical expertise with exceptional project leadership skills. Consistently delivers high-stakes projects on time, within budget, and to exacting standards.

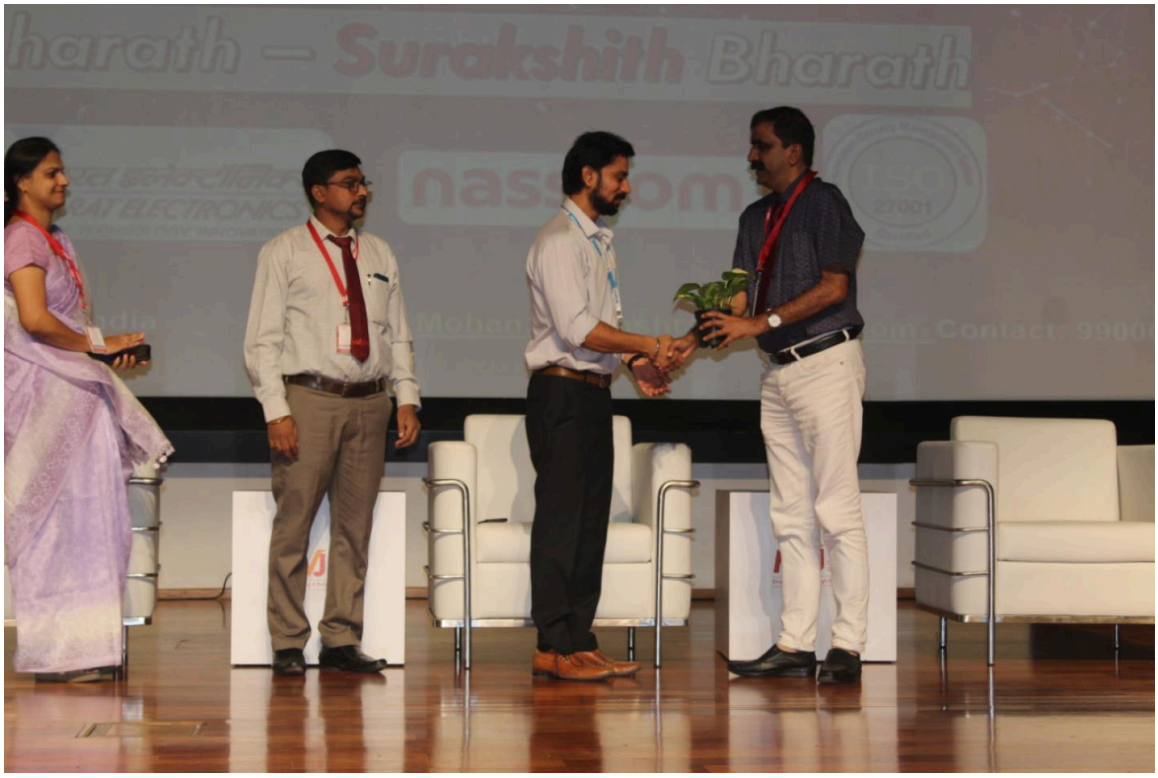
Adept at:

1. Mitigating project risks with proactive strategies
2. Fostering effective stakeholder relationships through clear communication
3. Optimizing resource allocation for maximum efficiency

