Global Initiative of Academic Networks

Course (Feb. 24 - 28, 2025)

TRUSTWORTHY SYSTEMS: DESIGN AND CHALLENGES

शिक्षा मंत्रालय
MINISTRY OF EDUCATION
सत्यमेव जयते

Department of Computer Science and Engineering
Indian Institute of Technology Patna, Bihar

Overview

Trustworthy systems are essential for ensuring user confidence and data protection in today's interconnected world. They prevent harm, safeguard sensitive information, and maintain business continuity. These systems are crucial in preventing fraud, ensuring security and safety in critical sectors, and promoting economic growth through innovation and investment. Trustworthy systems also help organizations comply with legal and regulatory requirements and contribute to national security. They have a positive social impact by reducing inequality and ensuring fair treatment. By fostering trust in technology, these systems enable the responsible and beneficial use of digital advancements, creating a safer and more reliable digital ecosystem.

Objectives

The primary objectives of the course are as follows:

- Expose participants to understand principles of trustworthy systems.
- Expose participants to different types of security attacks and possible defenses.
- Knowledge of trustworthy AI, using key concepts of security and AI.
- Expose participants to practical problems, solutions, and standards in different areas such as finance, transport and supply chain.

Foreign Faculty: Professor Carsten Maple

He is the Principal Investigator of the NCSC-EPSRC Academic Centre of Excellence in Cyber Security Research at the University and Professor of Cyber Systems Engineering in WMG. He is also a co-investigator of the PETRAS National Centre of Excellence for IoT Systems Cybersecurity where he leads on Transport & Mobility. He is a Fellow of the Alan Turing Institute, the National Institute for Data Science and AI in the UK, where he is a principal investigator on a $5 million project developing trustworthy national identity to enable financial inclusion. Prof. Carsten has published over 350 peer-reviewed papers and is co-author of the UK Security Breach Investigations Report 2010. He was formerly Chair of the Council of Professors and Heads of Computing in the UK, a member of the IoTSF Executive Steering Board, an executive committee member of the EPSRC RAS Network and a member of the UK Computing Research Committee, the ENISA CarSEC expert group, the Interpol Car Cybercrime Expert group and the Europol European Cyber Crime Centre.

Host Faculty: Professor Somanath Tripathy

He is a Professor in the Computer Science and Engineering Department of IIT Patna. He has published more than 120 research papers in different journals and conferences of repute. He was the Associate Dean, Academics from January 2016 to March 2017 and the Associate Dean, Administration from July 2021 to Nov 2023 at IIT Patna. His research interests include lightweight cryptography, security issues in resource-constrained devices, blockchain, Malware detection and Secure machine learning. He has been PI and Co-PI of several security-related projects.

Course Modules and Topics

Fundamentals of Security and Resilience: Securing the Future, Current trends in technology, cutting-edge attacks, and defense strategies, Security is not enough, Proactive risk management and recovery strategies, Privacy and Security, Digital Identity, Challenges such as identity theft and privacy, best practices for trustworthy digital identity management.

Data Privacy and Synthetic Data: Synthetic Data, Utility, and privacy preserving properties, Developing Trustworthy Synthetic Data, Practical techniques for generating useful synthetic datasets while maintaining data security and privacy, Trustworthy AI in Finance, Addressing data privacy, fairness, and transparency concerns with regulatory compliance.

Trust and Security in Emerging Technologies: Trustworthy Transport and Mobility, Ensuring safety, data privacy, and resilience against cyber threats, Trust in the Supply Chain, How Blockchain can help make Trustworthy Systems, Enhancing trust, data integrity, and transparency in transactions.

Cryptography and Advanced Security Techniques: Encryption algorithms, digital signatures, and protocols to secure data and communication, Advanced cryptography, including homomorphic encryption, zero-knowledge proofs, and secure multiparty computation. Privacy-preserving Machine Learning, Attacks, Defenses and Verifiability.

System Security and Cloud Computing: Analysis of the threat landscape, identifying vulnerabilities, and mitigating attack vectors, Understanding the unique security challenges in cloud computing, and protecting sensitive data and applications in cloud environments.

You should attend if you are

- Executive, engineer, and researcher from manufacturing, service, government, and R&D organizations.
- Student (BTech, MSc, MTech, PhD) and faculty from academic and technical institutions.

Course Fee

	Early Bird Registration
Students (UG/PG/PhD)	₹ 1,000
Academic Institutions (Faculty)	₹ 2,000
Industry/R&D Organizations	₹ 5,000

Registration link: https://forms.office.com/r/P6mqDFSeUg

No TA DA will be provided to the participants. Participants have to arrange their own accommodation and food. However, limited shared accommodation may be made available (subject to availability) in the Institute Hostels/ Guesthouse on request on first come first serve basis. Payment for accommodation and food is extra as per actual.

Organizing Institute: IIT Patna, Bihar

Indian Institute of Technology Patna is one of the new IITs established by an Act of the Indian Parliament on August 06, 2008. Patna which was known as Patliputra has been a center of knowledge since long has been attracting visitors and scholars from many parts of the world. This has been a land of visionaries. Some of the legends from this region include Lord Gautam Buddha, Lord Mahavir, Guru Gobind Singh, the famous astronomer Aryabhatta and the first President of India, Dr. Rajendra Prasad. IIT Patna has ten departments, including Computer Science & Engineering. The Department of Computer Science and Engineering at IIT Patna was established in 2008, with B.Tech in CSE and a PhD Program. The mission of the Department is to impart high-quality graduate and undergraduate education and carry out leading-edge research in various disciplines of Computer Science & Engineering. The Department also offers Ph.D. in research areas such as Cloud Computing, Machine Learning, Computer Vision, Network Security, Blockchain, Machine Learning Security, Malware detection, Cloud and IoT Security, NLP, and various other domains.

Patron
Prof. TN Singh

Course Coordinator
Prof. Somanath Tripathy
Dr. Satendra Kumar

Contact: som@iitp.ac.in
502, Block-2, CSE, IIT Patna, Patna, 801016, Bihar, India