Title of the Course: Security Aware CPS and IoT Design

1. Credit requirement:(L-T-P: 3-0-0, Credit: 3)
2. Please select the committee for Approval: PGPEC
3. Name of the Dept: ATDC
4. Please Specify the Level of the Subject: PG level
5. Whether the subject will be offered as compulsory or elective: Elective
6. Prerequisite(s) for the subject, if any (Please give the subject numbers and names): Not required
7. **Course Objective:** Cyber-physical systems (CPS) integrate sensing, control, networking and realtime computing elements into physical objects and infrastructure, connecting them to the Internet and to each other. On the other hand, Internet of Things (IoT) refers to any systems of interconnected people, physical objects, IT platforms, as well as any technology to manage the physical world enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies.

   Recent research reveals IOT is suffering from many widespread security issues. In fact, Attackers are being able to leak private information and attain complete remote control over IOT systems. Cyber physical systems have suffered from even greater consequences due to security vulnerabilities because of infrastructures' growing reliance on cyber physical systems. Traditional CPS devices used physical isolation for protection. However, recent CPSs have been deployed in places where they rely on direct connection to the Internet, or in places where an attacker could potentially have physical access to the device, vastly changing the threat model of existing CPS standards.

   Lack of security awareness during the design of the devices is one of the main causes of these vulnerabilities, as IoT/CPS devices tend to have a very large surface area that can be attacked. Consequently CPS and IOT based applications suffer many security flaws and adversarial attacks. This course discusses the basic security requirements for CPS and IOT, justifies with different case studies why security should be a primary concern during their development phase and focuses to introduce fundamental concepts for security aware design of them.
8. **Study Materials:**

   In this course, majority of the topics will be covered through lectures on important concepts available in the recently published articles, and presentations of the related papers. Some relevant books are:

   Books:

   - "Securing the Internet of Things" by Shancang Li, Li Da Xu, Syngress Publishing, 2017.
   - "Security Aware Design for Cyber Physical Systems" by Chung-Wei Lin, Alberto Sangiovanni-Vincentelli, Springer, 2017.
9. **Syllabus**

   (a) **Security Issues of Cyber Physical System [4L]**
   Types of attack models in CPS, Jamming attack in CPS and Anti-jamming, Case Study: Jamming Attacks on Mobile CPS in Target Tracking Applications

   (b) **FSM based and Graph based Security Aware CPS design [2L]**

   (c) **Security aware CPS design methodologies [6L]**
   Security mechanisms for CAN, Security aware TDMA Based Real Time System, Security mechanisms for V2V Communication

   (d) **ICS/SCADA System and Embedded Systems Security for CPS [4L]**

(e) **Security Requirements for Internet Of Things** **[3L]**
Introduction to IoT, Relationship Between CPS and IoT, Threats to Internet Of Things (IOT) Architectures

(f) **IoT threats specific to Access Control and Privacy** **[2L]**
Insufficient Authentication/Authorization, Threats to Access Control, Privacy, and Availability.

(g) **Authentication/Authorization for Smart Devices** **[4L]**
Transport Encryption, Secure Cloud/Web Interface, Secure Software/Firmware, Physical Layer Security.

(h) **IOT Node Authentication** **[4L]**
Public-Key-Based Authentication, Identify-Based Authentication, Lightweight Cryptography.

(i) **Security in Enabling Technologies** **[4L]**
Security in Identification and Tracking Technologies, Security in Integration of Wireless Sensor Network and RFID

(j) **Security Challenges for cloud assisted IoT applications** **[4L]**
Secure data sharing challenges, Encrypted Computation. Case Studies: Security for IOT in Retail and Health-care.

10. Names of the faculty members of the Department/Centers/School who have the necessary expertise and will be the willing to teach the subject (Minimum two faculty members should be willing to teach the subject)

    Ayantika Chatterjee, Soumyajit Dey

11. Do the contents of the subject have an overlap with any other subject offered in the Institute?

    Related Subjects offered by the Institute:

    CS61063: Computational Foundations of Cyber Physical Systems
    CS61066: Architecture and Protocols for Internet of Things

    Computational Foundations of Cyber Physical Systems (CS61063): Cyber-physical systems, which consist of physical systems tightly integrated and/or controlled by software, are ubiquitous in many safety critical domains, including automotive, avionics, railways, healthcare, atomic energy, power, and industrial automation. The principles of design and implementation of cyber-physical systems are remarkably different from that of other embedded systems because of the tight integration of real valued and dense time real time systems with software based discrete automated control. The objective of this course is to develop an exposition of the challenges in implementing a cyber-physical system from a computational perspective, but based equally on the principles of automated control. The course aims to expose the student to real world problems in this domain and provide a walk through the design and validation problems for such systems.

    Architecture and Protocols for Internet of Things (CS61066): This course introduces the basic components of IoT and their interdependencies, deployment models, and fundamental concepts of IoT networking. This course also includes data and communication protocols for IoT network, data handling in IoT, analytics, and data management for IoT devices. Cloud-centric IoT and virtualization with IoT system management are also included along with industrial IoT and interoperability in IoT.

    - Approximate percentage of overlap: 5%
    - Reasons for offering the new subject in spite of the overlap:
      Both the existing courses mostly concentrate on fundamental challenges of designing CPS and IOT and discusses their respective protocols. However, IoT/CPS systems are growing with immense importance in complexity and ubiquity. As they become smarter and as the interaction between the physical and cyber systems increases, the physical systems become increasingly more susceptible to the security vulnerabilities in the cyber system. Hence, if no work is done to improve sensing security, cyber security and control security, IoT/CPS based applications are bound to face severe challenges due to external hacking and adversarial attacks. Thus, a systematic approach towards

examining IoT/CPS devices is much needed. In this course, we primarily discuss how to incorporate these security concerns mostly in the design phase of different CPS/IOT components.