# FALAAH ARIF KHAN


## CONTACT INFO

Email: falaah@montrealethics.ai

Twitter: @FalaahArifKhan

Instagram:
mixed media: @thefaladox
comics: @themachinelearnist

https://falaaharifkhan.github.io/research/


Research Fellow | Artist in Residence

An Engineer/Scientist by training and an Artist by nature, I conduct fundamental research on Robust and Ethical ML and create Scientific Comics to translate the technical nuances of this work in a way that is accessible to the general public.

## EDUCATION

**Bachelor of Technology, Electronics and Communication Engg (with Distinction)**
Shiv Nadar University (2014-18)
GPA: 8.87/10
Thesis: Behavioral Biometrics and Machine Learning to secure Web Logins
Minor: Mathematics

## PUBLICATIONS

1. **Arif Khan F.**, Kunhambu S., G K. C. (2019) **Behavioral Biometrics and Machine Learning to Secure Website Logins**. In: Security in Computing and Communications. SSCC 2018. Communications in Computer and Information Science, vol 969.

## PATENTS

1. **Arif Khan, Falaah**, Kunhambu, Sajin and Chakravarthy G, K. **Behavioral Biometrics and Machine Learning to secure Website Logins.** US Patent 16/257650, filed January 25, 2019
2. **Arif Khan, Falaah**, Mohammed, Tousif, Gupta, Shubham, Dinh, Hung and Kannapan, Ramu. **Event-Based Search Engine**, US Patent 16/752775, filed January 27, 2020
3. **Arif Khan, Falaah** and Sharma, Hari Surender. **Framework to Design Completely Automated Reverse Turing Tests.** US Patent 16/828520, filed March 24, 2020 and US Patent (Provisional) 62/979500, filed February 21, 2020

## SCIENTIFIC COMICS

1. Falaah Arif Khan. Meet AI (2020), in AAAI Interactive Magazine
2. Falaah Arif Khan and Julia Stoyanovich. "Mirror, Mirror". Data, Responsibly Comics, Volume 1 (2020)

## WORK EXPERIENCE

**Research Fellow | International Institute of Information Technology, Hyderabad**
August 2020 - Current

Supervisor: C.V. Jawahar, CVIT Lab
Topic: Deep Bayesian Active Learning for Neural Machine Translation

**Artist in Residence | Montreal AI Ethics Institute**
July 2020 - Current

**Research Software Engineer II, Dell EMC Bangalore**
August 2019 - May 2020

- Implemented a bot detection filter to identify malicious attempts performed from headless devices (without browser activity), which brought the average number of attempts needed to be manually evaluated down by 87.6%, the average number of accounts that need to be manually protected down by 95% and in a recent credential stuffing attack, the system was able to successfully thwart 99.71% of the malicious requests
- Formulated a novel framework to design adaptive robust Completely Automated Reverse Turing Tests that learn on the fly and do not require periodic manual design. The framework works on Adaptive Mechanism design, by learning preferences of human users and custom deep adversaries. The optimal experimental design is learned using Bayesian Inference. The product is live on Dell login pages, globally.

**Research Software Engineer I, Dell EMC Bangalore**
July 2018 - August 2019

- Delivered a behavioral biometrics-based security product that classifies browser activity as being done by a human or by a bot. It is built using an auto associative neural network, trained on client biometrics such as keystrokes, click patterns and mouse dynamics. Classifications are made based on reconstruction error between the sample and the prediction. The product is live on Dell login pages, globally.
- Created a product traffic forecaster using a Recurrent Neural Network trained on activity logs of the product, to automate the continuous evaluation of product traffic. Insights from the forecaster have been used to alert any anomalous behavior. Instances where traffic has exceeded the baseline have helped identify adversarial action. Deteriorating product health has also been flagged using the baseline, when traffic has fallen below the baseline.
- Architected a graph signal processing approach to dynamic threat modelling. Application logs are used to model the product as a weighted directed graph, where vertices are code elements and edges indicate function calls between elements. Unsupervised learning models are used to set edge weights as indicators of vulnerability to a specific attack. Graph filters are then created and nodes that pass through the filter form the vulnerable subgraph. Superimposing all the vulnerable subgraphs with respect to the different attacks gives rise to a threat model, which is dynamic in nature and evolves as the product grows.

