Raja Hasnain Anwar

✉ ranwar@umass.edu | in LinkedIn | 🎓 Google Scholar | 🌐 rhasnainanwar.me | 📍 Amherst, MA, USA.

TECHNICAL SKILLS

Programming: Python, C/C++, Java, JavaScript, PHP, SQL, MATLAB

Technologies: Flask, Django, Tornado, FastAPI, Selenium, Hibernate, Spring, SQLAlchemy, Node.js, React.js, jQuery, MySQL, MongoDB, Git, Docker, Kubernetes, AWS, GCP, Kafka, Apache Spark

Tools: VS Code, Cursor, Android Studio, Visual Studio, Jupyter, Oracle, Tableau, Power BI, Travis CI, GitHub Actions

DS / ML / AI: Huggingface, Transformers, PyTorch, TensorFlow, Keras, Pandas, NumPy, NLTK, spaCy, Agentic VLMs, SFT, DPO, GRPO, RAG, Reinforcement Learning, Synthetic Data Generation, LLM Evaluation, LLM-as-a-Judge

EDUCATION

University of Massachusetts Amherst — Amherst, MA, USA
Ph.D. in Electrical and Computer Engineering — *Transfer in, Sep 2023 – Present*
  Teaching: ENG 191: First Year Seminar (Cybersecurity & AI)

The University of Arizona — Tucson, AZ, USA
Ph.D. in Management Information Systems — *Jan 2021 – May 2023, Transfer out*
  Teaching: Penetration Testing, Ethical Hacking, and Social Engineering; Fundamentals of Cloud Computing

National University of Sciences and Technology (NUST) — Islamabad, Pakistan
B.S. in Computer Science — *Sep 2016 – Jun 2020*
  Capstone Project: Multimodal Face2Voice: A novel learning paradigm called deep shared latent space learning with a penalization that eliminates branching in multimodal training.

PUBLICATIONS

- Ishtiaq, A. A., and **Anwar, R. H.**, et. al., "Cloud Nine Connectivity: Security Analysis of In-Flight Wi-Fi Paywall Systems," *WiSec 2025*.

- **Anwar, R. H.**, et. al., "In Wallet We Trust: Bypassing the Digital Wallets Payment Security for Free Shopping," *USENIX Security 2024*.

- Islam, M. R., **Anwar, R. H.**, et. al., "Characterizing Encrypted Application Traffic through Cellular Radio Interface Protocol," *IEEE MASS 2024*.

- **Anwar, R. H.**, et. al., "Redefining the Driver's Attention Gauge in Semi-Autonomous Vehicles," *MSWiM 2023*.

- **Anwar, R. H.**, et. al., "Detecting Privacy Threats with Machine Learning: A Design Framework for Identifying Side-Channel Risks of Illegitimate User Profiling," *AMCIS 2023*.

Talks
- "Human-in-the-Loop for Secure Digital Wallets Transactions," *SOUPS 2024*.

- "Keeping Eyes on the Road: The Role of Situated IS Delegation in Influencing Drivers' Situational Awareness," *ICIS 2021*.

EXPERIENCE

Microsoft — Redmond, WA, USA
Data Science Intern — *May 2025 – Aug 2025*
- Built an automated pipeline for synthetic data curation and filtering to finetune VLMs (CUA, Qwen, UI-TARS) for GUI agents.
- Developed an LLM-as-a-judge pipeline for GUI automation task evaluation and analysis with a focus on ensuring the safety of agent actions.
- Led SFT and GRPO on agentic VLMs, achieving significant performance improvement in productivity tasks.
- Developed evaluation environment and infrastructure for a new benchmark to test GUI agents on productivity tasks involving Microsoft Office Suite (Word, Excel, PowerPoint).

University of Massachusetts Amherst — Amherst, MA, USA
Graduate Research Assistant — *Sep 2023 – Present*

- Identified side-channels in the 5G control plane, achieving over 95% accuracy in user application and activity recognition over encrypted traffic using machine learning (IEEE MASS'24).
- Developed a GPU side-channel attack for ML model classification with over 90% accuracy against major VLM and LLM models (under review).
- Led an empirical study on in-flight WiFi paywall security and inferred network tomography and policies to launch tunneling and DoS attacks, across major ISPs and airlines (WiSec'25).

Kaiser Permanente
Pleasanton, CA, USA

Data Science Intern
Jun 2023 − Aug 2023

- Revamped a classification pipeline to accurately identify at-risk patient groups, resulting in 20% improvement.
- Employed spline-based feature transformation models to handle nonlinear features like patient age groups.
- Integrated SHAP value generation for in-depth analysis of the production model's behavior against sensitive features, i.e., gender, age, & race.
- Successfully integrated the developed AI models into a live system by the end of the internship.

The University of Arizona
Tucson, AZ, USA

Graduate Research Associate
Jan 2021 − May 2023

- Led systematic testing of financial systems and EMV protocol through tomographic analysis focusing on credit card transaction policy compliance (USENIX Security'24).
- Developed novel side-channel attacks on typing behavior, achieving 80% accuracy in user profiling and typed text classification using a novel ML-based framework (AMCIS'23).
- Designed a novel driver's attention-gauging and alert mechanism for semi-autonomous to improve takeover time in emergencies by 75x (MSWiM'23).

