Harshit Kumar

School of Electrical and Computer Engineering
Georgia Institute of Technology, Atlanta, USA

www.kumarharshit.com
hkumar64@gatech.edu
+1-470-685-5060

Education

Year	Degree/Examination	Institute	CGPA
2019 - 2024	Ph.D., Electrical & Computer Engineering	Georgia Tech	4.0/4.0
2014 - 2019	B.S. & M.S. Dual Degree, Electronics and Electrical Communication	IIT Kharagpur	9.04/10.0

Selected Work Experience/Internships

Graduate Research Assistant Aug 2019 - present
Georgia Institute of Technology, Atlanta, Georgia
Supervisor: Prof Saibal Mukhopadhyay

- *Hybrid Learning for Mission-Focused Artificial Intelligence* (Sponsor: Office of Naval Research)
  - Studied the impact of stochasticity on DNNs modeling discrete dynamical systems, like forest-fire evolution, **identifying and resolving DNN evaluation pipeline failures** [1].
  - Developed an attention-based **DNN architecture** for **data-efficient** and **scalable** prediction of Locally Interacting Discrete Dynamical Systems (applications in forest-fire, epidemic spread, and rumor propagation)[2].
- *Robust and Trustworthy Hardware-based Malware Detector (HMD)* (Sponsor: Semiconductor Research Corporation)
  - Designed a novel **statistical classifier** that corrects the noisy supervision signals from mis-labelled malware, resulting in a 6-7% decrease in false positive rates compared to existing methodologies [3].
  - Conducted a **robustness analysis of ML models** using an ensemble-based **uncertainty estimator** (with HMD applications), pre-emptively identifying failure points in **handling noisy and unseen samples** [4].
  - Designed **multi-OS multi-platform experiments** (creating custom malware sandboxes) for automated large-scale collection of data and custom dataloaders to train ML models for HMDs (I have done data). The trained model increases detection performance of current HMDs by 30-40% [5].

Research Scientist Intern May 2023 - Aug 2023
Whiterabbit.ai
Project: Breast Cancer Detection in 3-D Tomography Data, *Supervisor:* Thomas Matthews

- Designed a novel Transformer architecture-based DNN, utilizing temporal attention, for accurate detection of breast cancer anomalies in high-dimensional 3-D tomography data, resulting in significant reduction of false positives.
- Improved Classification AUC by 8% and Average Precision by 45%, compared to naive 2-D model extensions.

Security Researcher Intern May 2021 - Aug 2021
Red Team, Security Assurance Research, Client Computing Group, Intel
Project: Ransomware Detection, *Supervisor:* Chirag Shah

- Built a custom malware-analysis sandbox for large-scale data collection of hardware telemetry from sub-devices of a System on Chip (SoC). Telemetry is used to train the ML agent of the Ransomware detector.

Undergraduate Research Intern May 2018 - July 2018
New York University
Project: Security Analysis of RSFQ circuits, *Supervisor:* Prof. Ramesh Karri & Prof. Kanad Basu

- Performed formal security analysis of RSFQ circuits (used in quantum computers) for preventing IP-Piracy [6].
- Proposed first-of-its-kind attack and defense technique to protect the hardware Intellectual Property (IP).

Other Research Experiences

EDA Tools for Hardware IP Protection using Logic Encryption (Master's thesis) Sept 17 - April 18
Supervisor: Prof Santanu Chattopadhyay, IIT Kharagpur

- Developed satisfiability-guided encryption enhancements for synthesized netlists, to prevent the stealing of Design IP from adversaries in the semiconductor supply-chain [7],[14]. (Sponsor: Synopsys)
- Performed formal security analysis demonstrating the defense's resilience against powerful satisfiability attacks.

Data Acquisition System Oct 15 - July 16
Team KART, Formula SAE Team, IIT Kharagpur

- Developed a cost-effective Data Acquisition System (DAS) for a Formula Student race car, offering storage, wireless transmission, and real-time display at only 5% of commercial costs.

Selected Term Projects

Circuit Partitioning Using Graph Neural Networks JAN 2020 - APRIL 2020

Prof. Sung-Kyu Lim, Georgia Institute of Technology

- Implemented a Graph Convolutional Network based approach to solve the problem of graph partitioning, with applications in Electronic Design Automation (EDA).

Computer Architecture JAN 2020 - APRIL 2020

Prof. Thomas Conte, Georgia Institute of Technology

- Implemented a superscalar pipelined multi-core processor in C/C++ (with out-of-order and speculative execution), and a multi-core cache-coherence simulator.

Reverse Engineering of Malware JAN 2021 - APRIL 2021

Prof. Brendan Saltaformaggio, Georgia Institute of Technology

- Reverse engineered real-world malware using reverse engineering tools. Gained experience in anti-debugging, anti-VM, anti-disassembly, polymorphic, and obfuscation techniques used by the malware authors.

