+91 6360029877 Bengaluru, Karnataka, India sohan.mallikarjun@gmail.com

Sohan Hanabe Mallikarjun

COMPUTER SCIENCE ENGINEERING STUDENT

LinkedIn **GitHub** English, Kannada, Hindi

Professional Statement

Computer Science student with a strong foundation in cybersecurity, specializing in AI Security. Hands-on experience securing AI and web applications through real-world projects and internships. Naturally curious and driven to build secure systems that make a meaningful impact.

Education

2022 - 2026
JSS Academy of Technical Education
BE Computer Science and Engineering
(CGPA – 8.43)

2020 - 2022
Deeksha CFL PU College
Intermediate (PCMB)
(12th Percentage - 86%)

2018 – 2020
SJR Kengeri Public School
Secondary Education (9th-10th)
(10th Percentage – 95.6%)

Experience

SecurEyes | Onsite
Nov 2024 – Mar 2025
Bengaluru, Karnataka, India

AI Security & Application Security Intern

- **Identified vulnerabilities** in AI and traditional applications.
- Explored **security frameworks** tailored to AI systems.
- Implemented **proof-of-concept defenses** on local AI models.
- Studied real-world exploits to **document attack/defense strategies**.

Skills

Programming	C, JavaScript, HTML5, CSS, Bootstrap (Framework), Java, Python
Personal	Communication, Leadership, Teamwork, Problem-Solving, Critical Thinking
Operating Systems	Windows, Linux (Ubuntu, Kali)
Security Practices	Risk Management, Security Auditing, Network Security, Network Architecture, Cloud Computing

+91 6360029877 Bengaluru, Karnataka, India sohan.mallikarjun@gmail.com

Projects

Adversarial Backdoor Injection in LLMs: PoisonGPT Case Study
(PoC) | SecurEyes

- Demonstrated ethical backdoor injection in a fine-tuned Mistral-7B model via data poisoning and gradient manipulation.
- Simulated real-world AI threats aligned with MITRE ATLAS. Tested defenses in a constrained local setup.
- *Tools: Unsloth, PyTorch, LoRA, Gradient Hooks, CUDA, WSL, Quantized Models*

ML-Based DGA Detection Evasion
(PoC) | SecurEyes

- Executed black-box evasion attacks on an ML-based DGA detection model, reducing its accuracy from 82.9% to 0.06%.
- Designed test cases mapped to MITRE ATLAS (AML.T0043.001) to demonstrate real-world AI evasion risks.
- *Tools: Python, Postman, Kali Linux, ChatGPT, MITRE ATLAS*

Portfolio Website

- Developed and maintain a personal website to showcase projects, certifications, resume, and GitHub activity.
- Built using responsive web design principles for accessibility across devices.
- *Tools Used: HTML, CSS, Bootstrap, VS Code, GitHub Pages*

Certifications

Google

Foundations of Cybersecurity

Play It Safe: Manage Security Risks

Connect and Protect: Networks and Network Security

MongoDB

MongoDB for SQL Experts

Extracurriculars

Class Representative
2022 - Present

Elected as the class representative for the full course of Engineering. Bridging the gap between students & faculty and discharging my duties with ease.

Sponsorship Head
Anveshan 2025

Raised ₹92,000 in sponsorships and led a cross-year team. Co-managed the fest's planning, logistics, and execution. Anchored the event, representing the CSE department on stage.

NSS Core Volunteer
2023 - Present

Led cleanliness and waste management drives. Organized awareness walkathons on dementia, cancer, and animal welfare.

Rotary Interact Club President
2018 - 2019

Organized awareness and charity events. Raised ₹6,000 through eco-friendly bag sales, donated to an old age home in Kengeri.

Interests

AI Security Research | Reading Cybersecurity and Technology Books | Football Enthusiast | Exploring New Cultures Through Travel