IITB TRUST LAB

DIGITAL : SECURE : RESPONSIBLE

Internship Projects at Trust Lab

Project – 1
Advised by: Prof. Udayan Ganguly
Secure Remote Programming for Edge AI Microcontrollers Description : To create a secure web interface where the users sitting at a remote location can access the FPGA/microcontrollers which will be capable of running A.I. loads.

Project – 2
Advised by: Prof. Manjesh Kumar Hanawal
AI for cybersecurity: The project involves running malicious scripts collected from various sources like Virus Total, Malware Bazar, etc. in sandbox environment to understand their behaviour. The goal is to develop rich malware dataset that could be used to train ML algorithms

Project – 3
Advised by: Prof. Manjesh Kumar Hanawal
eBPF for Blocking malicious process: In cybersecurity it is important that once a malicious process is detected, it need to be blocked from creating child processes or killed. eBPF provides a suite of methods to manipulate with the packets at the Kernel level. The project will explore how eBPF can be used to block/kill malicious process.

Project – 4
Advised by: Prof. Swaprava Nath
Networks and Auction Design: The auction of a single indivisible item is one of the most celebrated problems in mechanism design with transfers. Despite its simplicity, it provides arguably the cleanest and most insightful results in the literature. When the information of the auction is available to every participant, Myerson [17] provided a seminal result to characterize the incentive-compatible auctions along with revenue optimality. However, such a result does not hold in an auction on a network, where the information of the auction is spread via the agents, and they need incentives to forward the information. In recent times, a few auctions (e.g., [10, 15]) were designed that appropriately incentivize the intermediate nodes on the network to promulgate the information to potentially more valuable bidders. We want to extend the problem of auction on a social network. See this for more details:
https://docs.google.com/presentation/d/1BhZ37zbb3FlYw_8VHsvvgtcRw0NJWh4MKTkVNxzfGNk/preview

Project – 5
Advised by: Prof RK Shyamasundar
Privacy in a Blockchain: Build applications on TestNet on Ripple for health care applications.

Project – 6
Advised by: Prof. Prof RK Shyamasundar
Analyse Fairness in various Blockchain Platforms: Assess fairness of varieties scalable solutions of scalability on blockchain platforms

Project – 7
Advised by: Prof. Ganesh Ramakrishnan
HIerarchical FEDERAted Learning for the INdian healthcare SYSTem (HI-FEDERAL-INSYST): The decentralized nature of healthcare data contributes to the difficulty in implementation of Machine Learning (ML) in the hospital ecosystem. A new method, Federated Learning (FL) has emerged as a promising solution enabling a central entity to gather insights from decentralized sources without sharing raw data. However, even application of FL in the Indian healthcare system presents unique challenges. Firstly, the data sharing rules vary within and outside organizations, leading to a complex hierarchy of trust. Secondly, different healthcare facilities use varied data acquisition devices and protocols, leading to disparities in data distribution. Thus, the decentralized nature of healthcare data and the hierarchical structure of the Indian

healthcare system pose significant obstacles to the successful application of ML and classical FL. To address these challenges, in the internship we propose a partially decentralized FL design. The research will focus on resolving the following key questions: 1) how to design a hierarchical communication topology and aggregation algorithms across different data distributions, 2) how to reason about different levels of privacy and convergence across different levels of hierarchy, and 3) rigorously evaluate the effectiveness of our proposed FL algorithm and other federated learning algorithms on healthcare datasets within a hierarchical topology.

Project – 8
Advised by: Prof. Kameswari Chebrolu
PULSE: Practical and Upbeat Labs for Security Education: The goal of the internship is to help in developing 20+ gamified security labs across 4 different security areas, that can be conducted at scale, across different student operating systems with minimal setup costs and with support for automated assessment. 2-4 based on availability.

Project – 9
Advised by: Prof. Vinay Ribeiro
Design and development of Smart Contract applications for Algorand Blockchain: Algorand is a blockchain created by Turing Award winner Silvio Micali. IIT Bombay is part of an Algorand Center of Excellence led by Purdue University, called MEGA-ACE. One of the objectives of MEGA-ACE is to build applications on top of the Algorand Blockchain, such as a CV registry for easy verification of CV details, land record registry etc. This project will involve building such applications, using the TEAL language used by Algorand. A basic understanding of blockchains would be desirable before the internship begins.

Project – 10
Advised by: Prof. Manoj Prabhakaran
Understanding the limits of Information-Theoretically Secure Multi-Party Computation: There is a rich landscape of secure multi-party computation models. While in some models, all functions can be securely computed, in many other models that is not the case. Further, in many such models, we do not understand which functions can be computed and which ones cannot be. In this project, we shall study some recent progress on such questions, and try to make further progress.