Mohammad Abdul Hadi

Malware Analysis | Large Language Models
SE | NLP | MLOps

CONTACT

38, Floor # 5, East Wing,
4321 Still Creek Dr,
Huawei Technologies Canada Co., Ltd.,
BC V5C 6S7,
Canada

hadi[dot]mashuk[at]gmail[dot]com
linkedin.com/in/mohammad-abdul-hadi/
sites.google.com/view/mohammad-hadi/
mohammad-abdul-hadi.github.io/
+1 250 899 6971

SUMMARY OF CURRENT WORK

As an AI Security Researcher (Senior Software Engineer) at Huawei Technologies R&D – Vancouver, I am deeply engaged in AI Security Research, focusing on the intersection of Malware Analysis and Large Language Models (LLMs). My key responsibilities include collaborating with malware analysts, developing and optimizing malware classification models, Refining, optimizing, and streamlining LLMs for targeted applications, and ensuring seamless deployment and operation of AI models in production environments. Additionally, I conduct cutting-edge research in AI and cybersecurity, monitor and analyze the performance of AI models, and maintain comprehensive documentation of my findings.

Previously, I spent two years developing a Malware Filter Framework (MFF) as part of an Embedded Emulator Development team. This role required skills in Linux Kernel development, memory management, and CPU performance profiling. I was responsible for designing, coding, (threat) modeling, debugging, and triaging issues for cloud/local service modules, while implementing effective design patterns and adhering to security frameworks. This foundational experience has seamlessly transitioned into my current role, equipping me with the necessary skills to excel in advanced AI-driven environments and contribute effectively to pioneering cybersecurity solutions.

In my pastime, I train and motivate underprivileged students from Bangladesh who aim to become stellar researchers and programmers. Currently, I am advising two research teams during the weekends. They are building components of a cutting-edge speech-to-text system suitable for Bangladeshi accents, which can help doctors effortlessly keep an organized medical history of impoverished patients.

EDUCATION

❑ MSc in Computer Science

The University of British Columbia (UBC), Canada

CGPA: 4.33 / 4.00 (Summa Cum Laude)
Supervisor: Dr. Fatemeh H. Fard

My research focused on the intersection of Transfer Learning (Large Language Models) and Software Engineering (SE) to solve critical software development-related issues, such as detecting anomalous software behavior, program-analysis, code-smells detection, generating code comments, program retrieval, and synthesis. I applied Knowledge Transfer and Distillation techniques to improve some popular Topic Modeling and Text Classification techniques. Through my research, I tried to understand and replicate 'good' software development processes by designing deep learning systems, which, in turn, attempted to generate and describe the features of interest from an application perspective. My end goal was to simplify software development for the masses and design AI-driven large scalable applications that can help developer communities solve software-related problems more efficiently with less effort.

❑ BSc in Computer Science and Engineering

North South University (NSU), Bangladesh

CGPA: 3.99 / 4.00 (1st position in School of Engineering and Physical Sciences)
Summa Cum Laude, Vice Chancellor's Gold Medalist

SCHOLARSHIPS, AWARDS & ACCOLADES

Name of the Scholarships and Awards	Recipient ratio		Institution		Year
• University Graduate Fellowship	5%	-	UBC	-	2020
• Dean's Entrance Scholarship	6%	-	UBC	-	2019
• Vice Chancellor's Gold Medal	1/1870	-	NSU	-	2019
• Faculty Research Grant	5%	-	EU	-	2018
• Capstone Project Design Grant	3%	-	NSU	-	2018
• 100% Undergraduate Scholarship	3%	-	NSU	-	2014
• Secondary (High) School Certificate Scholarship	0.01%	-	CCS	-	2010
• Junior (Elementary) School Certificate Scholarship	0.025%	-	SBK	-	2004

TECHNICAL KNOWLEDGE

• Languages	C, C++, Swift, Python, Go, Rust, Scala, Java, R, C#, SQL, Assembly;
• Web and Scripts	ASP, PHP, JavaScript, Typescript, D3.js, Node.js, JSON, AJAX, HTML, CSS;
• Frameworks	ASP.NET, Laravel, Bootstrap, Django, OOPHP, Flask;
• Tools	MATLAB, Logisim, Micro-wind, PSpice, emux8086, IDA;
• Libraries	PyTorch, TensorFlow, Keras, HuggingFace, Fast.ai, OpenNN, OpenML;

KEY ATTRIBUTES

- Determined to make a difference to individuals and communities.
- Fastidious, urbane, and eloquent with excellent communication skills.
- Approachable and non-judgmental.
- Self-Motivated, quick learning, and patient.
- Frequently stepping outside the comfort zone to pursue and cultivate diverse skillset.
- Always on my way to take challenges to unlock untapped potential.
- Enthusiastic about building a rich repertoire by searching beyond the immediate horizon.

