Muhammad Hassnain

Davis, California, 95616
(530) 760 9401 mhassnain@ucdavis.edu linkedin.com/muhammad-hassnain muhammad-hassnain

Education

University of California, Davis **Expected: June 2028**
PhD. in Computer Science *Davis, California*
Relevant Coursework: Computer and Information Security, Software Engineering, Design and Analysis of Algorithms, Computer Networks, Programming Languages and Compilers, Computer Networks

Lahore University of Management and Sciences **Sep. 2019 - May 2023**
Bachelor of Science in Computer Science *Lahore, Pakistan*
Relevant Coursework: Data Structures, Discrete Math, Algorithms, Operating System, Network Security, Software Engineering, Data Science, Advanced Programming, Human-Computer Interaction, Machine Learning, Speech Processing

Publications

Counterexamples in Safe Rust *ASEW'24*
Muhammad Hassnain, Caleb Stanford

Cargo-Sherlock: A formal checker for supply chain trust *PLDI'25 (under review)*
Muhammad Hassnain, Anirudh Basu, Caleb Stanford

Assessing Local LLMs for Developer Support in Software Engineering *MSR'25 (under review)*
ZeeraK Babar, Nafiz Imitiaz Khan, Muhammad Hassnain, Vladimir Filkov

Research Experience

Graduate Student Researcher | Rust, Python, Bash **Sep. 2023 – Present**
PL Davis, UC Davis *Davis, California*

- **Static Analysis Tool Development**: Developed *LHS*, an open-source Rust MIR analysis tool designed to detect memory safety issues and potential attack vectors within safe Rust code. This tool enhances the security of Rust applications by identifying vulnerabilities that may not be apparent through conventional methods. (WIP)
- **Supply Chain Trust Modeling**: Developed *Cargo-Sherlock*, an open-source automated reasoning tool that models and assesses trust within the Rust supply chain ecosystem. This project integrates programming language research with security analysis to fortify the integrity of Rust's package management system.
- **Counterexamples in Safe Rust**: Developed a project that examines the limitations and potential vulnerabilities within Rust's memory safety model. This research highlights scenarios where safe Rust may still be susceptible to memory safety issues, challenging common assumptions about Rust's security guarantees. Findings have been shared through multiple academic platforms and conferences.

Undergraduate Research Assistant | *Bash, Python, Docker, Linux, TypeScript, React, Rust* **May 2022 – August 2023**
Internet Security and Privacy Lab, LUMS *Lahore, Pakistan*

- **Privacy-Enhancing Web Refactoring** (Collaboration with UC Davis, Virginia Tech, and LUMS): Applied program analysis techniques to detect bundled code locations on webpages, achieving real-time detection with 98% accuracy. Refactored detected code to preserve only essential functions, significantly reducing tracking actions while retaining functionality.
- **Ads Accessibility Study** (Collaboration with University of Washington and LUMS): Initiated and led a study on web accessibility for visually impaired users. Developed a TypeScript and Puppeteer-based ad scraper to analyze ad accessibility across top-ranked and bottom-ranked websites on the Tranco list. Used automation and data analysis to identify variations across site ranks, highlighting ad platform providers and accessible ad characteristics.
- **Git Secrets Detection** (Collaboration with Meta and LUMS): Automated the cloning and scanning of the top 1,000 frequently updated GitHub repositories to detect secret leakages, such as encryption keys, API tokens, and account credentials. Implemented machine learning models to proactively identify sensitive information in new repositories.
- **NPM Hidden Dependencies Investigation** (Collaboration with NC State and LUMS): Analyzed undisclosed dependencies in NPM packages that were neither documented nor visible in dependency trees. Tracked the evolution of these hidden dependencies to understand their impact and progression over time.

