AKASH VARTAK

akashvartak@umbc.edu | akashvartak.1995@gmail.com | +1(443)941-5919
https://github.com/akash-vartak | https://akash-vartak.github.io/ | https://www.linkedin.com/in/akash-vartak/

SUMMARY

My broad areas of interest are Artificial Intelligence & Machine Learning targeting towards the use of **Graph Neural Networks for applications in Computer Vision**. Currently, I am a **PhD Student and Research Assistant at University of Maryland Baltimore County**. My current PhD research is focused on detection and classification of trojaned DNN models found in the wild. In the past, my Masters research focused on improving classification of everyday man-made objects using the text found on these objects.

EDUCATION

PhD, Computer Science *Expected: May 2027*
University of Maryland Baltimore County, MD
GPA - 3.89/4
Areas: Computer Vision, Deep Learning
Advisor: Dr. Tim Oates
Research Lab: Cognition, Robotics and Learning Lab (CORAL Lab)

Master of Science, Computer Science *May 2022*
University of Maryland Baltimore County, MD
GPA - 3.86/4
Coursework: Algorithms, Data Science, Machine Learning, Cryptography, Distributed Systems
Thesis: Using Text to Improve Classification of Man-Made Objects
Advisor: Dr. Tim Oates
Research Lab: Cognition, Robotics and Learning Lab (CORAL Lab)
Committee: Dr. Tim Finin, Dr. David Chapman

Bachelor of Engineering, Computer Engineering *May 2017*
Pune Institute of Computer Technology, SPPU, India
GPA - 3.4/4
Coursework: Data Structures, Object Oriented Programming, Operating Systems, Artificial Intelligence

SKILLS

- **Languages:** Python, JAVA.
- **Machine Learning/Data Science:** PyTorch, PyTorch-Geometric, NetworkX, Scikit-learn, Pandas, NumPy, Matplotlib, Seaborn, BeautifulSoup, pyttsx, Shell Scripting.
- **Other Tools and Technologies:** Git, LaTeX, MS Office (Word, Excel, PowerPoint).
- **Platforms:** Linux, Windows.

EXPERIENCE

Research Assistant *August 2021 – Ongoing*
University of Maryland Baltimore County, MD

- Researching the application of Graph Neural Networks to identify trojaned DNN models.
- Surveying the possibility of 'unlearning' in Large Language Models.

Software Analyst *July 2017 – July 2019*
Yardi Software India Private Limited, Pune, India

- Designed and developed a complete 3-tiered J2EE based MVC web application that communicated with a large-scale relational database.
- Identified and mitigated application security issues which was verified by third-party security testing team.
- Optimized invoice batch processing times from 2 weeks to 1 hour, by implementing a smart, scalable scheduling algorithm.
- Conceptualized and developed a complete end-to-end in-application chat feature.

Project Intern *August 2016 – March 2017*
E2open, Pune, India

- Predicted best price of an item for a given store to maximize sales by engineering a sales forecasting and price optimization machine learning algorithm.
- Worked with a vast repository of store-item combinations and item sales features like weather, demographics, survey feedbacks, sale trends and sale seasonality.

RESEARCH & PUBLICATIONS

Publications

[1] **Paper: Detecting Backdoors Using Graph Convolution Networks** *July 2025*

- Accepted for presentation at **International Joint Conference of Neural Networks (IJCNN) 2025** in Rome, Italy.
- Developed a graph convolutional network to detect backdoored CNN models in-the-wild.
- Proved that GCNs can be used as model-agnostic meta-classifiers and that the model learns to establish and leverage relational information from the CNNs by treating the CNNs as graphs.
- First of its kind: Representing DNNs and graphs and Capable of utilizing convolutional layers in addition to fully-connected layers.

[2] **Thesis: Using Text to Improve Classification of Man-Made Objects** *March 2021*

- Designed a multi-modal model that learns to associate objects in images with a linguistic concept purely through visual percepts.
- The model learns to reason about an object in context of the text found on the object itself and showed that text is a very useful signal when trying to classify and understand objects.

[3] **Paper: A Survey on Promotional and Base Level Forecasting using ARIMA**

- Research paper on Promotional and Base Level Forecasting and the use and application of ARIMA on Time Series data.