Technical Skills

- **ML/AI Concepts**: Neural Network Architectures (CNN, RNN, LSTM, GAN, Transformers), Computer Vision (Object Detection), Training and Evaluation (sequence-to-sequence similar to LLMs), classical ML, statistics
- **Programming Languages**: Python (PyTorch, Sklearn), C, C++, Powershell, MATLAB
- **Tools** : Git, LaTex, Linux, Slurm, MLflow, ASIC design flow (RTL design, Design Compiler, IC Compiler), NetLogo
- **Applications**: multi-variate time-series (malware detection), spatio-temporal data (forest-fire)

Positions of Responsibility

Graduate Student Mentor May 2022 - July 2022

Intel SURE Program, Georgia Institute of Technology

- Mentor in the SURE program (Intel-Georgia Tech collaboration), a summer research program designed to attract qualified under-represented minority students into graduate school (in the field of cyber-security).

Head of Electronics Subsystem May 2016 - May 2017

Team KART, Formula SAE Team of IIT Kharagpur

- Led a team of six students in developing numerous constituents of the electronic subsystem in a formula student car, e.g., data acquisition system and wiring harness.

Academic Honors and Awards

- Finalist in Qualcomm Innovation Fellowship India, 2019.
- Fellowship from Indian Academy of Sciences, Bengaluru, during the summers of 2017.

Relevant Coursework

Mathematical Foundations of ML, Deep Learning, Dynamical Systems, Linear Algebra, Probability and Random Process, Reverse Engineering of Malware, Advanced Computer Architecture, Advanced VLSI Design, Advanced Operating Systems, Signals and Systems, Estimation and Detection Theory, Digital Communications, Technology Entrepreneurship

Publications [Google Scholar]

Selected Publications:

1. "Studying the Impact of Stochasticity on the Evaluation of Deep Neural Networks for Forest-Fire Prediction", **Harshit Kumar** et al., *[under review at KDD 2024].*
2. "Learning Locally Interacting Discrete Dynamical Systems: Towards Data-Efficient and Scalable Prediction", Beomseok Kang, **Harshit Kumar** et al., *Learning for Dynamics and Control Conference, 2024.*
3. "RT-HMD: A novel Statistical Approach for Robust Real-Time Hardware-based Malware Detection under Weak Supervision formulation", **Harshit Kumar** et al., *[under review at ACM/IEEE ISLPED 2024].*
4. "Towards Improving the Trustworthiness of Hardware based Malware Detector using Online Uncertainty Estimation" **Harshit Kumar** et al., *ACM DAC 2021.*
5. "XMD: An Expansive Hardware-telemetry based Malware Detector to enhance Endpoint Detection", **Harshit Kumar** et al., *IEEE Transactions on Information Forensics and Security, 2023*
6. "Towards Increasing the Difficulty of Reverse Engineering of RSFQ Circuits" **Harshit Kumar** et al., *IEEE Transactions on Applied Superconductivity, 2019.*
7. "Efficient Key-gate Placement And Dynamic Scan Obfuscation Towards Robust Logic Encryption" Rajit Karmakar, **Harshit Kumar**, Santanu Chattopadhyay. *IEEE Transactions on Emerging Topics in Computing, 2019.*

Other Publications:

8. "Sparse Spiking Neural Network: Exploiting Heterogeneity in Timescales for Pruning Recurrent SNN", Biswadeep Chakraborty, Beomseok Kang, **Harshit Kumar**, and Saibal Mukhopadhyay, *ICLR 2024 poster*.
9. "Tackling Oversmoothing in Large Dense Graphs Using Hebbian-based Attention", Biswadeep Chakraborty, **Harshit Kumar** et al., *[under review at UAI 2024]*.
10. "Structured Latent Space for Lightweight Prediction in Locally Interacting Discrete Dynamical Systems" Beomseok Kang, Minah Lee, **Harshit Kumar**, and Saibal Mukhopadhyay, *IJCNN 2024*.
11. "Unsupervised Hebbian Learning on Point Sets in StarCraft II" Beomseok Kang, **Harshit Kumar** et al., *IJCNN 2022*.
12. "Machine Learning in Wavelet Domain for Electromagnetic Emission Based Malware Analysis" Nikhil Chawla, **Harshit Kumar**, and Saibal Mukhopadhyay. *IEEE Transactions on Information Forensics and Security, 2021*.
13. "BiasP: a DVFS based exploit to undermine resource allocation fairness in Linux Platforms" **Harshit Kumar** et al., *ACM/IEEE ISLPED 2020*.
14. "Securing IoT Devices using Dynamic Power Management: Machine Learning Approach" Nikhil Chawla, Arvind Singh, **Harshit Kumar**, Monodeep Kar, and Saibal Mukhopadhyay. *IEEE Internet of Things Journal, 2020*.
15. "On Finding Suitable Key-Gate Locations in Logic Encryption" Rajit Karmakar, **Harshit Kumar**, Santanu Chattopadhyay. *International Symposium on Circuits and Systems (ISCAS)-2018* .