Sahil Jain
Computer Science & Engineering
Indian Institute of Technology, Bombay
Email: jsahil730@gmail.com

UG Fourth Year(B.Tech.)
DOB: 09/07/2002
+91-8955598892

Education

Graduation with Honors	IIT Bombay	2022	9.66
Intermediate/+2	CBSE	2018	95.20
Matriculation	CBSE	2016	10.00

Interests

Cybersecurity (Cryptography, Reverse Engineering), SAT solvers, Probabilistic Programming, Systems and Architecture

Achievements

- Secured **All India Rank 2** in **IIT JEE Advanced** among 160 thousand shortlisted candidates 2018
- Achieved **All India Rank 40** in **JEE Mains Paper 1** examination among 1.04 million candidates 2018
- Bagged **First Position** in **InCTF Nationals** organized by Team bi0s among several Indian university teams 2022
- Ranked **4th** in India region and **28th** worldwide in the prestigious **CSAW CTF**, organized by NYUSEC 2021
- Awarded **Gold & Silver Medals** in International Olympiad in Cryptography, **NSUCRYPTO-2020** 2020
- Bagged **Advanced Performer (AP)** grade in 2 courses, awarded only to **Top 1 %** of the total students 2019
- Recipient of National Talent Search Examination **(NTSE)** Fellowship, awarded by NCERT 2016

Internships & Projects

Tapestry Pooling *September 2020 - July 2021*
Prof Manoj Gopalakrishnan, Prof Ajit Rajwade *RnD Project*

- Collaborated in a team of scholars from several institutes towards the growth of **Tapestry**, a novel quantitative **non-adaptive** pooling strategy to test large number of Covid samples, providing **upto 10x cost savings**
- Studied various **probabilistic programming** algorithms like **Markov Chain Monte-Carlo** used for solving the under-determined inverse problem of recovering individual sample concentrations from pooled results
- Assisted in the incubation of a startup for **mass commerical deployment** of the technology across the country
- Worked on and oversaw development of the cloud architecture for ease of use of the service for the consumers

Analysis of Random Number Generators *Spring 2021*
Prof Bernard Menezes | Course Project *Advanced Network Security & Cryptography*

- Performed security analysis for several popular RNGs like **Mersenne Twister**, **LCG** & **Dual-EC-DRBG**
- Demonstrated seed recovery in **Mersenne Twister** from merely **3 consecutive outputs** using **Z3 SMT solver**
- Implemented **Lattice & SMT-based** attacks on **Truncated LCGs** for recovery of seed & hidden parameters
- Demonstrated the well-known back-door in the "Cryptographically-Secure" Elliptic-Curve based **Dual-EC-DRBG**

Spectre : Exploiting Speculative Execution *Autumn 2021*
Prof Bernard Menezes | Course Project *Computer Architecture*

- Demonstrated **Proof-of-Concept** for Spectre vulnerabilities using **Flush+Reload & Evict+Reload** techniques
- Utilized **timing-based side-channel attacks** to exploit the vulnerability and access arbitrary memory

Upsell campaigns in Order History *May 2021 - July 2021*
Microsoft India | SDE Intern *Hyderabad, India*

- Implemented a feature to display **upsell campaigns for M365 & Xbox** on Microsoft account's order history page
- Utilized the account's current subscription status to retrieve and display just the relevant upsell campaings
- Worked in **ReactJS** for frontend and **C#** for backend and performed end-to-end testing of the complete functionality

Video Denoising using Low-Rank Matrix Completion *Spring 2020*
Prof Ajit Rajwade | Course Project *Advanced Image Processing*

- Implemented a three-step algorithm to denoise multi-channel videos containing a mixture of gaussian, poisson and impulsive noise by formulating it as a **Low-Rank Matrix Completion** problem, using **MATLAB framework**

SCLP Compiler *Spring 2021*
Prof Uday Khedker | Course Assignment *Implementation of Programming Languages*

- Constructed an end-to-end compiler for a C-like custom language using lex for scanning and yacc for parsing