Research

[1] **Semantically Coherent Adversarial Attacks on Computer Vision Models** *January 2025 – Ongoing*

- Developing approaches for semantically coherent adversarial attacks on machine vision, creating human-observable, natural scene elements that cause model errors.
- Implemented gradient tying mechanisms to coordinate pixel manipulation, ensuring synthesized objects specifically contribute to classifier misclassification.
- Exploring methods to embed objects naturally within images, addressing challenges of placement and visual realism in adversarial attacks.

[2] **Detection of Trojaned Deep Networks** *August 2022 – Ongoing*

- Developed a Graph Convolution Network based framework to detect trojaned deep learning models in-the-wild; A very fast and novel approach.
- Proved that GCNs can be used as model-agnostic meta-classifiers that learn to establish and leverage relational information from the DNNs by treating them as graphs.
- Pioneering approach that classifies DNN models using solely the static weights, without need of original DNN training data irrespective of DNN's domain.
- Actively being evaluated on MLPs, CNNs, and Reinforcement Learning models.

Talks and Awards

[1] **Poster: Detecting Backdoors Using Graph Convolution Networks** *October 2024*

- Poster presentation to members of NASA EDT at UMBC.

[2] **Invited Talk: Detecting Trojaned Models using GCNs** *August 2024*

- Presented an deep dive of my research at University of California San Diego to members of UCSD, iARPA and NIST.

[3] **Poster and Talk: Backdoor Detection using Graph Convolutional Networks** *May 2024*

- Best Poster Award at CSEE Research Day 2024.

PEER-REVIEWING EXPERIENCE

[1] ACM Transactions on Computing for Healthcare (ACM HEALTH) 2024

[2] Association for the Advancement of Artificial Intelligence (AAAI) 2024, 2025

[3] Conference on Neural Information Processing Systems (NeurIPS) 2023

[4] International Conference on Data Mining (ICDM) 2022, 2023

[5] Workshop on Knowledge-Infused Learning (KiL) at ACM International Conference on Knowledge Discovery and Data Mining (KDD) 2024

[6] International Conference on Learning Representations (ICLR) 2025

[7] International Joint Conference on Neural Networks (IJCNN) 2025

[8] Workshop on Data in Generative Models (The Bad, the Ugly, and the Greats) at International Conference on Machine Learning (ICML) 2025

PROJECTS

Multi-Artist Recommendation System (MARS) *October 2019 – December 2019*

- Recommendation system using a Naive Bayes machine learning model, to recommend a list of artists based on the song's lyrics, genre, mood, and artist meta-data like the artist's number of hits.

Price Optimization and Elasticity *August 2016 – March 2017*

- Prediction of optimal price-discount strategy for multiple store item combination for multiple items and categories.
- Achieved a low error rate of only 8-10% by using an ensemble of regression models and analysis of past retail sales and vast demographic survey data of multiple store−item combinations.

Wordy (https://github.com/akash-vartak/Wordy) *January 2016*

- A personal vocabulary trainer that displays a word and its meaning as a notification and can also provide pronunciation.

ACADEMIC POSITIONS

Historian/Secretary *June 2021 - July 2022, June 2023 - July 2024*
UMBC Graduate Students Association (GSA)

- Compiled meeting minutes of weekly and monthly Senate and Executive Council meetings.
- Regularly updated the GSA website by way of uploading all meeting minutes and making them available to the whole graduate school, and publishing Executive Council, Senator, and other member bios and contact information on GSA website.
- Cataloged a well-maintained list of student and faculty resources, mental health resources, and information on various research and professional development grants.
- Designed graphics for posters, fliers and website using Canva.

Teaching Assistant *August 2020 – May 2021*
UMBC Dept. of Computer Science and Electrical Engg.

- Delivered comprehensive support to students by addressing questions and queries.
- Evaluated student projects, assignments, homework, quizzes, and other assessments.
- Aided the teaching faculty in preparing the course structure when required.

UNDERGRADUATE ACTIVITIES

Event Head *June 2015 - May 2017*
PICT ACM Student Chapter

- Responsible of organizing technical events under the ACM Student Chapter umbrella in the university.
- Spearheaded the revitalization of the annual flagship event 'Pulzion' and helped achieved a year-on-year two-times increase in attendance by students, faculty and guest speakers from all over the country.