Title: Machine Learning in Hardware Security

Speaker: Prof. Urbi Chatterjee

Date: Wednesday, 7th September, 2022

Time: 6:40 PM

Venue: L18

Abstract:

Internet-of-Things frameworks have opened up an ubiquitous sensing-communicating-actuating network with information sharing across platforms, blended seamlessly in various areas of modern day-to-day living. But as with most emerging technologies, innovation comes first, and security is only an afterthought in reaction to discovered vulnerabilities. The "smart" devices deployed in IoT frameworks usually generate large quantities of security-sensitive data and create an alluring threat surface for an attacker to compromise the security and privacy of millions of users. Now, in past decade we have seen the growing contribution and success of ML and DL algorithms in every aspect of contemporary works. This has also drawn serious attention from the attackers to exploit ML/DL algorithms to find different vulnerabilities in security-critical applications, even at device level.

This talk is about sharing few ideas about how hardware security and machine-learning can be intertwined together. We will discuss three interesting testcases about a) how ML-based attacks can jeopardize security assurance of unconventional hardware root-of-trust primitives, b) how a malicious app can launch an ML-based acoustic side-channel attacks on the microphone of a smart mobile device and retrieve the whole call history without accessing the contact book, c) On the other hand, how ML-based analysis can be used as countermeasure against Hardware Trojan insertion in integrated circuits.

Bio:

Urbi Chatterjee is an Assistant Professor in the Department of Computer Science and Engineering, Indian Institute of Technology Kanpur since 2021. Before joining IITK, she completed her Ph.D. from Indian Institute of Technology Kharagpur in the year 2020. Her broad area of research is Hardware Security. She mainly works on physically unclonable functions, secure authentication and key exchange protocol design for internet-of-things, unmanned aerial vehicles and smart cars etc. She is also recently exploring topics in the area of automated protocol verification tools, security aspects of modern computing paradigm, near-field and far-field side channel attacks such as acoustics, electromagnetic radiations and network data remanence.