

Aarav Varshney

+91-7289988234 | aarav.varshney22@gmail.com | [linkedin.com/in/aarav22](https://www.linkedin.com/in/aarav22) | github.com/aarav22 | www.aaravvarshney.in

EDUCATION

Ashoka University

Sonepat, India

Postgraduate Diploma in Advanced Studies and Research

Sept. 2022 – May 2023

- Graduated Cum Laude with a thesis titled “Anonymous Proof of Account Ownership” under Mahavir Jhawar.
- Advanced Major in CS; Relevant coursework includes Information and Coding Theory, Reading, Reviewing, and Presenting Scientific Papers, Rapid Prototyping and Experimentation, and Machine Learning for Finance.

Ashoka University

Sonepat, India

Bachelor of Science in Computer Science, Minor in Mathematics

Aug. 2019 – May 2022

- Graduated Cum Laude with Major GPA of 3.73/4.0.
- Relevant coursework includes Computer Security and Privacy, Blockchain and Cryptocurrencies, Theory of Computation, Advanced Programming, and Abstract Algebra.

WORK EXPERIENCE

Teaching Fellow & Teaching Assistant

May. 2023 – Present

Ashoka University

Sonepat, India

- TF for CS-2361 (Blockchain and Cryptocurrencies), TA for CS-1340 (Computer Networks), CS-2362 (Computer Security and Privacy), and CS-2375 (Database Management Systems).
- Conducted weekly office hours, tutorials, evaluated assignment and supervised course-projects.

Software Engineer

June 2022 – Aug. 2022

Amuse Labs

Bengaluru, India

- Implemented a POC for voice-controlled digital puzzles using Alexa SDK to increase distribution channels.
- Wrote a Typescript library to develop Alexa-controlled puzzles on any front-end.
- Built a nginx reverse-tunneling server and dockerized applications to set up future development.

Backend Developer

Mar. 2022 – June 2022

SALT (Funded by YC'W22)

Bengaluru, India

- Redesigned the Doc-to-Pdf conversion techniques to decrease overall document registration time by 30-40 % in Node.js; worked on creating microservices for document templating engine to allow autofills.
- Automated deployment pipeline with GitHub workflows and AWS.

Founder & Head of Development

Sept. 2020 – Aug. 2022

Beyond Design Studio

Chennai, India

- Led team of 20-30 members to execute industry projects accumulating net profits of over Rs. 3L+; worked with various tools and frameworks — Next.js, TailwindCSS, Node.js, Express.js, and GCP across multiple projects.
- Formed partnerships with DaurCom, InIFarms, Quintessentially and Niti Aayog for development projects and tech maintenance.

RESEARCH EXPERIENCE

Research Assistant

Nov. 2022 – Present

Defense Research & Development Organisation (DRDO)

Delhi, India

- Led the project to develop a python-based software for post-quantum key management using PQC primitives — Dilithium and Kyber. We are currently working on integrating the software with DRDO's existing systems.
- Implemented custom-built post-quantum X.509 certificates that do not rely on third-party libraries yet maintain verifiability through OQS's OpenSSL.

Research Assistant

Aug. 2020 – Sep. 2020

Chegu Ruthwik

Remote

- Submitted a report to identify the best customer segment and necessary strategies for developing a pilot model of a sustainable and cost-effective oral hygiene product.
- Analyzed market surveys to study consumer preferences on oral hygiene habits.

PUBLICATIONS

[1] YouChoose: A Lightweight Anonymous Proof of Email Account Ownership

Aarav Varshney, Prashant Agrawal, and Mahabir Prasad Jhanwar

under submission

- We propose and implement a concrete YouChoose protocol for SMTP-TLS and discuss the implementation aspects for anonymously proving email account ownership using SMTP over the TLS secure channel.
- We also look into using a zk-SNARK based approach to extend anonymous PAO paradigm to shared email servers.

[2] Transitioning to a Post-Quantum Key Management Framework

Mahabir Prasad Jhanwar, Aarav Varshney and Adit Dhawan

in progress

- We propose and implement a post-quantum key management solution to safeguard the existing communication infrastructure against quantum adversaries.

OTHER ACTIVITIES

Head of Technology

Dec. 2019 – May 2022

Ashoka Business Review

Ashoka University, India

- Supervised and maintained tech development at ABR; directed 2 interviews with experts for a blockchain podcast series.

Teacher

Dec. 2021 – Jan. 2022

South Asian Winter Camp

Remote

- Designed and taught a CS curriculum to a class of 30+ high school students inculcating programming, ethics and career options.

PROJECTS

Trading App | *Typescript, Socket.js, Node.js, Next.js, PostgreSQL, GCP*

April. 2022 – Aug. 2022

- Designed backend to handle 200+ users on a live stock-trading app with price and news updates synchronized every minute.
- Timed events with cron scheduler and used sockets to push updates to user devices. Deployed on GCP's App engine and Cloud SQL.

Jaan Pehchan | *Javascript, Node.js, ReactNative, Neo4j, Heroku*

Jan. 2022 – May 2022

- Engineered fullstack to build a social networking app for small businesses (MSMEs); The app garnered 500+ downloads on Google Play Store.
- Visualized & established relationship with 60K+ nodes using Neo4j database.

The New Geography | *Kotlin, Java, Android Studio*

July 2020 – Aug. 2020

- Built an android app to educate users about various restrictions put on internet.
- Reverse-engineered censoring on Google Maps by translating China's GCJ-02 geodetic datum to WGS-84.

ACHIEVEMENTS

- **Nomination for Microsoft Research Fellowship** CS Dept., Ashoka University
- **Dean's List** Dean of Academic Affairs, Ashoka University
- **Top 20% in DevCTF: Capture the Flag** IIT Delhi

REFERENCES

Mahvir Jhawar

CS Dept., Ashoka University

mahvir.jhawar@ashoka.edu.in

- Capstone project/thesis advisor and supervisor for multiple projects.

Debayan Gupta

CS Dept., Ashoka University

debayan.gupta@ashoka.edu.in

- Course instructor and advisor for multiples Independent Study Modules (ISMs).

Deva Madala

Amuse Labs

deva@amuselabs.com

- Project supervisor at Amuse Labs.