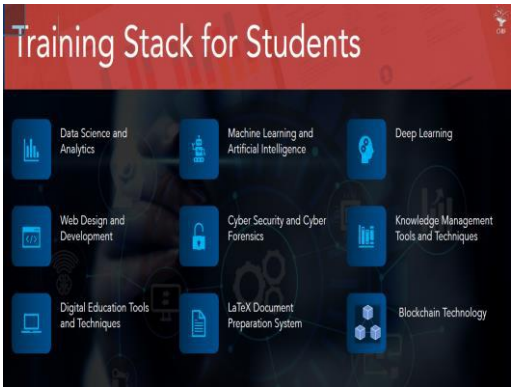
A Report on One day visit to
Computational Intelligence Research Foundation
Organized by Department of Computer Science & Engineering (Cyber Security)
21.02.2024



Submitted by: Mr. M. Mutharasu, Assistant Professor Dept of C.S.E (Cyber Security).
Attended by: Mr. T. Thiyagu Assistant Professor, Dept. of CSE(CS);
Ms. G. Kanishka, Assistant Professor, Dept. of CSE(CS);
Mrs. M. Sai Lakshmi Preethi, Assistant Professor, Dept. of CSE(CS)

Report received on 21.02.2024

Mode of Conduct: Offline
Purpose of Visit: Expression of Interest for MOU between CIRF, Chennai and MITS, Madanapalle.

About the Company:

CIRF is a Section 8 Company (Registered under Ministry of Corporate Affairs, Government of India). Established on 2017.CIRF a 12A and NGO Darpan certified company.
CIRF is a research-driven organization focused on providing learning and development and research-outsourcing services to students, researchers, and institutions. Company helps students develop in-demand technology skills to build better careers. Contribute to nation building through innovative mentoring and research-driven transformation.

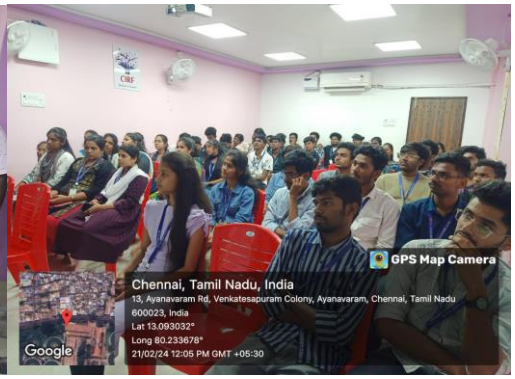
Visit to CIRF:

The faculty team started the journey at 3.30 AM and reached the Computational Intelligence Research Foundation located in Ayanavaram, Chennai at 10.00 AM.
At the outset, the faculty team was welcomed and briefed about the company, its vision and facilities of CIRF by **DR DOREEN ROBIN ME., PhD**, Founder and Director, CIRF.

After a brief introduction, a visit to the training facility of CIRF was done. The faculty team of MITS was accompanied by Dr. Doreen Robin M.E., PhD for the visit.
The MITS team visited the first section of the facility is training. In this session Dr. Doreen Robin ME., PhD clearly explained about industry standards and industry needs, How to gain a knowledge?

Preliminary discuss on expression of Interest for MOU:

Evaluating the potential for collaborative projects or initiatives that capitalize on the strengths of both institutions to tackle industry challenges and foster innovation.



Session conducted on AI with Robotics for III year students:

The relationship between AI (Artificial Intelligence) and robotics is tightly intertwined, as AI often serves as the intelligence behind robotic systems, enabling them to perceive, learn, and act autonomously.

AI with robotics represents the cutting-edge fusion of artificial intelligence (AI) technologies with the physical embodiment of robots, creating a new frontier of intelligent machines. This interdisciplinary field aims to imbue robots with cognitive abilities, enabling them to perceive, learn, make decisions, and act autonomously in the real world. At its core, AI empowers robots with advanced sensory capabilities, such as understanding their environment through cameras, lidar, and other sensors, and processing this data using machine learning algorithms for object recognition and navigation. This integration allows robots to autonomously make decisions, plan paths, and optimize tasks, paving the way for applications across various industries. From manufacturing, where AI-driven robots optimize production lines and perform quality control, to healthcare, with surgical assistants and rehabilitation aids, the impact of AI in robotics is profound.

Moreover, AI-powered robots are revolutionizing logistics and warehousing with efficient inventory management, transforming transportation with self-driving cars and drones, and even exploring distant planets and asteroids in space missions. However, challenges such as ensuring safety in human environments, addressing ethical considerations, and achieving seamless integration between AI algorithms and mechanical systems remain. Recent advances such as soft robotics, human-robot interaction, explainable AI, and swarm robotics showcase the rapid evolution of this field. Looking ahead, the future promises even more sophisticated AI-driven robots, tailored for specific tasks, capable of adapting to new environments, and collaborating seamlessly with humans in a wide range of applications, underlining the transformative potential of AI with robotics.

Course Outcomes:

CO 1: Analyse the intricate relationship between artificial intelligence (AI) and cyber-physical systems (CPS).
CO 2: Evaluate real-world applications of AI in cyber-physical systems across various industries, recognizing the transformative impact of AI-driven technologies on industrial processes, automation, and decision-making.
CO 3: Synthesize knowledge gained.
CO 4: To identify emerging trends and challenges in the integration of AI with cyber-physical systems, Strong AI, weak AI and Specialized AI.
CO 5: Demonstrate a comprehensive understanding of the ethical considerations, security implications, and potential societal impacts associated with the widespread adoption of AI-driven technologies in cyber-physical systems, emphasizing the importance of responsible innovation and decision-making in industrial settings.

Session conducted on Cyber Security for II year students:

Cybersecurity is the practice of protecting digital systems, networks, and data from unauthorized access, cyberattacks, and other malicious activities. It involves a combination of technologies, processes, and best practices aimed at safeguarding sensitive information and ensuring the integrity, confidentiality, and availability of digital assets. Cybersecurity measures include implementing firewalls, antivirus software, encryption techniques, and multi-factor authentication to prevent and detect intrusions.

Cyber security stands as a vital safeguard against threats to sensitive information and critical infrastructure. This field encompasses a broad spectrum of measures, from encryption protocols and firewalls to behavioural analytics and threat intelligence. As cyber threats evolve in sophistication, so too must the defence mechanisms. Artificial intelligence (AI) plays a pivotal role in this landscape, offering predictive analytics to anticipate potential breaches, automated responses to thwart attacks in real-time, and the ability to sift through vast amounts of data for anomalies. However, the cat-and-mouse game between cyber attackers and defenders persists, with ethical hacking, penetration testing, and continual updates to security protocols forming the frontline defence. The future of cyber security lies in the collaborative efforts of human expertise and AI-driven solutions to stay one step ahead of evolving threats, ensuring the integrity and resilience of our digital infrastructure.

Course Outcomes:

CO 1: Identify key cybersecurity threats: Students will gain the ability to recognize various cybersecurity threats prevalent in today's digital landscape, including malware, phishing attacks, and social engineering tactics.
CO 2: Understand cybersecurity defence mechanisms: Students will develop an understanding of different cybersecurity defence mechanisms and strategies employed to safeguard digital assets.
CO 3: Analyse real-world case studies: Students will analyse real-world cybersecurity breaches and incidents, understanding the root causes, impact, and lessons learned from these incidents.
CO 4: Apply best practices: Students will learn best practices for implementing cybersecurity measures within organizational contexts, including policy development, security awareness training, incident response planning, and continuous monitoring, enabling them to contribute to strengthening cybersecurity posture in their respective organizations.