Undergraduate Research Assistant | *Figma, Angular, Node, Mongoose* **May 2022 – May 2023**
Technology for People Initiative Lab, LUMS *Lahore, Pakistan*

- Oversaw and enhanced the **Digital Archives of Pakistan** website; navigated legacy code to rectify bugs, modernized features to boost user experience, and reinforced the platform's role as a pivotal digital repository for Pakistan's history

Talks

Counterexamples in Safe Rust

- ASEW '24 (Sacramento, Oct 2024)
- Stanford University (Security Lunch) (Stanford, Oct 2024)
- University of California, Davis (Systems Seminar) (Davis, Oct 2024)

Projects

Cargo-Sherlock: Trust Modeling in Rust Supply Chain Security | *Rust, Automated Reasoning* **Jan 2024 – Present**

- Developed *Cargo-Sherlock*, an open-source tool for automated reasoning that models trust within Rust's supply chain. This project combines programming language research with security analysis, providing transparency and assessment of trust factors in Rust's package management.

Rust Static Analysis Tool | *Rust, Python, Program Analysis* **June 2024 – Present**

- Designed *LHS*, an open-source static analysis tool for Rust's MIR (Mid-level Intermediate Representation) to detect potential memory safety issues and identify attack vectors in "safe" Rust code. This tool enhances Rust's security by pinpointing vulnerabilities beyond conventional safety checks.

Counterexamples in Safe Rust | *Rust, Program Analysis* **Published 2024**

- Co-authored and published a paper exploring scenarios where Rust's memory safety guarantees can be compromised. This work provides insights into limitations within Rust's safety model, contributing new understanding to the programming languages community.

LLMs as Coding Assistants | *LLMs (GPT, LLAMA2 , Falcon, Mistral) , Empirical Software Engineering* **Jan 2024 - Mar 2024**

- Developed a comprehensive evaluation framework for Large Language Models (LLMs) as coding assistants, analyzing their performance in simulating developer responses on Stack Exchange and Reddit platforms.
- Demonstrated LLMs' potential in software engineering research by achieving notable performance metrics, such as high cosine similarity and BERT scores, indicating their effectiveness in generating human-like responses across various coding domains.

Anycast Domain Name System | *Bash, Virtual Box, Linux , Python, Bind9* **Sep 2023 - Dec 2023**

- Engineered a distributed DNS framework, enhancing resilience against DoS attacks using a primary-secondary server replication strategy and load balancing, for improved traffic distribution and minimized single point of failure.
- Conducted performance evaluations comparing traditional single-server DNS setup with the distributed model under high-volume traffic scenarios. Demonstrated the robustness of the distributed system with a consistent 100% response rate, showcasing its effectiveness in maintaining uninterrupted internet accessibility under cyber-attack conditions.

Bloodlink : Automated Blood Donation Request System | *Flutter, Node, Mongoose, Git, Trello, Firebase* **Jan 2022 - May 2022**

- **Bloodlink Mobile Application Development**: Managed a team of five developers, transforming focus group insights on blood donation processes into a user-friendly Figma prototype aligned with UI/UX material guidelines.
- **Deployment & Testing**: Successfully transitioned the prototype into a fully-functional mobile application, with comprehensive user testing ensuring optimal functionality. The app is now available on the Play Store.

Keyword Spotting System *Google Colab, Python* **Jan 2022 - April 2022**

- Adapted the wave2vec 2.0 model, originally developed by Meta, to fine-tune its performance for the Urdu language, achieving significant advancements in linguistic AI for low-resource languages.
- Attained a high accuracy level of up to ninety percent in keyword spotting for Urdu, developing a system capable of detecting specific words within audio inputs, demonstrating the model's effectiveness in language processing tasks

Awards and Honors

- Fellowship at UC Davis (2023)
- Best TA of the Batch Award (LUMS 2023)
- Placed on Deans' Honor List LUMS (2019-2020)
- National Outreach Program Schoalrship (2019-2023)
- Merit Based Scholarship for Higher Secondary School (2017-2019)
- 44th position overall in country in High School Exams 44/226,619 (2017)

Technical Skills

Languages: Rust, Python, C, C++, JavaScript, HTML/CSS, Haskell, Bash, Latex
Frameworks: ReactJS, Node.js, Express.js, AngularJs, Flutter, Bootstrap
Databases: PostgreSQL, MongoDB, MySQL, Firebase, MySQL, SQLite
Developer Tools: Git, Docker, AWS, Heroku, Google Cloud, Trello, Postman, Selenium, Figma , Bind9