# Syed Rizwan Haider

371 Fairfield Way, Lab 423
Storrs, CT, 06269
✉ syed.r.haider@uconn.edu

## Interests

Computer Architecture & Architectural Security, Software Development, Mobile Application Development

## Education

**2017–2019** **MSc. Electrical Engineering**, *University of Connecticut*, Storrs, CT, USA.
Graduate Research Assistant in Secure Computation Lab.
Thesis: *"A Secure Enclave Migration Mechanism for Optimal Resource Management across Multiple Systems"*.

**2012–2016** **BSc. Computer Science**, *University of Lahore*, Lahore, Pakistan.
Thesis: *"Invigilator: Employee Monitoring and Management System"*.

**Courses** Secure Processor Architecture, Computer Architecture, Design and Analysis of Algorithms, Cryptography, Mobile Application Development for Health Care, Digital Image Processing.

## Academic Projects and Experience

**2017–Present** **Graduate Research Assistant, University of Connecticut**.

*Research Adviser: Prof. Marten van Dijk*.

**1. Leveraging Intel-SGX's Enclave Migration for Resource Management in a Multi-System Setup**.
- Devised a library to automate the migration process of Intel SGX enclaves to achieve balanced distribution of *memory* and *compute* resources across multiple system cores.
- **Employed Tools**: Intel-SGX SDK v2.4, C/C++, Visual Studio, PLayPUF (a special PUF), Linux, and Windows.
- **Skills Acquired**: Performance Analysis, Memory Bottleneck Analysis.
- Publication under preparation for "**IEEE International Symposium on Hardware Oriented Security and Trust 2020**".

**2. Self-Recovering Certificate Authorities using Backward and Forward Secure Key Management**.
- Developed smart self-recovering certificate authorities (CAs) to promise strong security guarantees against an adversary with perfect monitoring capabilities to leak secret data via the micro-architecture or digital state.
- **Employed Tools**: Intel SGX SDK 2.4, C/C++, Visual Studio, IPUF, LPNPUF, MIRACL, Windows, and Linux.
- **Skills Acquired**: Elliptic Curve Cryptography Implementation, Implementation of Intel SGX Local/Remote Attestation, Application/Library Optimization, and Multi-Module Integration.
- Publication under preparation for "**IEEE Symposium on Security and Privacy 2020**".

**Spring 2019** **3. Memory Management Simulator:** Devised a sequential simulator in C++ to model a memory management system consisting of a 4-way set-associative L1-cache and off-chip DRAM. Implemented a *Pseudo LRU* replacement policy for cache-line replacement and *Write-Back* policy for DRAM updates.

**Spring 2019** **4. Memory Integrity Verification:** Developed Merkle tree and MAC tree models in Python for memory integrity and freshness verification.

**Fall 2018** **5. Intel-SGX based Policy Enclave Implementation:** Introduced a policy checker in an Intel-SGX enclave, called policy enclave, for performing attestation and authentication in a real setting. An illustrative example of an ATM-machine was implemented to verify the correct functionality of the policy enclave.

**Fall 2018** **6. Android Application for Back Pain Management:** Worked in collaboration with the University of Connecticut Health Care department for developing an Android-based mobile application to keep track of a patient with back-pain history. It was further extended to support online appointment scheduling.

## Technical Skills

**Programming & Scripting:** C/C++, Java, Android (Kotlin, Java, XML), C#, Python, JavaScript, jQuery, HTML, CSS3, PHP, Assembly Language.

**SDKs and Libraries:** Intel-SGX SDK, MIRACL (Open source SDK for elliptic curve cryptography)

**Development Tools:** Android Studio, Visual Studio, NetBeans, Eclipse, MATLAB, LaTeX, PCSpim, MySQL, WAMP, XAMPP, Windows, Linux, Microsoft Office, Adobe Photoshop, Macromedia Flash.

## Teaching Experience

**2016–2017** **Programming Language Instructor**, *The Programmer*, Lahore, Pakistan – Taught Android (Java, XML), Java, and C/C++ to several student at the institute.