# SHIKHAR SAKHUJA


**Software Engineer (Product & Machine Learning)**

shikharsakhuja@gmail.com | shikhar394.github.io | shikhar394 | +1 639-318-0007
Toronto, Ontario, Canada | shikhar394


## EXPERIENCE

### Motive Inc. / Software Engineer

August '21 – Ongoing — Toronto, Ontario, Canada

- Digitizing the physical economy by building fintech, electronic fleet tracking and AI solutions for **>1,000,000 long-haul truck drivers across 250,000 transportation companies.**
- Building backend infrastructure for **Motive Cards (Corporate Cards) and spend management systems**. Handling **>$300,000,000 of transactions**.
- Engineer and maintain distributed backend systems and APIs using **Ruby on Rails, SQL, GoLang, and PostgreSQL DB.** hosted on AWS.

### Labforge Inc. / Software Engineer

June '20 – July '21 — Waterloo, Ontario, Canada

- Orchestrated end-to-end machine learning pipelines using **Python, AWS, Docker, and Kubernetes** for rapid deployment of deep learning models. Processed and analyzed a large dataset of >1,000,000 high-resolution images.
- Built client-facing camera interface using **Electron, React, Redux, and GoLang, with gRPC and Protobuf** for IPC. Used by >1,000 users.

### University of Waterloo / Graduate Research Assistant

September '19 - April '21 — Waterloo, Ontario, Canada

- Detecting CAN Bus intrusions with 100% precision using **ensemble of LSTM, Transformers, and CNN models** (<100,000 parameters) that can run on low-compute environments.
- Detected SSH attempts on an HP Network Switch through only its power consumption with 99% accuracy using **LSTM**.

## EDUCATION

### M.Math. in Computer Science *(Ph.D. Track)*

GPA: 91/100

**University of Waterloo**

September '19 - April '21 — Waterloo, Ontario, Canada

### B.Sc. in Computer Science (Honors)

GPA: 3.7/4

**New York University**

August '15 - May '19 — Shanghai, China | NYC, USA

## SELECT PUBLICATIONS

- S. Sakhuja, M. Dunne, S. Fischmeister, *"The Boy Who Cried Wolf: On Precision in CAN Bus Intrusion Detection,"* $8^{th}$ Embedded Security in Cars Conference (ESCAR), USA 2021.
- S. Sakhuja, R. Cohen, *"Ridesafe: Detecting Sexual Harassment in Rideshares,"*, 33rd Canadian Conference on Artificial Intelligence, Canadian AI 2020, Ottawa, Canada.

## SKILLS & LANGUAGES

- Experienced in Object Oriented Design and in working with languages such as Python, GoLang, C, C++, Javascript, ReactJS, and Java.
- Proficient in English, Hindi, Mandarin, Punjabi and Urdu.

## PROJECTS

**BookRec** (React, GoLang)

- Building a **highly curated online book forum** experience by leveraging data from user's activity on social media.
- Conducted **20+ user interviews** and working on Beta release.

**RideSafe** (React Native, Redux, Python)

- An application that leverages Natural Language Processing to **tackle sexual harassment in rideshares.**
- Identifies emotional distress in female voice with **100% recall using SVM and 1D CNN**.

**LogsThatTalk** (Electron, React, Redux, Python)

- A **conversational agent** that interacts with system logs and uses **machine learning to generate security reports.**
- Pilot studies showed that **100% users felt they saved time and effort** while using the chatbot to access logs over manually.

**Nwitter** (React, Redux, PostgreSQL, GoLang)

- A **fault-tolerant distributed social networking application** made to look and feel like Twitter.
- Implemented **Viewstamped Replication** for data persistence and consensus.

**Ilmademia** (Flutter, Dart, Firebase, Python)

- An intelligent platform that offers homework support to high-school students from **countries with limited internet access.**
- Pilot study being run on **students from 4 countries in South Asia.**

**Voice[H]over** (Java in Processing)

- An HCI system built using Computer Vision and Natural Language Processing algorithms that **allows people with Cerebral Palsy and other immobilizing disabilities to talk using an eye controlled virtual keyboard.**
- **Winner of Assistive Tech** track at HackNYU '17. Code open sourced on GitHub.

**SCIDS** (Python)

- A side-channel based intrusion detection system that offers **integrity assessment and runtime monitoring** for network equipment.
- Uses machine learning to **identify attacks such as Firmware Manipulation, Hardware Tampering, and Log Forging with a average precision of 99%.**