


Agnideven Palanisamy Sundar

Brooklyn, NY 11237

+1 (317) 869 2212 | agnideven@gmail.com | agnideven.github.io | linkedin.com/in/agnideven-sundar | 

<https://scholar.google.com/citations?user=whNrL10AAAAJhl=en>

Machine learning specialist with a Ph.D. in Computer Science, passionate about leveraging advanced ML techniques to drive innovation and solve complex data-driven challenges in AI and data science..

Skills

Machine Learning	LLMs, Tensorflow, PyTorch, Keras, Pandas, NumPy, Predictive Analysis, Matplotlib, Data Mining, NLTK
Programming and OS	Python, C, Java, C++, Bash Scripting, CUDA, GoLang, Linux(Ubuntu[ML] & RedHat[Crypto])
Graph & Web Scraping	Neo4J, NetworkX, PyTorch Geometric (PyG), DGL (Deep Graph Library), BeautifulSoup, Selenium, Scrapy
Soft Skills	Analytical-thinking, Attention to Detail, Communication, Teamwork, Adaptability, Time-management

Work Experience

Research Engineer Intern, Samsung Research America [Knox Solutions Innovation]

May 2024 - Aug 2024

- Engineered a sophisticated Synthetic Data Generation algorithm utilizing LLMs to produce Android System Logs, enhancing anomaly detection capabilities on mobile devices.
- Contributed to an innovative anomaly detection initiative on mobile devices, leveraging machine learning models and statistical approaches to help businesses identify and mitigate unusual and potentially malicious user behavior.

Research Assistant, Computer and Information Science, IUPUI

Jan 2019 - May 2024

- Scraped thousands of restaurant reviews from TripAdvisor to build a Neo4J graph-based restaurant recommendation system, enhancing recommendation accuracy.
- Collected and analyzed all AARP posts and reviews up to 2019 for a Kelly School of Business NLP project, driving insights through advanced text analysis.
- Engineered versatile, model-agnostic security methodologies, ensuring adaptability across diverse ML models, and contributed to multiple research papers focused on enhancing ML system security.
- Developed innovative algorithms inspired by real-world applications to enhance ML system robustness against security threats.
- Acted as a **peer reviewer for numerous high-impact journal papers**, ensuring rigorous academic standards and contributing to the advancement of research quality.

Teaching Instructor - Information Tech Architectures, Computer Information and Graphics

Jan 2023 - May 2023

Technology, IUPUI

- Delivered comprehensive lectures on theoretical and practical aspects of computing to freshmen, covering hardware, software, network architecture, and foundational security across various operating systems for a class of twenty-six undergrads.

Teaching Assistant, Computer and Information Technology, IUPUI

Jan 2020 - May 2024

- Recognized with the **Teaching Assistant Award** in April 2023 for exceptional skills in distilling complex concepts, like Cryptography, Systems Programming, and Big Data Analytics, both at Graduate and Undergraduate levels, into understandable formats.

Publications

Toward Multimodal Vertical Federated Learning: A Traffic Analysis Case Study.

July 2024

IEEE ICCCN

- Fused a text model with traffic data and an image model based on CCTV feeds to devise a comprehensive Traffic Intensity Predictor.
- Curated a pioneering Vertical Federated Learning Dataset, contributing a valuable resource for the research community.

The Cost of Privacy: A Comprehensive Analysis of the Security Issues in Federated Learning

Feb 2024

Chapter from Book "Network Security Empowered by Artificial Intelligence - Springer"

- Investigated the security vulnerabilities in Federated Learning, detailing how its decentralized nature exposes it to adversarial attacks.
- Outlined defense mechanisms to mitigate these vulnerabilities, focusing on the low-level impact of the attacks/defenses on the ML model.

GAN-inspired Defense Against Backdoor Attack on Federated Learning Systems

Sept 2023

IEEE MASS

- Formulated a resilient GAN-inspired (Generative Adversarial Network) defense mechanism for Federated Learning systems, effectively neutralizing diverse backdoor attacks.
- Secured **3rd place in the CERIAs Symposium '22** poster presentation, showcasing this impactful research.

Multi-Armed-Bandit-based Shilling Attack on Collaborative Filtering Recommender Systems

Dec 2020

IEEE MASS

- Reimagined the multi-armed bandit strategy to craft a sophisticated spam user, effectively manipulating recommender systems.
- Enabled targeted item recommendations to 40% of users with a minimal 10% attack size, demonstrating exceptional efficacy.

Please view Google Scholar for a complete list of 10+ other published research works

Jan 2020 - Present

Education

3.8/4.0 **PhD in Computer Science**, Purdue University - Indianapolis | Indiana, USA 2020-24

3.8/4.0 **MS in Computer and Information Science**, Indiana University Purdue University Indianapolis | Indiana, USA 2018-20

7.2/10 **BE in Electronics and Communication Engineering**, Anna University | Tamil Nadu, India 2011-15

Noteworthy Courses: Cryptography | Advanced Information Assurance | Big Data Analytics | Intelligent Systems | Operating Systems | Algorithm Design and Analysis.