**Software Engineering Intern, Dell EMC Hyderabad**
January 2018 - April 2018

Prototyped a human vs human, genuine/imposter classification model, to identify account match attacks on web logins and evaluated the efficacy of this model for a password-less authentication system. The model can differentiate two human subjects that are using the same credentials to log in, on the basis of their login behavior

## AWARDS/HONORS

- **Game Changer Award** from Hemal Shah, SVP and Regional CIO, Dell EMC for outstanding innovation in the security features of the Dell Access and Identity Management (DAIS) Product (August'19)
- **Winner, AI Center of Excellence Hackathon**, Dell EMC (July '19)
- **Winner, Shark Tank**, Dell EMC (June '19)
- **Winner, SafeHack (Security Hackathon)**, Dell EMC (April'19)
- **Long Term Investment Award** from Dell EMC (March'19)
- **Dell Champion Award** from Dell EMC (March'19)
- **Winner, Hack.Fin (FinTech Hackathon)**, Dell EMC (Dec'18)
- **Winner, HackLabs Innovation Rally '18 Hackathon**, Dell EMC (Sept'18)
- **Recipient of Category 'A' Scholarship** (Complete Waiver of Tuition Fees) at Shiv Nadar University (Aug'14)

## TECHNICAL SKILLS

**Tools and Languages**
Python, C#, dotnet, Java, JavaScript, Verilog, MATLAB, LT Spice. Databases: Mongo, SQL, Redis

**Certifications**
'Foundations of AI/ML', International Institute of Information Technology, Hyderabad (May '18)

**Analytical Skills**
Classification, Regression, Time Series Analysis, Word Embeddings, Clustering, Neural Networks,
Tree Based Models, Support Vector Machines, Bayesian Models, Ensembles, Auto-Encoders, Convolutional Neural Networks, Deep Learning Models, Generative
Adversarial Networks, Mathematical Modelling, Graph Theory, Signal Processing on Graphs, Algorithmic Game Theory

**Project Skills**
Pivotal (Extreme Programming), Agile

## BLOG

https://thefaladox.wordpress.com/

**Research-cum-Teaching Assistant, Basics of Electrical and Electronic Circuits | Dept of Electrical Engineering, Shiv Nadar University**
August 2017 - December 2017

**Instructor:** Prof R. N. Biswas (IIT Kanpur)
Designed, conducted and graded weekly lab experiments and tutorials for a class of 30-40 students. Also assisted in conducting and grading the final lab examination.

**Research-cum-Teaching Assistant, Digital Electronics | Dept of Electrical Engineering, Shiv Nadar University**
August 2017 - December 2017

**Instructor:** Prof Sonal Singhal (Shiv Nadar University)
Designed, conducted and graded weekly lab experiments and the final lab examination for a class of 30-40 students.

**Intern | Defence Research and Development Organization, Hyderabad**
July 2017 - August 2017

**Supervisor:** Dr Laxman Prasad (Programme Air Defence, DRDO)
Studied and simulated security protocols in communication networks.

**Student Tutor, Mathematical Methods | Learning and Academic Support Center, Shiv Nadar University**
January 2017 - May 2017

**Instructor:** Prof Ajit Kumar (PhD, University of Houston)
Curated supplementary course content, delivered lectures and conducted tutorials and practice tests for class of 20-30 students

## RESEARCH PROJECTS

**Automated Driver,** As part of 'Foundations of AI/ML' Certification @IIIT-H
January 2018 - May 2018

- Implemented basic operations of automated driving, including detecting traffic signs and traffic signal states, identifying obstacles and the subsequent suitable navigation. The automated driver is created by training a convolutional neural network with navigational images and a clustering algorithm using LIDAR data of a bot moving in a simulated environment using Gazebo simulator and ROS.

**Booking Assistant,** As part of 'Foundations of AI/ML' Certification @IIIT-H
January 2018 - May 2018

Created a chatbot that serves as a booking assistant, implementing two skills of making restaurant reservations and movie bookings. Implemented in Python, the bot distinguishes between intents, extracts required attributes and makes suitable recommendations

**Fingerprint Classification,** Supervised by Prof Madan Gopal (IIT Delhi)
August 2017 - December 2017

- Performed fingerprint classification on the NIST fingerprint dataset, by using Convolution Neural Networks (CNN), as both a feature extractor and a classifier. The features extracted by the CNN were also used to train a Support Vector Machine and their classification accuracies were compared.

**Tornado Prediction,** Supervised by Prof Madan Gopal (IIT Delhi)
January 2017 - May 2017

Forecasted tornado occurrences in the United States, including their magnitude and source (state), using a Recurrent Neural Network trained on data of tornado occurrences between 1950 to 2009 across the United States published by the Storm Prediction Center.