Emil Biju

emilbiju@stanford.edu | emilbiju.github.io | emilbiju | emilbiju

Education

Stanford University *2023–2025*
M.S. in Electrical Engineering, Focus Area: Machine Learning/AI California, USA
- Coursework focused on machine learning, deep learning, NLP, and signal processing.
- Research in interpretable machine learning and applications to deep learning and LLMs.

Indian Institute of Technology Madras (IIT Madras) *2017–2021*
B.Tech (Honours) in Electrical Engineering (**CGPA: 9.70/10**), Minor in Deep Learning Chennai, India
- Graduated as the department's **second topper** out of 53 students.
- Received the top grade (S) in all courses from the Computer Science, Mathematics, and Humanities departments.
- B.Tech Thesis: Sample-specific Attention Masks for Model Transparency and Adversarial Detection

Publications in machine learning & algorithms

1. **Input-specific Attention Subnetworks for Adversarial Detection** [Paper]
   Emil Biju, A. Sriram, P. Kumar, M. Khapra; ACL 2022 (Findings), Dublin, Ireland
2. **Joint Transformer/RNN Architecture for Gesture Typing in Indic Languages** [Paper]
   Emil Biju, A. Sriram, M. Khapra, P. Kumar; COLING 2020, Barcelona, Spain
3. **Perturbation Analysis of Practical Algorithms for the Maximum Scatter TSP** [Paper]
   Emil Biju, S. Raman; ALENEX workshop @ SODA 2022, Virginia, U.S.A.
4. **Vocabulary-constrained Question Generation with Rare Word Masking & Dual Attention** [Paper]
   Emil Biju; 🏆 Best Paper Honorable Mention; ACM CODS-COMAD 2021, Hyderabad, India

Professional Experience

Microsoft R&D *2021–2023*
Data & Applied Scientist (Full-time, **2 years**) Bangalore, India
- Worked on ML research for cybersecurity applications, focusing on OAuth cloud app security.
- Developed industry-first machine learning solutions using knowledge graphs, anomaly detection, computer vision, and NLP to model cyber attack patterns, track app behavior, and avert security threats.
- Deployed & maintained models that process terabytes of data every day meeting stringent goals on latency and efficacy.
- **Filed a patent**, published a **paper** at MLADS 2022 & received an **early promotion** for exceptional work.

Microsoft R&D *May–July 2020*
Data & Applied Scientist Intern Hyderabad, India
- Developed CNN and Transformer-based deep learning models to analyze multi-spectral satellite images for estimating biomass in agricultural fields and identifying prospective areas for oil exploration.
- Designed a data structure for the open-source package, `xarray` to support tree-based hierarchical data storage.

GE Healthcare R&D *May–July 2019*
Data Scientist Intern Bangalore, India
- Used graph-based keyword clustering and topic ranking to analyze text in service records of healthcare machines.
- Set up an automated pipeline to flag common failure patterns and suggest quality improvement opportunities.
- Reduced the time taken to extract insights from service records by 11x and was appreciated by company leaders.

Scholastic Achievements

- **IIT Madras Silver Medal:** Awarded the Dr. Dilip Veeraraghavan Memorial Award by IIT Madras for featuring as the institute's second topper based on overall CGPA and cumulative performance in H category courses.
- **NTSE Scholarship:** Awarded by the Govt. of India based on a nationwide exam with 0.1% acceptance rate.
- **KVPY Fellowship:** Awarded by the Govt. of India based on a nationwide exam and interview with 2.5% acceptance rate to identify students with scientific research potential.
- **Samsung-IITM Pravartak Fellowship:** Awarded for research work on interpretability of Transformer models.
- **Best Paper Honorable Mention:** Awarded for my publication at ACM CODS-COMAD 2021.
- **GRE**: 333/340 (Quant:170, Verbal: 163, AWA: 5); **TOEFL**: 117/120 (R: 30, W: 30, S: 30, L: 27)

Research Projects

Adversarial Detection in Transformer Models using Attention Subnetworks *Jan–Nov 2021*

B.Tech thesis | Guide: Prof. Pratyush Kumar, IIT Madras *Paper* | *Webpage*

- Studied the self-attention framework in Transformers to improve their interpretability and robustness.
- Demonstrated that Transformers contain input-specific attention subnetworks that are interpretable and can be used to detect adversarial inputs.
- Improved the state-of-the-art accuracy in adversarial detection by 7.5% across 10 NLP tasks and 11 attack types.

