

# SHASHANK BAGDA

## Research Engineer - AI Systems & Hardware Security | HW-SW Co-Design

Email: [work.shashankbagda@gmail.com](mailto:work.shashankbagda@gmail.com)

Mobile: +65 9039 3206

GitHub: <https://github.com/ShashankBagda>

Portfolio: <https://shashankbagda.github.io/>

Linkedin: <https://www.linkedin.com/in/shashank-bagda/>

---

### SUMMARY

Master's student in **Software Engineering** with hands-on research experience in secure and high-performance **AI systems**, adversarial threat modeling, and hardware-software co-design. Proficient in **C++**, **Python** and **Java**, with experience building and benchmarking system-level optimizations using PyTorch/TensorFlow, SIAM and GEM5. Focused on designing scalable, trustworthy and performance efficient AI systems at the intersection of ML infrastructure and computer architecture.

---

### EDUCATION

#### NATIONAL UNIVERSITY OF SINGAPORE | ISS

Aug 2025 -  
Sep 2026

Master of Technology - [Software Engineering](#)

- Coursework: Software Architecture & Design, Cloud-Native & Platform Engineering, DevSecOps, Secure SDLC, Agile Methodologies

#### MARWADI UNIVERSITY

Sep 2021 -  
May 2025

Bachelor of Technology - [Information and Communication Technology](#)

- Honors: First Class with Distinction
- 

### PROJECTS

1. **Hardware Security & Systems Research (IIT Guwahati)**
    - Conducted system-level research on secure and performance-efficient multicore architectures, including NoC security analysis, adversarial threat modeling, and simulation-driven benchmarking.
  2. **Handwriting to G Code**
    - Designed an AI-driven pipeline converting handwritten input into machine-readable control instructions, focusing on robustness, preprocessing accuracy, and system reliability.
  3. **Telecom Architecture**
    - Designed and documented a scalable telecom system architecture, analyzing performance, reliability, and fault-tolerance trade-offs using graph-based modeling.
- 

### RESEARCH EXPERIENCE

#### INDIAN INSTITUTE OF TECHNOLOGY - GUWAHATI

Research Intern

May 2024 - Aug 2024

- Designed and evaluated **homogeneous and heterogeneous AI system architectures** using the **SIAM simulator**, enabling scalable training and inference across 12+ distinct AI workload configurations.
- Reduced end-to-end processing latency by 22–28% through **parallel execution** and **in-memory computing** techniques on multicore platforms.
- Engineered **hybrid network structures** that improved inference responsiveness and sustained throughput under production-scale deep learning workloads.
- Conducted system-level performance benchmarking across 8000+ simulation runs, analyzing latency, throughput, and resource utilization trade-offs.
- Developed high-performance experimental pipelines in **C++** and **Python**, automating configuration sweeps and reducing research iteration time by ~35%.

- Designed and implemented **Hardware Trojan Detection** mechanisms for **multicore Network-on-Chip (NoC) systems**, improving system trustworthiness under adversarial conditions.
- Performed **threat modeling** and attack-defense evaluation to quantify security performance trade-offs in cyber-physical and on-chip communication systems.
- Evaluated NoC security and performance using the **GEM5 simulator (Garnet Standalone)** across 3500+ simulation scenarios, identifying critical attack vectors and communication bottlenecks.
- Improved on-chip communication efficiency by implementing dynamic routing algorithms in **C++** and **Python**, reducing average packet latency by 17–21%.
- Delivered measurable gains in system resilience (~30%) and hardware efficiency (~18%) through detailed simulation-driven performance analysis.

---

## SKILLS

### Programming & Systems

- Languages: C++, Python, Java
- Parallel & Performance Computing: Multicore processing, system profiling, performance optimization

### Machine Learning & AI

- Frameworks: PyTorch, TensorFlow
- Core Concepts: Deep Learning, Neural Networks, Model Optimization, Performance Benchmarking
- AI Safety & Security (Foundational): Adversarial ML concepts, Threat Modeling, Robustness Evaluation

### Systems & Hardware

- Computer Architecture, Digital Systems
- Embedded & IoT Systems: Arduino, Raspberry Pi, ESP8266/ESP32, Zigbee
- Circuit Design & Simulation: PCB Design, Circuit Simulation, Logic Design

### Software & Platforms

- Backend & APIs: REST APIs, Java (JSP/Servlets), MySQL
- Web (supporting): ReactJS, HTML, CSS, JavaScript

---

## INTELLECTUAL PROPERTIES

### Patent

- Method for Converting Handwritten Characters into Machine-Readable Instructions (202421033236)

### Copyright

- Telecom Architecture (8416/2023-CO/SW)

---

## AWARDS, HONOURS & ACHIEVEMENTS

- Student Startup and Innovation Policy (SSIP) Hackathon 2022 - Second Highest Honour (Government of Gujarat, India)
- Club Founder Award 2024 - Circuitology Club, Marwadi University

---

## LEADERSHIP & STEM ACTIVITIES

- Chair - IEEE MEFGI Student Branch (2024): Led student operations, coordinated technical events, and collaborated with industry professionals.
- Founder - Circuitology Club (2021): Built a 110+ member technical community, secured USD 3,500+ in funding, and organized 30+ workshops and STEM outreach sessions.