WORK EXPERIENCE (1/2)

❑ Huawei Technologies Canada Co., Ltd., BC, Canada

AI Security Researcher (Senior Software Engineer - Anshi Lab) Oct 24 – Present

I am Working on the intersection of Malware Analysis and LLM. The key responsibilities include:

- **Collaborate with Malware Analysts:** Work closely with malware analysts to identify the requirements, scopes, and environments for implementing LLM solutions in malware detection and analysis.
- **Model Development and Optimization:** Develop, evaluate, optimize, and scale core malware classification models. Enable large-scale training and inferencing of advanced AI models on novel AI hardware.
- **AI Algorithmic Innovation:** Operate at the intersection of AI algorithmic innovation, purpose-built AI systems, tools, frameworks, and software to drive forward the capabilities of malware detection technologies.
- **LLMOps and System Integration:** Design, integrate, and maintain systems for LLM operations, ensuring seamless deployment and operation of AI models in production environments.
- **Research and Development:** Conduct cutting-edge research in AI and cybersecurity, staying abreast of the latest developments in both fields to continuously improve our malware detection capabilities.
- **Cross-functional Collaboration:** Work closely with researchers, developers, and other stakeholders to ensure the successful implementation and scaling of AI solutions.
- **Performance Monitoring:** Monitor and analyze the performance of AI models in detecting and classifying malware, making necessary adjustments to improve accuracy and efficiency.
- **Documentation and Reporting:** Maintain comprehensive documentation of research findings, model development processes, and system integration efforts. Report progress and results to stakeholders.

Software Engineer (Data and Privacy Protection Technology Lab) Oct 22 – Oct 24

I am working on Malware Filter Framework – MFF. MFF's technology map requires skills in Linux C programming, memory management, optimization and troubleshooting, CPU performance profiling, Linux Kernel development, and user-space C process development. As a Software Engineer on the Network Appliance Embedded Software Development team, I:

- Participated in software design, coding, debugging, threat modeling, and triaging issues for the cloud/in-device service modules throughout all aspects of MFF's development lifecycle. During my tenure, I improved the product performance by ~315%.
- Proactively sought out and participated in module refactoring to optimize the overall design and preserve the coding standards by collaborating with my colleagues.
- Implemented and maintained effective software design patterns to improve and streamline the overall architecture, ensuring the codebase is optimized and efficient.
- Introduced and incorporated the best software engineering practices in the industry, (i.e., testing, design, and software building technologies) to improve efficiency.
- Prioritized the adoption of the established and emerging security frameworks, isolation techniques, encryption standards, coding practices, tools, and exploits, to enhance the collective efficiency of our product.

❑ The University of British Columbia, BC, Canada Sep 2019 — Sep 2022

Research Assistant

- Machine Learning
- Software Engineering
- Natural Language Processing
- Data Analysis and Visualization

Teaching Assistant

- COSC 328: Computer Networking
- COSC 304: Database Management System
- COSC 341: Human-Computer Interaction
- COSC 407: Parallel Computing

WORK EXPERIENCE (2/2)

❑ **Singapore Management University (SMU)** Jul 2021 – Feb 2022

Research Assistant (Software Analytics Research Lab – SOAR Lab)

Project: DeepHarvest: The tool collects and links pieces of information about APIs in different libraries from diverse online resources; It also disambiguates simple API names.
Supervisors: Dr. David Lo, SMU; Dr. Fatemeh H. Fard, UBC.

❑ **Scrawlr Inc., BC, Canada** May 2021 – Aug 2021

Software Developer Intern (Mitacs)

Project: High-throughput linguistic content comparison and sentiment analysis.
Supervisors: Dr. Fatemeh H. Fard, UBC; Dr. Jonathan Shahen, Scrawlr.

❑ **Niedner Inc., QC, Canada** Jan 2020 – Jun 2020

Software Developer Intern (Mitacs)

Project: Modeling and optimization of woven composite hydraulic tubes, to reduce in-service defects and failures—Phase II.
Supervisors: Dr. Abbas S. Milani; Dr. Fatemeh H. Fard, UBC.

