FAIZAN AHMAD

+1 (434) 249-3480
fa7pdn@virginia.edu

EDUCATION

University of Virginia *2018-Present*
Masters in Computer Science
Research Areas: Cyber Security, Vulnerability Analysis, Deep Learning, Data Science, Computer Vision, Text Analytics.

FAST National University Lahore *2014-2018*
Bachelors in Computer Science Overall GPA: 3.72/4

COMPUTER SECURITY ACHIEVEMENTS

· **Bug Bounties.** Received bug bounties, gifts and acknowledgements for finding vulnerabilities in web applications of 30+ companies including ***Google***, ***Microsoft***, ***Apple*** and more.

· **Security Blog.** Ran a successful blog (Fsecurify) about machine learning and security with 1 million visits within a year. Posts from the blog were featured on multiple high ranked websites such as Hackernews and Computerworld.

· **Open Source Security Tools.** Built a tool for automated Cross Site Scripting detection which has been widely used by users to find XSS vulnerabilities. It was used by the *director of an Infosec Blue Team at Microsoft* to find a bug in ***Pentagons Hack the Pentagon program.***

RESEARCH EXPERIENCE

University of Virginia August 2017 - Present
Graduate Research Assistant *Advisor: Dr. Ahmed Abbasi*

· Working with Pfizer for ***adverse event detection of drugs*** from search queries data of a large number of users. Using enriched auto encoders with a user modeling approach, we have achieved state of the art results.

· Designed and developed a deep learning architecture leveraging multiple novel embeddings including demographical and parallel representations embeddings for ***psychometrics text classification***.

University of Iowa August 2017 - July 2018
Research Assistant *Advisor: Dr. Zubair Shafiq*

· Lead a research project on ***adversarial machine learning***. Used genetic algorithms and multiple types of word embeddings to obfuscate text against several state of the art authorship attribution systems.

University of Illinois Urbana-Champaign December 2016 - August 2017
Research Assistant *Advisor: Dr. Mathew Caesar*

· Worked on analyzing the causes of typing errors for website domains, created an extensive user-centric typographical model based on human hand anatomy and applied machine learning to detect the most likely typed typos of a domain. This work resulted in a publication: ***It's All in the Name: Why Some URLs are More Vulnerable to Typosquatting (IEEE INFOCOM 2018)***.

Lahore University of Management and Sciences January 2016 - July 2018
Research Assistant *Advisor: Dr. Fareed Zaffar*

· Lead a project on ***detecting child unsafe content*** on media streaming platforms such as Youtube Kids. Developed a highly accurate multi-faceted deep learning architecture including Convolutional and Recurrent Neural Networks to flag harmful content for children.

· Worked on ***cryptomining detection using hardware performance counters***. Developed a machine learning system to flag mining in any website with 99% accuracy. Ran our system in the wild and found hundreds of mining websites using advanced obfuscation techniques that went undetected by all previous methods.

· Worked with doctors at *UC Davis* to develop a deep learning system for ***detection of Tuberculosis*** using X-ray images and biomarkers.

· Worked on conducting a survey study for our proposed defense against compelled certificate attacks. Resulted in a publication: ***Detecting and Defending against Compelled Certificate Attacks using Origin-Bound CAPTCHAs (SECURECOMM 2018)***

INDUSTRY EXPERIENCE

Yotascale August 2016 - March 2017
Remote Machine Learning Engineer *Silicon Valley*

· Developed a probabilistic anomaly detection system to inform users about any anomalous activity in their cloud systems.

Medialogic February 2017 - November 2017
Machine Learning Engineer *Lahore*

· Created a machine learning based pipeline to predict demographics of users watching television.

RELEVANT COURSES

Core Courses
Introduction to Algorithms
Data Structures
Databases
Assembly Language
Operating Systems
Computer Networks
Computer Architecture
Artificial Intelligence

Other Courses
Convex Optimization
Deep Learning for Computer Vision (MOOC)
Natural Language Processing
Digital Image Processing
Software Security by Program Analysis
Introduction to Graduate Statistics
Machine Learning (MOOC)
Cryptography (MOOC)

PUBLICATIONS

· Bringing the Kid back into YouTube Kids: Detecting Inappropriate Content on Video Streaming Platforms (In Submission to ICWSM 2019)
Faizan Ahmad, Hammas Saeed, Shiza, Fareed Zaffar, Christo Wilson

· Countering Cryptojacking and Parasitic Miners on the Web (In Submission to IEEE INFOCOM)
Rashid Tahir, Sultan Khan, **Faizan Ahmad**, Hammas Saeed, Fareed Zaffar

· Finding Needles in a Haystack: Deep Learning for Rare Adverse Event Detection, INFORMS Workshop on Data Science 2018
Faizan Ahmad, Ahmed Abbasi, Brent Kitchens, Daniel Zeng

· A Deep Learning Architecture for Psychometric Natural Language Processing, INFORMS Workshop on Data Science 2018
Jingjing Li, Ahmed Abbasi, **Faizan Ahmad**, Hsinchun Chen

· It's All in the Name: Why Some URLs are More Vulnerable to Typosquatting, IEEE INFOCOM 2018
Rashid Tahir, Ali Raza, **Faizan Ahmad,** Jehangir Kazi, Fareed Zaffar, Chris Kanich, Matthew Caesar

· Detecting and Defending Against Certificate Attacks with Origin Bound CAPTCHAS, SECURECOMM 2018
Adil Ahmad, **Faizan Ahmad**, Lei Wei, Vinod Yegneswaran, Fareed Zaffar