

Aarav Varshney

+91-7289988134 | 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 in “Anonymous Credentials” under Prof. Mahavir Jhavar.
- 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; relevant coursework includes Computer Security and Privacy, Blockchain and Cryptocurrencies, Theory of Computation, Advanced Programming, and Abstract Algebra.

RESEARCH EXPERIENCE

Research Assistant

Nov. 2022 – Present

Ashoka University & Defense Research and Development Organization (DRDO)

Sonepat, India

- Leading the development of a post-quantum key management software built on top of PQC primitives (Dilithium and Kyber), with a focus on seamless integration into DRDO's existing systems.
- Implemented custom post-quantum X.509 certificates without relying on third-party libraries, ensuring verifiability through OQS's OpenSSL.

Research Assistant Intern

Aug. 2020 – Sep. 2020

Chegu Ruthwik

Remote

- Compiled a comprehensive report identifying the optimal customer segment and outlining essential strategies for developing a pilot model of a cost-effective oral hygiene product.
- Conducted in-depth analysis of market surveys to assess consumer preferences related to oral hygiene habits.

WORK EXPERIENCE

Teaching Fellow & Teaching Assistant

Aug. 2021 – Dec. 2023

Ashoka University

Sonepat, India

- Instructed and assisted in courses including CS-2361 (Blockchain and Cryptocurrencies), CS-1340 (Computer Networks), CS-2362 (Computer Security and Privacy), and CS-2375 (Database Management Systems).
- Facilitated student learning through weekly office hours, tutorials on Hyperledger Fabric, TLS, SQL, and assessed assignments and course projects.

Software Engineer Intern

June 2022 – Aug. 2022

Amuse Labs

Bengaluru, India

- Developed an Alexa app for playing Amuse Labs puzzles like quizzes and crosswords via voice commands, enhancing user accessibility and creating new revenue opportunities, notably with The Washington Post.
- Overcame technical challenges in voice command design and API development with Amuse's backend. Also crafted a TypeScript library, enabling websites to offer Alexa-integrated quizzes.

Backend Developer Intern

Mar. 2022 – June 2022

SALT (Funded by YC'W22)

Bengaluru, India

- Contributed to the development of a document templating service, enabling users to generate customized PDFs through form inputs for various use-cases. Achieved a 30-40% reduction in document generation time by optimizing backend processes and reviewing different templating implementations.

Co-Founder & Head of Development

Sept. 2020 – Aug. 2022

Beyond Design Studio

Chennai, India

- Led team of 20-30 members, successfully delivering industry projects and generating net profits exceeding Rs. 3L+. Employed a diverse range of tools and frameworks, including Next.js, TailwindCSS, Node.js, Express.js, and GCP, across various projects.
- Cultivated partnerships with esteemed organizations, such as DaurCom, InIFarms, Quintessentially, and Niti Aayog, for collaborative development projects and ongoing tech maintenance initiatives.

PUBLICATIONS

[PUB01] YouChoose: A Lightweight Anonymous Proof of Account Ownership

Aarav Varshney, Prashant Agrawal, and Mahabir Prasad Jhanwar

IACR ePrint

- We proposed and implemented a concrete YouChoose protocol for anonymously proving account ownership for SMTP and HTTP based protocols over the TLS secure channel.
- We also look into using a zk-SNARK based approach to extend anonymous PAO paradigm to develop anonymous SSO without requiring any changes at the server.

[REPORT01] Transitioning to a Post-Quantum Key Management Framework

Mahabir Prasad Jhanwar, Aarav Varshney and Adit Dhawan

available on request

- We propose and implement a post-quantum key management solution to safeguard the existing communication infrastructure against quantum adversaries. The report details the implementation of X.509 PQC certificates without relying on third-party libraries.

PROJECTS

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

April. 2022 – Aug. 2022

- Designed backend capable of handling 200+ users on a live stock-trading app, ensuring updates every minute.
- Synchronized using a cron scheduler to push updates to users. Hosted on GCP's App Engine using Cloud SQL.

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

Jan. 2022 – May 2022

- Engineered a full-stack solution for a social networking app catering to small businesses (MSMEs). The app achieved 500+ downloads on the Google Play Store.
- Managed 60K+ nodes and their connections using the Neo4j database.

MindBlock | JS (React Native) Development

April 2021 - May 2021

- Developed an intuitive educational app on Bitcoin, employing analogies (produced YouTube videos) and interactive tools (using BlockCypher APIs) for effective learning.
- Structured the app into 7 modules, each focusing on key aspects of Bitcoin, promoting a sequential learning experience for users.

OTHER ACTIVITIES

Head of Technology

Dec. 2019 – May 2022

Ashoka Business Review

Ashoka University, India

- Supervised and maintained tech development at Ashoka Business Review. Directed two expert interviews for a blockchain podcast series.

Teacher

Dec. 2021 – Jan. 2022

South Asian Winter Camp

Remote

- Designed and taught a comprehensive computer science curriculum to a class of 30+ high school students. The curriculum included programming, ethics, and discussions on career options. [View Poster](#)

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

Associate Professor, CS Department, Ashoka University

mahvir.jhawar@ashoka.edu.in

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

Debayan Gupta

Assistant Professor, CS Department, Ashoka University

debayan.gupta@ashoka.edu.in

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

Deva Madala

Technical Lead, Amuse Labs

deva@amuselabs.com

- Project supervisor at Amuse Labs.