❑ **Eastern University, Dhaka, Bangladesh** Jul 2018 — Aug 2019

Lecturer, Department of Computer Science and Engineering

Courses Taught:

- Mathematical Analysis for CS
- Digital Logic Design
- Structural Programming - JAVA
- Computer Architecture
- Web Programming
- Design and Analysis of Algorithm
- Intro to Software Engineering

❑ **North South University, Dhaka, Bangladesh** Aug 2016 — Aug 2019

Lab Instructor, Department of Electrical and Computer Engineering

- Computer Organization and Architecture
- Programming Language II - Java
- Database Systems
- Digital Logic Design
- Microprocessor, Micro-controller and Peripheral Devices

Teaching Assistant, Department of Electrical and Computer Engineering

- Introduction to VLSI design.
- Introduction to Frameworks for Web-development

Teaching Assistant, Department of English and Modern Languages

- Introduction to Composition - I
- Introduction to Advanced Intermediate Compositions
- Introduction to Fiction and Creative Storytelling

VOLUNTEER EXPERIENCE

- **ICSE 2021** May 2021
- **ICSE-2020** Jun 2020 – Jul 2020
- **ACM Joint ESEC/FSE, 2020** Nov 2020 – Dec 2020

Student Volunteer

Student Volunteers (SV) managed sessions at different time slots around the globe. SVs were given training on new technologies so that we could be part of large-scale production. SVs helped to organize live streaming of the conference presentations and online Q&A.

- **Archer K. Blood Library and EMK Center, USA Embassy, Dhaka, Bangladesh** Mar 2018 — Aug 2018

Workshop Designer & Instructor

- Designing and conducting workshops to teach technical web development and freelancing skills for the underprivileged Bangladeshi community.
- Technological Soft-Skill development programs for teenagers and preteens.

- **NSU ACM Student Chapter,** Jul 2017 — Mar 2018
  North South University, Dhaka, Bangladesh

  Programming Tutor and Workshop Designer
  - Design, Implementation, and Analysis of Algorithms
  - Basic and Object-Oriented Programming
  - Problem Solving using C, C++, Java, Python

PUBLICATIONS

- **M. A. Hadi** and F. H. Fard. 2022. What Do Developers Discuss on PyTorch Discussion Forum and How to Serve Developers Better via Crowd Sourced QA platforms? Submitted to SANER 2022.
- **M. A. Hadi** and F. H. Fard. 2022. On the Potential of Domain-Specific Pre-training of Contextual and Non-Contextual Word Embeddings: A Study on App-Review Analysis. Submitted to SANER 2022.
- K.G. Luong, **M. A. Hadi**, F. Thung, F. H. Fard, and D. Lo. 2021. FACOS: Finding API Relevant Contents on Stack Overflow with Semantic and Syntactic Analysis. Submitted to SANER 2022.
- **M. A. Hadi** and F. H. Fard. 2021. Evaluating Pre-Trained Models for User Feedback Analysis in Software Engineering: A Study on Classification of App-Reviews. arXiv preprint arXiv:2104.05861. 2021.
- **M. A. Hadi** and F. H. Fard. 2020. AOBTM: Adaptive Online Biterm Topic Modeling Algorithm for Version Sensitive Short Texts Analysis. IEEE ICSME 2020.
- **M. A. Hadi** and F. H. Fard. 2020. ReviewViz: Assisting Developers Perform Empirical Study on Energy Consumption Related Reviews for Mobile Applications. ACM MOBILESoft 2020.
- **M. A. Hadi** and F. H. Fard. 2020. Geo-Spatial Data Visualization and Critical Metrics Predictions for Canadian Elections. IEEE CCECE, 2020.

RESEARCH PROJECTS (1/2)

- **DeepHarvest**: This tool collects and links pieces of information about APIs in different libraries from diverse online resources, such as GitHub, Twitter, Stack Overflow, Stack Exchange, Jira Issue Comments, etc.
  [SOAR, SMU 2021]
- **DeepRecommend**: Outputs API sequences that are most relevant and positively rated for a functionality query expressed in mixed natural language and source code based on data curated by DeepHarvest.
  [SOAR, SMU 2021]
- **Study on the Frontline Fighters against COVID in Bangladesh**: This study aims to understand the stress experienced by the frontline doctors at the COVID-19 specialized hospitals. We examine the stark difference between health care practices, environments, and policies between developed and underdeveloped countries. We thoroughly investigated several unexplored aspects of underdeveloped countries' healthcare ecosystems to help the community shape more sustainable policies.
  [Continuous Project - NSU 2021]
- **High-throughput linguistic content comparison and sentiment analysis**: Assessed different architectures and current solutions; we finally combined multiple inputs (e.g., lexical features) to enhance the existing models for online adaptive syntactic plagiarism detection.
  [Scrawlr Inc., BC 2021]
- **Evaluating Pre-Trained Models for User Feedback Analysis in Software Engineering**: A Study on Classification of App-Reviews.
  [FardLab, UBC 2021]
- **AOBTM**: Adaptive Online Biterm Topic Modeling Algorithm for Version Sensitive Short Texts Analysis.
  [FardLab, UBC 2020]
- **Data Visualization and Analysis for Archaeological Records:** Analysis of Attribute-to-Attribute co-occurrence patterns in the OpenContext archive on Digital Index of North American Archaeology (DINAA).
  [FardLab, UBC and Dept. of Archeology, UBC – 2020]
- **Data Analysis, Modeling and Optimisation of woven composite hydraulic tubes**, to reduce in-service defects and failures - Phase II (Interactive analytical tool for customizable NN architectures and ML Models.)
  [Niedner Inc., FardLab, UBC, and MMRI, UBC – 2020]
- **ARISE**: Artificial Intelligence in production planning and management; Implemented a simple proof-of-concept Transfer Learning approach for Josef Schulte.
  [Universität Paderborn, DE, Josef Schulte, DE, Fardlab, UBC, and MMRI, UBC – 2020]
- **ReviewViz**: Assisting Developers Perform Empirical Study on Energy Consumption Related Reviews for Mobile Applications. This tool automatically collects and labels energy related reviews from Google Play.
  [FardLab, UBC – 2020]

