Yatharth Goswami

✉ ygoswami@iitk.ac.in | yatharth0610.github.io | github.com/yatharth0610 | +91-9982144450

Academic Details

Examination	Department / Board	Institute	Year	CPI/%
Graduation	Computer Science and Engineering	IIT Kanpur	2023	9.8/10.0
Intermediate/+2	Maharashtra Board (HSC)	Alpha Junior College of Science	2019	90.31
Metriculation	Board of Sec. Education, Rajasthan	SMJT Senior Sec. School, Bikaner	2017	93.67

Scholastic Achievements

- Secured **All India Rank 110** in **JEE Advanced 2019** among 2.3 Lakh eligible aspirants *(2019)*
- Secured **All India Rank 448** in **JEE Mains 2019** among 11,57,125 candidates *(2019)*
- **Academic Excellence Award** for exceptional performance in Academics at IIT Kanpur *(2019-21)*
- Recipient of prestigious **Director's Scholarship**, awarded to 6 students at IIT Kanpur. *(2020)*
- Secured perfect **10.0/10.0** grade points in **1st, 4th, 5th** and **6th** semester at IIT Kanpur. *(2022)*
- Awarded **A*** grade in **PG Level** course of Modern Cryptology under **Prof. Manindra Agarwal.** *(2021)*
- Awarded **A*** grade in **PG Level** course of **Intro to Machine Learning.** Awarded to only **1** student in a class of **204** students which included UGs, Masters and PhD students from IITK. *(2021)*

Olympiads and Other Achievements

- **Gold Medalist** in the Saptang Lab Security Hackathon in **9th Inter IIT Tech Meet**. *(2021)*
- Recipient of prestigious **KVPY fellowship** by Dept. of Science and Technology, Govt. of India *(2018,2019)*
- Received **Gold Medal** and **Certificate of Merit** for being in the national top 42 candidates at INChO *(2019)*
- Attended the **OCSC** Camp for **International Chemistry Olympiad**. *(2019)*
- Amongst the top students across the nation in **NSEA** selected to appear for **INAO**. *(2019)*
- Awarded the certificate of merit for being in the national top 1% in **NSEJS** (Junior Science Olympiad). *(2017)*
- Global rank **1001** out of **9004** global participants in Google HashCode 2021. *2021*

Internships and Research Projects

Privacy Preserving Heavy Hitters

[May2021-July2021]

Research Intern | Summer@EPFL'21 | Prof. Jean Pierre Hubaux — *LDS Lab, EPFL*

- Worked on **Securely** tackling **Heavy hitter problem** for Origin-Destination flows using modern Crypto Primitives like **Fully Homomorphic Encryption**.
- Studied **SOTA** comparison and sorting algorithms for **BFV/BGV** and **CKKS** schemes.
- Benchmarked the SOTA implementations for performing comparison operations using **Fully Homomorphic Enryption** and **MPC** schemes.
- Learned about data-structures for compactly representing **large datasets** like **Count-min sketches** and **Bloom Filters**.
- Used Geospatial libraries like **GeoPandas** and **Uber's h3** to build a pipeline for converting any custom **shape file** to **Origin-Destination matrix.**
- Used libraries like **Bokeh** for visualisation and **Dask** for performing large **Distributed Operations**.
- Designed an initial prototype of the solution using **BFV** scheme.

Malware Needs "Attention" too!

[Jan2021-Apr2021]

Research Project | Prof. Sandeep Shukla — *C3i Centre, IIT Kanpur*

- Used **API fragments** and **NLP models** for **classifying malicious** and **benign** files.
- Use the analogy of **language vocabularies** to generate API call embeddings using Word2Vec model which made sense sematically.
- Combining normal **LSTMs with attention** layers to get the **global correlations**
- Built technique stable to measures like **obfuscation** and outperforms other works using similar approach.