Hostel Management System *Spring 2021*
Prof Umesh Bellur | Course Project *Database Lab*

- Created a **Hostel Management** web-application based on **MVC Architecture**, using **NodeJS** and **PostgreSQL**
- **Optimized database design** for efficient queries and developed the product keeping in mind users' needs

MyRacket Interpreter *Spring 2019*
Prof Amitabha Sanyal | Course Assignment *Abstractions and Paradigms in Programming*

- Designed an interpreter of a custom language called **MyRacket**, using **Environment Model** of Evaluation

xv6++ *Autumn 2021*
Prof Mythili Vutukuru | Course Assignment *Operating Systems*

- Enhanced the existing **xv6 operating system** with a priority based **weighted process-scheduling algorithm**
- Added enhancements such as **lazy heap allocation**, **copy-on-write fork** & **userspace synchronization primitives**

Splitwise Clone *Autumn 2019*
Prof Amitabha Sanyal | Course Project *Software Systems Lab*

- Developed an Android application for record-keeping transactions with friends, allowing partial repayments of money

RacKonnect : Social Network *Spring 2019*
Prof Amitabha Sanyal | Course Project *Abstractions and Paradigms in Programming*

- Developed a **Social Networking** application in **Racket**, using **Object Oriented Programming**

Cryptanalysis : Substitution Cipher Cracker Tool *Spring 2019*
Prof Amitabha Sanyal | Course Assignment *Abstractions and Paradigms in Programming*

- Created mono-subsitution-cipher cracker in **Racket**, utilizing ETAI & Dictionary-Closure cryptanalysis techniques

Arithmetic in Finite Fields *Winter 2019*
Prof Manoj M. Prabhakaran | Winter Project

- Studied efficient algorithms for carrying out arithmetic over **Finite Fields** of characteristic 2, and explored developing alternate algorithms based on a new transformation

Spanning Tree Protocol : Implementation *Spring 2020*
Prof Varsha Apte | Course Assignment *Computer Networks*

- Implemented **Spanning Tree Protocol** from scratch, which is used in **Switching and Bridging** in **C++**

Positions Of Responsibility

Technical Manager | *Cybersecurity Club* *June 2021 - Present*

- Responsible for **leading and representing the institute** in Security Hackathons, CTF contests and similar events
- Responsible for **promoting cybersecurity culture** and enlargening the cybersecurity community in the institute
- Responsible for organizing and conducting cybersecurity-aimed technical events and sessions in the institute

Convener | *Cybersecurity Club* *July 2020 - May 2021*

- Developed and deployed several challenges for institute's **internal CTF** with more than **100 active participants**
- Created beginner-tutorial blogs on wiki site with **1000s** of daily visitors worldwide, teaching them about **pwning**

Teaching Assistant | *CS 101 - Introduction to Programming* *November 2020 - February 2021*

Teaching Assistant | *PH 108 - Electricity and Magnetism* *January 2020 - May 2020*

Technical Secretary | *Hostel 16 Technical Council* *July 2018 - April 2019*

Technical Skills

Programming Languages	: C/C++, Julia, Python, Java, C#, SQL, SageMath, Rust, Golang, Bash
Web Development	: NodeJS, ReactJS, JavaScript, TypeScript, Django, PHP
Software Tools	: Z3, Ghidra, gdb, pwntools, Docker, Git, Android Studio, GNU Make, WireShark, ns-3

Extracurricular Activities

- Served as the **captain** of IIT Bombay's representative Capture The Flag team, **IITBreachers** **2021-22**
- Bagged **Gold Medal** as a team in **Network Security Hackathon** event in **Inter-IIT Tech Meet** **2021**
- Bagged **2nd** position out of 95 participating teams in CTF organised by **Cybersecurity Club, IITB** **2020**
- Secured global team rank **227** out of 15817 teams in **picoCTF**, organised by **Carnegie Mellon University** **2019**
- Served as a volunteer under **NSS, IIT Bombay**, devoting 80+ hours to community service **2018-19**