Paper Publication

Mentor Name	Domain/Category	Project Title	Project Abstract/PS Description
Dr. Kishorebabu Dasari	Cyber Security	AI-Powered Intrusion Detection System (IDS)	Description: Develop an intelligent IDS that uses machine learning/deep learning to monitor network traffic and detect malicious activities in real time. Objectives: Detect DoS, DDoS, brute force, port scans, and zero-day attacks. Improve detection accuracy and reduce false positives using ensemble or deep models.
		AI for Malware Analysis and Classification	Description: Classify malware samples based on behavior or static features using deep learning, enabling faster threat detection in antivirus systems. Objectives: Automate malware family classification. Use opcode, bytecode, or behavior logs for feature extraction.
		Phishing and Spam Detection with NLP	Description: Use NLP models to detect phishing and spam messages in emails, SMS, and chats by analyzing content, intent, and structure. Objectives: Build real-time phishing detection system. Use transformers (like BERT) for better contextual understanding.
		Quantum Machine Learning for Threat Detection	Description: Apply quantum machine learning (QML) techniques like variational classifiers to detect cyber threats in network logs or malware behavior. Objectives: Simulate quantum-enhanced models for security classification. Compare classical vs quantum approaches.
	Aggriculture	AI-Powered Crop Disease and Pest Detection	Description: Use image classification to detect plant diseases or pests from leaf images or field drone footage, helping farmers act early. Objectives: Classify diseases (e.g., rust, blight) using CNNs. Integrate with smartphone app for field usability
		AI-Powered Weed Detection System	Description: Identify weeds in agricultural fields using deep learning-based object detection (e.g., YOLO) and image segmentation (e.g., U-Net). Objectives: Detect weed locations for precision pesticide application. Deploy model on drones or field robots.