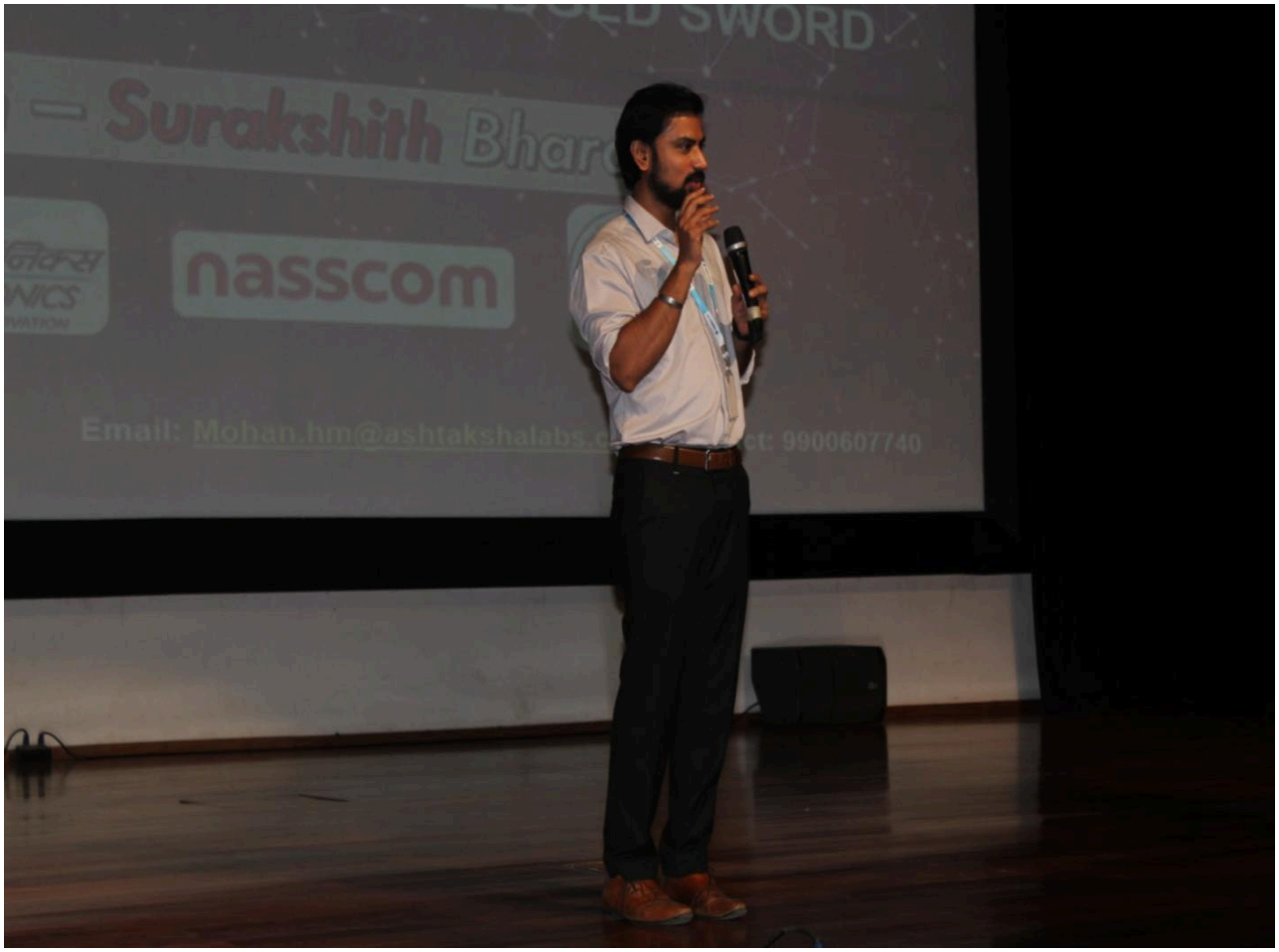
A passionate advocate for continuous improvement, driving innovation in project management processes to elevate team performance and deliver exceptional outcomes."



The event featured a prestigious dais, where honored dignitaries, who had been specially invited, were seated.



Dean Outrich Dr Ajayan Sir presented a sapling to Speaker as a token of love and appreciation, symbolizing the growth and nurturing of relationships.



Speaker started a session

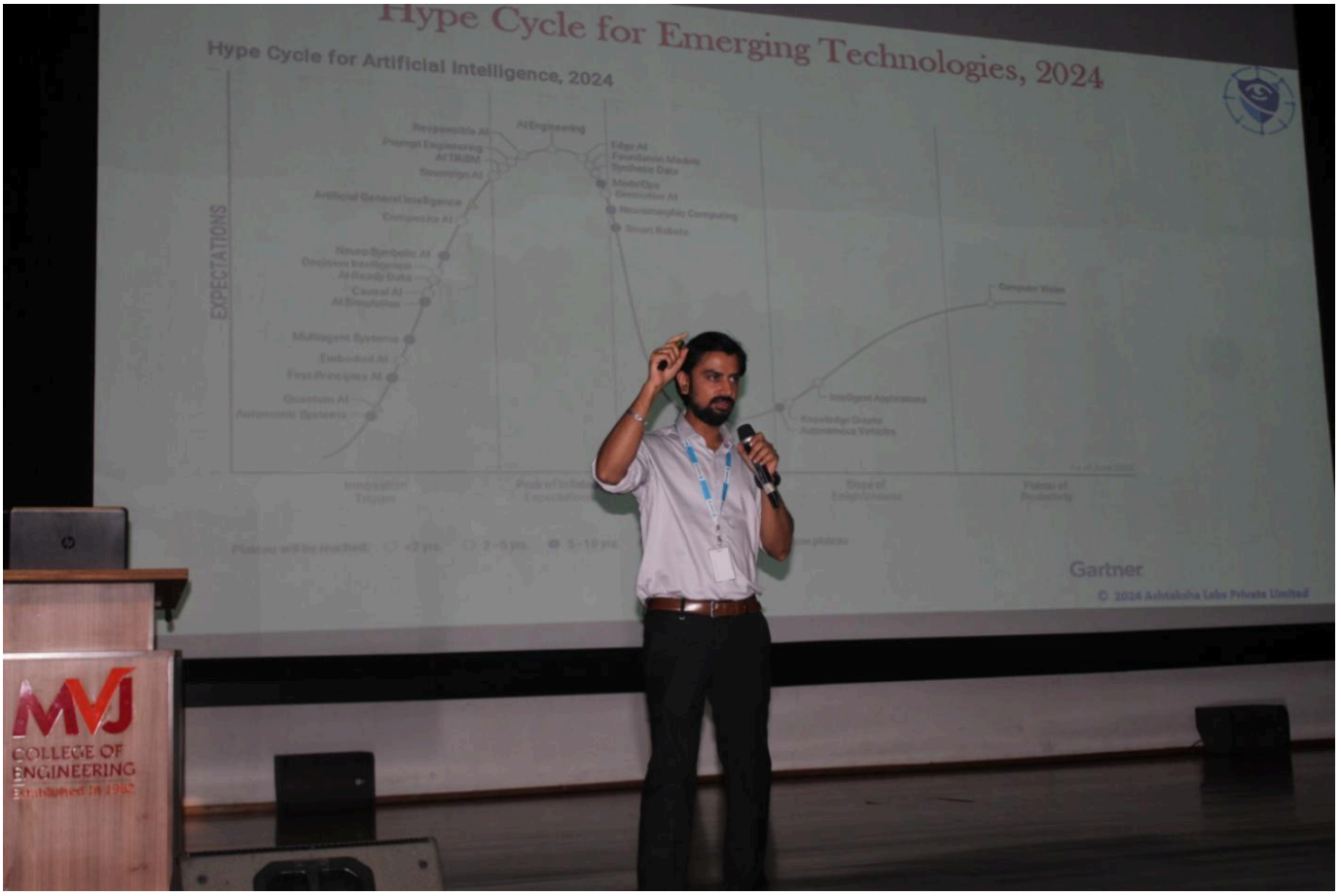
The guest speaker shared insightful perspectives on Artificial Intelligence (AI) and Cyber Security, covering the latest trends, challenges, and opportunities in these rapidly evolving fields. The presentation aimed to educate and enlighten the audience on the implications of AI and Cyber Security on modern society, fostering a deeper understanding of these critical technologies