Decentralised Mechanism Design using Blockchains *Code Here*

[Oct2020-Nov2020]

Course Project CS711 | Guide: Prof Swaprava Nath — *IIT Kanpur*

- Implemented various **Sealed-Bid Auction Mechanisms** using Blockchains.
- 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.**

Memory Overhead Analysis of container based android devices *[Jan2022-Apr2022]*

Undergraduate Researcher | Guide: Prof Debadatta Mishra *IIT Kanpur*

- Ported a recent android sandboxing solution **VPBox** for Android phones to **emulator** systems. **Presentation**
- Manually adapted the vanilla **aosp** and **goldfish kernel** for emulators to include changes in original paper.
- Implemented a BFS inside kernel which on being given a start pid, walks over **VM** areas of all the processes in the subtree of the given process.
- Used the **pseudo sysfs filesystem** in linux kernel to get the above information for **init** processes of all the **virtual phones** as well as host by setting up **callbacks** for the same inside kernel.
- Reported potential **ineffectiveness** in sharing of some physical pages using memory data captured with reason.

Key Projects

GIPSC: Golang to MIPS Compiler *Code Here* *[Jan2022-Apr2022]*

Course Project CS335 (Compiler Design) | Guide: Prof. Amey Karkare, Prof. Subhajit Roy

- Implemented a **compiler** for a fully functional subset of the **Go** language, using **Python**.
- Designed a **lexer**, **parser** and **semantic analyzer** that supports Go features including **Short Variable Declaration, Multilevel Pointers, Struct, Array, Floats** and **Labelled Statements**.
- Generated **3AC Opcodes** for ease of conversion to MIPS assembly in Code Generation phase.
- Implemented some **advanced** features like **Constant folding, Syscall wrappers, Custom File Importing, Multiple Returns** and **Multiple Assignments**.
- Awarded with the **best score** for the project among all groups in the course.

Parallel Programming *Code Here* *[Jan2022-Apr2022]*

Course Project CS433 (Parallel Programming) | Guide: Prof. Mainak Choudhary

- Implemented and Optimized **Parallel Algorithms** taking into account underlying **cache effects** for solving **Travelling Salesman Problem** and **Lower Triangle Solver** using **OpenMP** APIs.
- Implemented and compared various software locks like **Lamport's Bakery, Spin-lock, Test-and-test-and-set, Ticket** and **Array Lock** with no **false sharing** using instructions like **cmpxchg**.
- Implemented and compared various barriers like **Sense-reversing** and **Tree barrier** both using **busy wait** and **POSIX Conditional Variables**.
- Implemented **GPU Algorithms** for **Gauss Siedel Solver** and **Matrix Vector Product** further optimised using **tree reduction** and **shared memory** on **NVIDIA GPUs**.
- Received **perfect score** and **great remarks** for all the reports submitted.

Building GemOS *[Aug2021-Nov2021]*

Course Project CS330 (Operating Systems) | Guide: Prof. Debadatta Mishra

- Created **file archiving utility** and enabled **IPC** using C system calls like **pipe(), fork()** and **exec()**
- Implemented **system calls** for **pipe** and **persistent pipe** structures sharing data between multiple processes
- Developed a basic **debugger** using **INT3** for functions featuring **stack backtrace** of function addresses
- Improvised **clone()** system call to develop a library of **threading APIs** with **private memory areas**

Attacking Cryptosystems *Code Here* *[Fall 2021]*

Course Project CS641 | Guide: Prof. Manindra Agarwal *IIT Kanpur*

- Broke various cryptosystems like **DES**, **AES** and **RSA** as part of a game during the course.

Clustering multidimensional data *Code Here* *[Aug2021 - Nov2021]*

Course Project MTH511 | Guide: Prof. Dootika Vats *IIT Kanpur*

- Implemented the EM-algorithm **Guasssian mixture model** for **multidimensional data** using R language.
- Cross Validated the result using **BIC criteria** and tuned the hyperparameters accordingly.

