## V Pramodh Gopalan

☑ pramodh@iitk.ac.in | 🖆 pramodh-g.github.io | 🖸 github.com/pramodh-g | 🔊 +91-7400047180

#### ACADEMIC DETAILS

Examination	Institute	Year	CPI/%
Graduation	IIT Kanpur	2023	9.12/10.0
High School, CBSE	Ryan International School, Mumbai	2019	96.2
Secondary School, CBSE	Delhi Public School, Mumbai	2017	10/10

Research Interests: Statistics, Privacy and Security of Machine Learning, Stochastic Optimization.

#### SCHOLASTIC ACHIEVEMENTS

- Academic Excellence Award for exceptional performance in Academics at IIT Kanpur. (2020)
- Secured All India Rank 217 in JEE Advanced 2019 among 230K eligible aspirants. (2019)
- Secured All India Rank 217 in JEE Mains 2019 among 1.1 Million candidates. (2019)
- Awarded the prestigious KVPY fellowship by Dept. of Science and Technology, Govt. of India. (2019)
- Amongst the top students across the country to appear for the nation-level olympiads in Physics and Astronomy, INPhO and INAO respectively. (2019)
- Participated in a training camp for appearing in **INMO**(Indian National Math Olympiad). (2018)
- Recipient of the National Talent Search (NTSE) scholarship awarded by the NCERT. (2017)

### Internships and Research Projects

Defending against Poisoning Attacks in Machine Learning [May 2021-Present] Research Intern | Prof. Alina Oprea NDS2 Lab, Northeastern University

- Working on Creating **Defenses** against **Poisoning** Attacks in **ML**, using **Ensembles** of models.
- Extended existing implementations of attacks to accommodate **Drebin** and **MNIST** Datasets, and tested the attack efficacy on them.
- Formulated a theoretical framework, and derived a lower bound on the effectiveness of the defense.
- Carried out **experiments** to validate the **theoretical** claims, and **visualized** the results **interactively** using libraries like **Pluto.jl** and **Makie.jl**.
- A report can be found *here*.

# Image Preprocessing as an Adversarial Defense • Code Here Research Project | Prof. Vireshwar Kumar

[Aug 2020- Jan 2021]

IIT Delhi

- Examined CV based navigation models for **Unmanned Aerial Vehicles** to determine **adversarial weak-**nesses
- Conducted a **literature review** on **Defenses** to Adversarial Examples from the **Reading List** of Nicholas Carlini.
- Implemented various Adversarial Defenses based on Image Preprocessing, such as Blurring, Pixel Shuffling, Secret Key based Block Shuffling.

Decentralised Mechanism Design using Blockchains © Code Here [Oct 2020 - Nov 2020] Course Project CS711 | Guide: Prof Swaprava Nath IIT Kanpur

- Learned about various problems in Blockchains related to **privacy** and tackling them using modern Cryptographic Primitives like **Secure MPC**.
- Modelled a game theoretic version of privacy problem in Blockchain as **Normal Form Game** and inferred various **equilibriums** that may be present according to different applications.
- Presented an analysis of how effective the current Enigma Protocol is, and proposed an **alternative better approach** for a particular step by using **VCG Mechanisms**.

## KEY PROJECTS

## Model Zoo: A study in GANs (7) Code Here

[Summer 2020] IIT Kanpur

Summer Project | Programming Club

- Learned about Convolutional Neural Networks in depth and implemented architectures like **ResNET** and **VGG** using **Pytorch**.
- Carried out a literature review on GANs and implemented basic GAN and DCGAN on MNIST and CIFAR-10 Datasets.
- Read papers on Context Encoders and implemented it using Pytorch.
- Studied Audio Generation using WaveGAN.
- Created Blogs mentioning related Literature, along with Results and Architectures.

Summer Project | Stamatics Club

- Explored various sampling methods like Inverse Transform, Accept-Reject, Bernoulli Factories, Importance Sampling, Box-Muller and Ratio of Uniforms used in Monte Carlo Algorithms.
- Studied optimization methods like **SGD**, **Newton-Raphson**, **MM** and **EM** algorithms used in estimation of parameters.
- Implemented Probit Regression model in Julia on the titanic dataset to estimate chances of survival.
- Introduced to MCMC and MH algorithms and topics in Bayesian Modelling such as Bayesian Linear and Logistic Regression

InfoSec IITK

[Feb'20 - Apr'20]

Semester Project | Association of Computing Activites

IIT Kanpur

- Studied various exploits such as **Binary Exploitation**, **SQL injection**, **Steganography**, and tools to use them like **gdb**, **SQL map**, **Steghide**, and **StegSolve**.
- Participated in numerous CTFs as a part of the project evaluation.

#### TECHNICAL SKILLS

- Programming & Scripting Languages: C++, C, Python, Julia, Bash, R
- Libraries and Frameworks: Pandas, NumPy, seaborn, scikit-learn, PyTorch, PyTorch-Lightning, Flux.jl, Tensorflow/Keras(familiar).
- Utilities: Git, LATEX gcov, gtest, Markdown, Docker

### Relevant Coursework

- Computer Science: Fundamentals of Programming, Data Structures and Algorithms, Game Theory and Mechanism Design, Computer Organisation, Software Development, Operating Systems<sup>†</sup>, Theory of Computations<sup>†</sup>, Advanced Algorithms<sup>†</sup>, Introduction to Machine Learning<sup>†</sup>
- Mathematics: Real Analysis, Linear Algebra, Probability Theory, Logic for CS, Bayesian Analysis, Statistical Simulation and Data Analysis in R <sup>†</sup>, Markov Chain Monte Carlo <sup>‡</sup>, Numerical Methods in Engineering <sup>‡</sup>.
- Online Courses: Reliable and Interpretable AI (ETH Zürich), Introduction to Deep Learning using Tensorflow (Coursera)

‡ - Upcoming Courses † - Ongoing Courses

## Positions

## Secretary, Programming Club

Programming Club, IITK

[May 2020 - Apr 2021] IIT Kanpur

- Part of a team of 20 students responsible for holding various events to the campus community of more than
  over 8000 students
- Responsible for managing a Competitive Programming Competition for students of the institute for a month.
- Hold

#### Mentor - Julia for Machine Learning

[Apr 2021 - Jul 2021]

IIT Kanpur

Association for Computing Activities, IITK

- Introduced Julia, A High Performance Language to about a group of 30 students.
- Delivered Lectures on various aspects of Julia, Such as Multiple Dispatch, Type Inference, Meta-programming and Loop Fusion.
- Introduced them to fundamental concepts in Machine Learning such as Probability and Statistics, Different modes in Automatic Differentiation, Gradient Descent.

Student Guide

[Nov 2021-May 2021] IIT Kannur

Counseling Service IIT Kanpur

Mentored six freshmen throughout their first year and exposed them to academic and extracurricular opportunities available in the Institute.