Students actively participated In the event

The event saw enthusiastic participation from students, who engaged actively with the speaker, asking insightful questions and displaying a keen interest in the topic. The interactive session was marked by a high level of energy and excitement, as students seized the opportunity to learn from the speaker's expertise and experiences.

Here are the highlights of "AI and Cyber Security: A Double Edged Sword"

AI in cyber security presents a double-edged sword. On the positive side, AI enhances threat detection and incident response, improves security information and event management (SIEM), and enables predictive analytics for proactive security measures. Additionally, AI automates security processes, increasing efficiency. However, there is also a negative edge. AI increases vulnerability to AI-powered attacks, such as sophisticated deepfakes and AI-driven phishing. Moreover, AI algorithms can be biased, leading to false positives and misidentification. The effectiveness of AI also relies on high-quality training data.



Speaker explained about the hype cycle for emerging technologies in 2024

The hype cycle is a graphical representation of the maturity, adoption, and social application of emerging technologies. It begins with the Innovation Trigger, where early-stage technologies like Quantum Computing and Synthetic Data generate interest and excitement. As these technologies gain traction, they reach the Peak of Inflated Expectations, where AI and the Metaverse are currently, with high expectations, significant investment, and widespread media coverage, but often unrealistic expectations. However, when these technologies fail to meet expectations, they enter the Trough of Disillusionment, where Blockchain and Autonomous Vehicles are currently, facing challenges and skepticism. As understanding and performance improve, technologies like 5G and Edge Computing move up the Slope of Enlightenment, with growing practical applications. Finally, mature technologies like Cloud Computing and IoT reach the Plateau of Productivity, with widespread adoption and delivering real value and benefits.

To navigate this double-edged sword, organizations must implement AI responsibly and address potential risks. Continuous monitoring and updating of AI systems are crucial. Furthermore, collaboration between AI and cyber security experts is essential for success. By acknowledging the dual nature of AI in cyber security, we can harness its benefits while minimizing its drawbacks, ensuring a more secure digital future.

The outcomes of the guest lecture on "AI and Cyber Security: A Double Edged Sword" in points:

Knowledge Outcomes:

1. Understanding of AI and its applications in cyber security
2. Awareness of the benefits and risks of AI in cyber security
3. Knowledge of AI-powered threats and attacks
4. Familiarity with AI-driven security solutions and tools
5. Understanding of the importance of responsible AI implementation

Skill Outcomes:

1. Ability to analyze AI's role in cyber security
2. Skill to evaluate AI-powered security solutions
3. Ability to identify AI-driven threats and vulnerabilities
4. Understanding of how to implement AI responsibly
5. Ability to think critically about AI's impact on cyber security

Attitude Outcomes:

1. Appreciation for the importance of cyber security in the AI era
2. Awareness of the need for responsible AI development and use
3. Recognition of the potential risks and consequences of AI in cyber security
4. Interest in exploring AI-driven security solutions
5. Commitment to staying informed about AI and cyber security advancements

Behavioral Outcomes:

1. Application of knowledge to real-world cyber security scenarios
2. Implementation of AI-driven security solutions
3. Active participation in discussions on AI and cyber security
4. Continuous learning and professional development in AI and cyber security
5. Promotion of responsible AI practices in personal and professional settings

Faculty Coordinator of the event:

POSHITHA M (AP, Dept of CSE)