RESEARCH PROJECTS (2/2)

- **Geo-Spatial Data Visualization** and Critical Metrics Predictions for Elections: Successfully predicted the outcome of 10/13 provincial elections from 2018 to 2020.
  [FardLab, UBC – 2020]

- **Visualization tool that illustrates the propagation of spurious hadiths among narrators**: The tool also tags the propagation points with some recorded events (e.g., wars, personal/clan dispute). We studied user reflection on Hadiths (quotes from Prophet Muhammad (PBUH)) after their exposure to our visualization tool. We suspected that these tagged events could have provoked aberrant dissemination of particular quotes, making them the most popular and referenced throughout history.
  [MIT and NSU – 2019]

- **A web application that proposes varying consultation fees for doctors in their private practices:** The web-based tool depends on several parameters (e.g., severity and ubiquity of the diagnosed disease, the effort put into detecting the disease, patients' perceptions on doctors' behavior). We used fuzzy logic classification and Linear Discriminant Analysis as the parameters were non-conforming throughout the entire user population.
  [NSU and EU – 2019]

- **A Quantitative Study to Understand the Impact of Smartphone Apps Usage on Students' Academic Results** in the Context of Bangladesh: The study showed negative correlation between high social media application usage and satisfactory above average academic results.
  [EU- 2019]

- **A pet like robot for blind people with autonomous navigation** implementing Simultaneous Localization and Mapping (SLAM) algorithms. For unstructured environment mapping, an XBOX-360 Kinect was used along with a 3D-Depth Camera; for localization, a Neato XV-11 LIDAR was used. The whole system was based on Linux Operating System. This project was highly acclaimed in NSU Capstone 2018.
  [NSU 2018]

- **Web Application for immigrant donor outreach** to help poor students in the underdeveloped countries. It also includes a decentralized fuzzy auction system to serve funds.
  [NSU 2018]

- **A warehouse management system** and a web-portal for Teachers' Association of Chittagong City Corporation, Bangladesh. This was part of a project funded by Ministry of Education, Govt. of Bangladesh.
  [CCC 2017]

- **An efficient course advising system** for North South University implementing a Bidding Approach coupled with Gale-Shapley Student Deferred Acceptance algorithm.
  [NSU 2017]

- **An Aeroplane turbulence detection device** capable of measuring simultaneous Passengers' heartbeat using the "Inertial Measurement Unit" to predict stressful conditions.
  [NSU 2016]

- **A low-cost Braille device** with Arduino micro-controller with a voice synthesizer for word pronunciation.
  [NSU 2016]

- **4-Bit ALU with 16 operations** with an implementation within the micro-programmed basic computer.
  [NSU 2016]

REFERENCES

Huang (Benny) Shengqiang
Senior Principal Engineer
Embedded Software Development Team
Data and Privacy Protection
Technology Lab
Huawei Technologies Canada Co., Ltd.
4321 Still Creek Dr., BC V5C 6S7, Canada
Phone: (+1) 604.618.0423
Email: huang.shengqiang@huawei.com

Dr. Abbas Milani
Professor
(Postdoctoral, MIT;
Ph.D., University of McGill)
Mechanical Engineering
The University of British Columbia
Office: EME 4203
Phone: (+1) 250.807.9652
Email: abbas.milani@ubc.ca

Dr. David Lo
Professor
(B.Eng., NTU; Ph.D., NUS)
School of Information Systems
Singapore Management University
Office: 80 Stamford Road,
Singapore 178902
Phone: (+65) 68280599
Email: davidlo@smu.edu.sg