Defence Seminar	
Seminar Title	: Design of False Data Injection Attacks and Their Detection and Mitigation in a Cyber-Physical System
Speaker	: Sushree Padhan (Rollno : 519cs1007)
Supervisor	: Ashok Kumar Turuk
Venue	: Convention Hall, CSE Department
Date and Time	: 29 Jun 2025 (5 PM)
Abstract	: Cyber-physical systems (CPSs) are susceptible to various attacks, of which false data injection (FDI) attacks are more critical. An attacker can launch an FDI attack at any chosen location in a CPS and modify the cyber and physical system&rsquos data, causing errors in the system&rsquos proper functioning. It is important to analyze FDI attacks at possible vulnerable locations and detect and mitigate them to defend the CPS. This thesis is is an attempt in this direction. The thesis proposes strategies to design, detect, and mitigate FDI attacks in CPSs. A steady-state Kahman filter is used in the design of FDI attacks. Seven types of FDI attacks are proposed, in which each attack sequence follows a non-zero mean and zero-mean Gaussian distribution based on Kullback-Leibler (KL) divergence. It is observed that FDI attacks, in which the attacker simultaneously modifies the sensor measurements, actuator inputs, and physical system&rsquos state, generate maximum state estimation error. Next, a defense strategy is proposed for detecting and mitigating the non-zero mean and zero-mean Gaussian FDI attacks that simultaneously compromise the physical system, sensor measurements, and actuator inputs under a steady-state Kahman filter. A watermarking scheme is used to aid a Chi-square detector for attack detection. An attack mitigation scheme is proposed using control input synthesis and operating region concept. In this defense strategy can detect and reduce the FDI attacker&rsquos effect on the system. Considering a time-varying Kahman filter, the non-zero mean Gaussian FDI attack types are designed, where the attacker simultaneously compromises the physical system, sensor measurements, and actuator sing a time-varying compensition signal are proposed to mitigate the attacker forsquos effect. It is observed for the proposed defense strategy against FDI attacks is proposed. In the first stage of the defense strategy, the watermarking technique aids a Chi-square detector for attack detection. In the second stage of the