IITK Bucks *Code Here* *[Summer 2020]*

Programming Club, IITK *IIT Kanpur*

- Implemented a **Fully Functional** Node of blockchain using NodeJS.
- Learned about the basics of the functioning of **Blockchains**, **Crypto-Currencies** and **Private-Key Cryptography**.
- Learned about Programming Concepts specific to **JavaScript** like **Async Functions** and **Event Loops**.
- Learned about **Tunneling Softwares** like **ngrok** and used them to test the nodes.
- Implemented the **Miner** using the concepts of **Multithreading** in NodeJS.

HCL-C3i Hub Cybersecurity Hackathon *Code Here* *[Jul2020-Aug2020]*

Online Project (Hackathon) | C3i Hub, IITK

- Ranked **25th** out of around **3400** teams from all around the world and built a **Deep Learning** based solution to distinguish Malicious executables.

Quantum Computing with Qiskit *Code Here* *[Summer 2020]*

Online Project (Workshop)

- Learned the basics of **Quantum Computation** and **Quantum Physics**.
- Implemented various algorithms such as **Teleportation, Deutsch Josza Algorithm, Grover's Algorithm, IBM's BB84 Protocol** and **Quantum Fourier Transform** with IBM's **Qiskit**.

Private Computation Using Cryptographic Primitives *Code Here* *[Summer 2020]*
Programming Club, IITK *IIT Kanpur*

- Implemented **Distributed Point Function (DPF) library** using the principles of **Function Secret Sharing (FSS)** in Rust.
- Learned about various Cryptographic Primitives used for **Private Computation** like **Function Secret Sharing**, **Fully Homomorphic Encryption**, **Yao's Garbled Circuits** and **Shamir's Secret Sharing**.
- Used various libraries like **gtest, grpc, google/benchmark** for making tests and benchmarking final code.

Technical Skills

- **Programming & Scripting Languages:** C++, C, Python, R, JavaScript, Rust(Familiar), Bash, GoLang(Familiar)
- **Libraries/Technologies:** Pandas, NumPy, matplotlib, GeoPandas, Shapely(Familiar), Dask(Familiar), Bokeh, h3(Familiar), LaTeX , Cutter, IDA, Git, LibreCAD, Tensorflow, Gambit, gcov, gtest, Markdown
- **Development:** HTML, CSS, Bootstrap, JavaScript, NodeJS(Proficient), Django(Familiar), MongoDB(Familiar)

Key Courses Undertaken

A* Intro to Machine Learning
A Operating Systems
A Computer Networks
A Advanced Algorithms
A Software Development and Operations
A Logic for Computer Science
A : *Grade*

A* Modern Cryptology
A Statistical Simulation & Data Analysis
A Theory of Computation
A Game Theory and Mechanism Design
A Probability in Computer Science
A Microeconomics
A* : *Grade for Exceptional Performance*

A Compiler Design
A Parallel Programming
A* Real Analysis
A Computer Organisation
A Abstract Algebra
A Linear Algebra

Positions

Secretary, Programming Club *[May2020-Apr2021]*
Programming Club, IITK *IIT Kanpur*

- Wrote a blog on Reverse Engineering for making campus aware of techniques prevalent in the CTFs
- Helped in conduction of **Deep Learning Hackathons** on various domains and helping students by providing related materials.
- Responsible for managing Competitive Programming Competition for students of the institute for a month.
- Responsible for managing Competitive Programming Competitions and writitng blogs.

Mentor - Numbers Made Dumber *[Apr2021-June2021]*
Stamatics, IITK *IIT Kanpur*

- Mentored 33 freshman students, covered Number theoretic theorems and basics of cryptography.

Mentor - Blocks and Chains *[Apr2021-Ongoing]*
Association for Computing Activities, IITK *IIT Kanpur*

- Mentoring 19 freshman and sophomore students, covered basics of how blockchains work through blogs and assignments.