About the Institution

Kongunadu College of Engineering and Technology (KNCET) is an Autonomous, self-financing Engineering College established in the year 2007, Approved by AICTE, New Delhi, Affiliated to Anna University, Chennai, Accredited by NBA(CSE, ECE, EEE & Mech), NAAC, Recognized by UGC with 2(f) & 12(B) and Certified by ISO 9001:2015. The College has 9 UG courses(AD ,AE,BME, Civil, CSE, ECE, EEE, IT and Mechanical Engineering) and 2 PG courses such as Applied Electronics and CSE. ECE and Mechanical departments have been recognized as approved research centers by Anna University. A Separate department Campus to Corporate is to train the students in the area of communication, soft skills and aptitude etc., through which obtaining top notch placements with the facilitation of diverse options in IT industries, core industries, ITES and startup firms respectively. The Kongunadu International Cell assists students explore opportunities to work and study in foreign countries. The college has obtained many awards & recognition from various government/private authorities and received research grants from funding agencies for doing projects, establishing MODROBS labs, organizing FDPs, STTPs, National and International Conferences,Seminars and Workshops. MSME Incubation Center and Unnat Bharat Abhiyan (UBA) schemes are approved by the Government of India. The College has signed MOUs with Industries, academics, hospitals and R&D Institutions. Various Professional societies, clubs and cells are supporting students to become industry ready graduates, to do higher studies and to become successful entrepreneurs. The sports teams have won many prizes in various events at National level including Zonal, Inter Zonal and University level Sports Championship. The College attracts outstanding students by virtue of its discipline, modern infrastructure, library and faculty members.

About the Department

The Department of Information Technology (IT) was established in the year 2007, with an intake of 60 students in it for UG course - B.Tech. IT. The Department is supported by a team of well qualified and highly experienced faculty members and technical staff who deliver their skills to the students through effective teaching-learning environment. The faculty members in the department are specialized in various areas like Wireless Networks, Network Security, Data Science, Cyber Security, Artificial Intelligence, Machine Learning, Image Processing, Cloud Computing, Mobile Computing and Software Engineering.

Address for Communication

Dr.K.Muthumanickam HOD/IT
Coordinator
FDP on
"AI-Powered Approaches for Modern Cybersecurity Challenges"
Kongunadu College of Engineering and Technology
Namakkal-Trichy Main Road,
Thottiam,Trichy(Dt)-621 215,
Tamilnadu
Mobile: +91-8012505010
E-mail ID: fdpit@kongunadu.ac.in
URL: **www.kongunadu.ac.in**

Online Faculty Development Programme on

"AI-Powered Approaches for Modern Cybersecurity Challenges"

19.02.2024 to 23.02.2024

Organized by

Department of Information Technology

KONGUNADU COLLEGE OF ENGINEERING AND TECHNOLOGY
(Autonomous)
Approved by AICTE, New Delhi,
Affiliated to Anna University, Chennai,
Accredited by NAAC with B++ Grade,
Recognized by UGC with 2(f)&12(B),
Accredited by NBA (CSE,ECE,EEE & MECH),
An ISO 9001:2015 certified Institution.
Namakkal-Trichy Main Road,
Thottiam,Trichy(Dt)-621 215,
Tamilnadu.
Website : www.kongunadu.ac.in

DEPARTMENT VISION AND MISSION

Vision

To become an Internationally Renowned Institution in Technical Education, Research and Development by Transforming the Students into Competent Professionals with Leadership Skills and Ethical Values.

Mission

- Providing the Best Resources and Infrastructure.
- Creating Learner-Centric Environment and Continuous Learning.
- Promoting Effective Links with Intellectuals and Industries.
- Enriching Employability and Entrepreneurial Skills.
- Adapting to Changes for Sustainable Development.

About the FDP

AI is transforming cybersecurity by enhancing threat detection, automating responses, and analyzing vast data for anomalies. These advancements help organizations proactively address evolving cyber threats while also presenting new challenges for security professionals. AI enhances the accuracy and speed of threat detection through advanced algorithms that identify complex attacks. Predictive analytics allows organizations to anticipate emerging threats, enabling proactive measures. AI-driven automation streamlines incident response processes, reducing response times and minimizing potential damage. Automated systems can handle routine tasks, allowing security teams to focus on more complex issues. AI monitors user behavior patterns to detect deviations that may indicate security breaches or insider threats. AI is revolutionizing cybersecurity by providing innovative solutions that enhance threat detection, automate responses, and improve overall security posture. However, organizations must also navigate the challenges associated with AI implementation to fully leverage its potential in combating modern cyber threats.

As AI technology advances, malicious actors can leverage it to develop more sophisticated attacks, posing new challenges for cybersecurity teams. AI systems can inherit biases from training data, leading to unfair outcomes that may disproportionately affect certain groups. There is a shortage of professionals with the expertise needed to develop and manage AI-driven cybersecurity systems, limiting their effectiveness. Seamlessly incorporating AI into existing security infrastructures can be complex and may necessitate significant adjustments.

FDP Objectives

- Enhance phishing detection mechanisms by analyzing email content and identifying malicious intent.
- Utilize AI to analyze transaction patterns for more effective fraud detection.
- Identify and prioritize vulnerabilities based on their potential impact and likelihood of exploitation.
- Continuously monitor systems to address vulnerabilities proactively before they can be exploited.
- Implement continuous verification of user and device access to ensure only authorized entities interact with critical resources.
- Invest in training and development programs to equip cybersecurity professionals with the necessary skills to manage AI-driven systems.

Course Contents

- Introduction to Cybersecurity
- Role of AI and ML in Cybersecurity
- The Growing Role of Deep Learning in cybersecurity
- The Impact of Adversarial AI and Machine Learning on Cybersecurity
- Deep Learning for Cryptanalysis
- AI-Powered Model creation and training simulations
- Evolution of Cybersecurity: Traditional vs. AI-driven Approaches
- AI in Fraud Detection: Case Studies and Best Practices in Cyber Security
- Future Trends in AI and Cybersecurity

Resource Persons:

The resource persons for the program shall include faculty members of the NIT, Host institute, Industry experienced and skilled experts from reputed organizations/industries.

Eligibility:

Faculty members of the AICTE approved institutions, Research scholars, PG Scholars, participants from Government, Industry Bureaucrats/Technicians/ Professionals/School Teachers and staff of host institutions.

Registration Procedure:

Candidates will be informed about their registration status via email and will receive a confirmation email upon successful registration. A digital certificate will be issued to all candidates who achieve a minimum of 80% attendance.