IndicSwipe: Decoding Swipe Gesture Inputs to Indic Language Keyboards *Jan–July 2020*

Undergraduate research | Guide: Prof. Mitesh Khapra, IIT Madras *Paper* | *Webpage*

- Curated a training dataset of swipe gestures for 300k words in 7 Indic languages by using the brain's motor control principle of jerk minimization to simulate swipe inputs to a smartphone keyboard.
- Developed a Transformer-LSTM model for accurate swipe decoding and an ELMo-inspired word embedding model for fast/parallelized spelling correction. Achieved state-of-the-art accuracies of 70-95% across 7 languages.

Approximation Algorithms for the Maximum Scatter TSP *Jan–Aug 2021*

Undergraduate research, IIT Madras *Paper* | *Webpage*

- Devised 6 discrete approximation algorithms for the NP-hard maximum scatter traveling salesman problem.
- Performed smoothed analysis with various perturbations and edge-cost metrics to benchmark the stability, speed and accuracy of these algorithms. Demonstrated their practical utility using real-world datasets.

Risk propagation in Knowledge Graphs for detecting Cyberattack Campaigns *Sept–Nov 2022*

Cybersecurity research team, Microsoft | Lead contributor ***Patent filed***

- Built a knowledge graph representing OAuth cloud apps and their metadata properties, developed an algorithm to propagate risk scores between nodes, and used k-connectedness to detect dense campaign clusters.
- Uncovered 4 real-world cyberattack campaigns involving over 2,000 malicious apps that have now been disabled.

App Governance Copilot using GPT-3 *May–July 2023*

Cybsersecurity research team, Microsoft | Lead contributor

- Developed a GPT-3 based assistant specialized in cybersecurity for assisting SOC analysts in investigation, hunting and remediation of security threats from malicious OAuth cloud applications.
- Demonstrated how LLMs can be extended to domain-specific API's and services through few-shot prompting for seamless interaction.

Relevant Coursework

Computer Science: Introduction to programming, Data Structures and Algorithms, Topics in Design and Analysis of Algorithms, Introduction to Automata, Languages and Computation

Machine Learning: Introduction to Machine Learning, Deep Learning, Natural Language Processing, Advanced Topics in Signal Processing (Computer Vision/image processing), Data Mining

Mathematics: Linear Algebra, Probability Foundations, Graph Theory, Series & Matrices, Differential Geometry

Electrical: Computer Organization, Digital Signal Processing, Information Theory, Microprocessors, Digital Systems, Analog systems, Circuits & networks, Internet of Things, Electromagnetics, Electrical Machines, Solid State Devices

Technical Skills

Programming Languages: Python, C, C++, PySpark, SQL, ARM, Verilog
Libraries: TensorFlow, Keras, OpenCV, Numpy, NLTK, Matplotlib, Scikit-learn, and other ML libraries
Interests: Machine learning, Deep learning, NLP, Signal processing, Discrete algorithms

Leadership Roles & Extra-curricular activities

Founder, Passion JEE: Created a blog to mentor engineering aspirants in India & clocked over 6k views to date.

Learning champ, Microsoft: Curated learning material for new employees and organized learning sessions for 1000+ employees in the cybersecurity team.

Academic Service: Served as a paper reviewer for the MLADS 2021 conference and a mentor for college freshers.

Coordinator, Extra Mural Lectures: Invited top speakers and organized the flagship guest lecture series of IITM.

School Head Boy: Popularly elected by the school community and headed the students' council in my 10th grade.

Public Speaker: Featured as the lead emcee/speaker at several prominent events in college and at work.