

Education

Bachelor of Technology

Undergraduate degree program

Major: Information Technology

Final grade: 7.8 CGPA

J.C Bose University Of Science And Technology

September 2020 – Present

Class 12th(CBSE Board)

higher school program

Major: Non-Medical Studies

Final grade: 89.2%

Senior Shri Ram Model School

March 2019 – March 2020

Experience

Independent Researcher/Auditor

Participating in audit contests held by Immunefi and Code4rena

September 2022 – Present

Remote

- Found several bugs of varying severity on Immunefi, which you can see [here](#).
- Participated in c4 contests twice and found 3 high, some low, and some gas findings.
- Completed challenging CTFs like Damn Vulnerable DeFi and Ethernaut, which have helped me improve my skills. Solutions for Damn Vulnerable DeFi can be found [here](#).
- Created a repo containing common defi vulnerabilities which can be found [here](#).

Yacademy

Fellow

10th April 2023 – 12th May 2023

Remote

- Conducted smart contract audits on EVM-based blockchains twice.
- Found four bugs of varying severity(1 unique medium).
- Learned a lot from the challenges, guest speakers, delving into codebases, and tackling a big project.

Full-stack Blockchain Solutions

Contract basis developer

October 2021 – July 2022

Remote

- Led the development work of decentralized apps.
- Worked on various protocols including StabilityDAO.
- My work included front-end development using technologies such as TypeScript, Nextjs, Reduxjs, TailwindCSS, and Etherjs, as well as back-end development with Solidity, Hardhat, and Foundry.

Full-stack Blockchain Developer

EthOnline 2022 hacker

September 2022

Remote

- Created REI(Real Estate Investment) based on the idea of NFT. fractionalization and trading real estate NFTs.
- During this, Worked on Front-end, Subgraph, and Smart contracts.
- Tech stack includes Next.js, Solidity, IPFS, TheGraph, Ethers, and Wagmi.

Writings

Denial-of-Service(DoS) Attacks

Attack vectors

2023

[here](#)

This article focuses on how denial-of-service (DoS) attacks can potentially damage a protocol, with a specific target audience of beginner to experienced smart contract security researchers. The article discusses seven common DoS attacks that researchers should pay close attention to during audits.

PROJECTS

ERC20-In-Yul

2023

ERC20 Contract

[here](#)

Created an ERC20 contract using Inline Yul, expanding my expertise in storage and memory management within the EVM. Acquired in-depth knowledge of various opcodes, memory management techniques, and gas efficiency during the project development.

UniswapV2

2022

Decentralized Exchange

[here](#)

Developed a clone of Uniswap v2, a decentralized exchange protocol, gaining expertise in gas-saving techniques, Uniswap v2 architecture, and the constant product formula.

lendnow

2023

A lending and borrowing protocol

[here](#)

Developed a lending and borrowing protocol inspired by Aave and Compound, expanding my expertise in key concepts including health factor, liquidation, interest rates, and their practical application within the project.

zkSortedArray

2023

ZK Circuit in Circom

[here](#)

Developed a circuit utilizing Circom and Snarkjs to verify the sorting of an array, furthering my understanding of snarks. Explored the Pinocchio protocol and gained familiarity with key concepts, including homogeneous encryption, constraints, and more.

RSA

2023

RSA algorithm in Rust

[here](#)

Developed a RUST CLI tool for generating private and public keys, encrypting, and decrypting messages. Gained knowledge in number theory, key generation, and the encryption/decryption process during the project.

REI

2022

Real estate Investment

[here](#)

REI enables fractionalized real estate NFT trading. The tech stack includes TheGraph, IPFS, Ethers, Wagmi, Next.js, Hardhat, and Solidity. Gained extensive knowledge in creating subgraphs, frontend development, smart contract implementation, and their seamless integration while working on the project.

NFT-Marketplace

2022

NFT Marketplace

[here](#)

Designed and developed an NFT marketplace facilitating the trading of NFTs with ERC2981 royalties. Acquired in-depth understanding of ERC2981 and ERC721 standards, along with proficiency in implementing patterns such as CEI (Check Effect Interaction) throughout the project.

Skills

Programming Languages	C/C++, Javascript/Typescript, Python, Solidity, Rust
Markup Languages	HTML, CSS
Development Environment	Foundry, Hardhat, Truffle
Popular Libraries	React.js, Express.js, Mongoose.js, Numpy, Pandas
Data Query Languages	SQL
Runtime Environments	Node.js
Miscellaneous	Linux, Git

Soft skills

Documentation and Presentation	Skilled at creating documents and delivering presentations
Teamwork	Very good at working in teams and discussing things.
Problem-solving	Proficient in problem-solving.