TUKL-NUST R&D Center
Islamabad, Pakistan

Research Assistant
Apr 2017 − Jun 2020

- Built an Android app to scan vehicle registration plates using an OCR and display the owner's details from a public database. This app is a part of the RoadwayIntel vehicle surveillance project in the city of Islamabad.
- Gathered 120 hours of video dataset for fish detection and tracking in the wild, used for population estimation.
- Automated image superimposition to generate 20 images per document extraction sample by augmenting foreground and background settings.
- Unified text mining and personally identifiable information (PII) detection pipelines to mask private information from public judicial archives with 70% accuracy.

Hochschule RheinMain
Wiesbaden, Germany

Research Assistant
Jun 2019 − Aug 2019

- Generated a dataset with over 1,000,000 entity pair data points from raw English and German Wikipedia texts for entity relation extraction.
- Architected an LLM pre-training pipeline that leverages context similarity as an entity relation estimator to automate 100% of labeling.

VisionX Technologies
Islamabad, Pakistan

Machine Learning Engineer
Jun 2018 − Jun 2019

- Engineered an OCR and heuristical information extraction pipeline to digitalize hand-written tabular property records with 85% accuracy.
- Developed a web tool to visualize and correct extracted data improving pipeline efficiency by 50%.
- Reproduces multiple solutions from Kaggle's CDiscount Classification challenge and designed hierarchical deep learning models for large-scale visual recognition and classification.

Al Jazeera
Remote

Machine Learning Engineer
Aug 2018 − Dec 2019

- Implemented and trained a key frame extraction model to summarize videos and select top visuals making headlines generation 70% faster.
- Designed and trained an image captioning model for 70% faster on-demand news headlines generation from key frames.
- Integrated real-time audio transcription services for Arabic and English in a live stream with a 5-second delay.
- Developed a large-scale sentiment analysis system to monitor real-time trends from news and social media in English and Arabic.
- Automated multimedia search with an audio matching tool for automatically retrieving audio/video samples using a 10-second audio query.
- Developed a large-scale faces-in-the-wild recognition tool for identifying celebrities from live streams.

Press & Media Coverage

Investopedia: "Cybersecurity Alert: Why Your Mobile Wallet May Not Be Safe Even With a VPN", July 05, 2025.

CNET: "Are Digital Wallets Safe? Here's How to Protect Your Financial Information in 2024", Sep 25, 2024.

Consumer Affairs: "Study: The Safety of ApplePay and GooglePay Called Into Question", Sep 16, 2024.

PaymentsDive: "Academics Question Digital Wallet Security", Sep 04, 2024.

Hacker Dose: "Digital Wallet Loophole Allows Criminals to Shop for Free with Locked Cards", Sep 04, 2024.

Business West: "New Study Reveals Loophole in Digital Wallet Security", Aug 30, 2024.

National Science Foundation (NSF): "A New Study Reveals Loopholes in Digital Wallet Security", Aug 23, 2024.

Association for Computing Machinery (ACM): "A Loophole in Digital Wallet Security", Aug 23, 2024.

Forbes: "This Week In Credit Card News", Aug 22, 2024.

TechRadar Pro: "Digital Wallets Allow for the Use of Stolen Credit Cards" (MSN, Yahoo! Tech), Aug 20, 2024.

The Register: "Digital Wallets Can Allow Purchases With Stolen Credit Cards", Aug 20, 2024.

PYMNTS: "5 Emerging Security Imperatives for Digital Wallets", Aug 21, 2024.

Kaspersky: "Digital Wallets Can Enable Cybercriminals to Make Purchases with Stolen Credit Cards", Aug 20, 2024.

NewsBytes: 'Security Flaw Allows Stolen Credit Card Use on Digital Wallets", Aug 20, 2024.

Help Net Security: "Stolen, Locked Payment Cards Can be Used with Digital Wallet Apps", Aug 19, 2024.

ScienceX: "Best of Last Week—..., Loophole in Digital Wallets,...", Aug 19, 2024.

UMass News: "New Study Reveals Loophole in Digital Wallet Security—Even If Rightful Cardholder Doesn't Use a Digital Wallet", Aug 14, 2024.

Honors & Awards

2025 – **Teaching Fellowship:** Selected by College of Engineering at the University of Massachusetts Amherst.

2025 – **ACM WiSec:** Received NSF travel grant to attend ACM WiSec 2025 in Arlington, VA, USA.

2024 – **ACM IMC:** Received NSF travel grant to attend ACM Internet Measurement Conference in Madrid, Spain.

2024 – **IEEE MASS:** Received NSF travel grant to present my work at IEEE MASS 2024 in Seoul, South Korea.

2024 – **USENIX Security:** Received registration grant to attend USENIX Security in Philadelphia, PA, USA.

2024 – **Teaching Fellowship:** Selected by College of Engineering at the University of Massachusetts Amherst.

2023 – **NSDI:** Received USENIX travel grant to attend NSDI'23 in Boston, MA, USA.

2023 – **POWDER RENEW:** NSF-funded workshop on POWDER wireless emulator at UofU.

2022 – **Colosseum Young Gladiator:** NSF-funded master class on Colosseum wireless emulator at NEU.

2021 – **Nunamaker-Chen Scholarship:** Selected by MIS department at The University of Arizona.

2020 – **Summer@EPFL:** Selected for prestigious summer internship programme (2% acceptance rate).

2020 – **Huawei UG Star Researcher:** Received for best undergraduate research project.

2019 – **DAAD Research Fellow:** Selected for German Academic Exchange Service (DAAD) research fellowship.