Padmaksha Roy

padmaksha@vt.edu | Google Scholar

Research Interests

PhD candidate, ECE, Virginia Tech *Aug 2021 - Present*

- My research focuses on the interdisciplinary field of machine learning for anomaly/intrusion detection, out-of-distribution(OOD) generalization, uncertainty quantification, and designing robustness strategies against adversaries. My work spans applications in cybersecurity, IoT, cyber-physical systems, and time-series anomaly detection. I am also exploring how LLMs and in-context learning can be leveraged to improve zero-day anomaly detection. During my PhD, I have published in leading machine learning venues like *TMLR, ECML, PAKDD, ICDM(ML4Cyber)* and also in *IEEE Journals, AAAI Workshop, and ACM venues.*

Key Publications

A Multidirectional Meta-Learning Framework for Class-Generalizable Anomaly Detection

- In this paper, we address the problem of class-generalizable anomaly detection, where the objective is to develop a unified model by focusing our learning on the available normal data and a small amount of anomaly data(few shot) in order to detect the completely unseen anomalies. To achieve this, we propose a multidirectional meta-learning algorithm. At the inner level, the model aims to learn the manifold of normal data. At the outer level, the model is meta-tuned to maximize the margin between softmax confidence scores of normal and most confident anomaly samples, treating normals as in-distribution (ID) and anomalies as out-of-distribution (OOD). Paper published at **ICDM(ML4Cyber) 26'**. **[Link]**

Beyond Marginals: Learning Joint Spatio-Temporal Patterns for Multivariate Anomaly Detection

- In multivariate time-series data (such as cyber-physical systems), anomalies often emerge from joint deviations across interrelated variables, even when individual signals appear normal. Most existing methods assume conditional independence, which oversimplifies real-world interactions. Our approach explicitly models joint spatial (Copula modeling) and temporal (Transformer's self-attention) dependencies in the latent space while decoupling marginal distributions to detect multi-variate anomalies. Published at **TMLR 25' [Link]**

Improving Novel Anomaly Detection with Domain-Invariant Latent Representations

- Novel or zero-day anomalies are rare, evolving, and therefore difficult to detect. Meanwhile, different domains exhibit unique feature correlations, making it challenging to identify unseen domains. In this work, using multi-task learning and information regularization (principle of relevant information preservation), we show how to construct a latent space from known domains that is free of domain-specific bias yet generalizes well to unknown domains. Published at **ECML-PKDD 25' (Research)**. **[Link]**

Latent Space Correlation Aware Autoencoder for Anomaly Detection in Skewed Data

- In this work, we address some of the limitations of the Euclidean distance when used as a reconstruction error to detect anomalies (especially near anomalies) that have a similar distribution as the normal data in the feature space. We propose a latent dimension regularized autoencoder that leverages a robust form of the Mahalanobis distance (MD) to measure the latent space correlation to effectively detect near as well as far anomalies. Published at **PAKDD 24'** conference.**[Link]**

Defense against Joint Poisoning and Evasion Attacks: a Case Study of DERMS

- DERMS are vulnerable to intrusions that could potentially harm the real world. Model-based intrusion detection techniques are data-centric but an undetected attack on the data could lead to making wrong operational decisions for the system. In this paper, we propose a bi-level optimization problem to build a robust model to defend against simultaneous poisoning and evasion attacks in cyber-physical power systems. Using diverse poisoning and evasion attack scenarios, the proposed method performed better compared to the existing techniques. Paper published at **AAAI Workship- AI for Cybersecurity 24'**. **[Link]**.

Deep diffusion-based forecasting of COVID-19 by incorporating network-level mobility information with Graph Neural Networks and Mixture Density Networks

- Proposed an Auto-regressive Mixed Density Network on a county-level graph network by incorporating intra and inter-county mobility information to forecast covid deaths and infection. We found that adding the mobility information in the graph convolution network improves both forecasting and uncertainty quantification (confidence). Paper published in **IEEE/ACM ASONAM 21'**. **[Link]**

Surveys

A Survey of Data Security: Practices from Cybersecurity and Challenges of Machine Learning. **[Link]**.

Education

Virginia Polytechnic Institute and State University, ECE Washington D.C.
Doctor of Philosophy in Computer Engineering *August. 2021 – Present*

Virginia Polytechnic Institute and State University, ECE Washington D.C.
Master of Engineering in Computer Engineering with focus in Machine Learning, CGPA 3.66 *Aug. 2019 – May. 2021*

Programming Skills

Languages: Python, Pytorch, Shell Script, Flask, Pandas, Numpy, Scikit, Keras, SQL, AWS, EC2, S3, Sagemaker, Agentic AI -RAG, LangChain, LangGraph

Work Experience

Argonne National Lab (Math and Computer Science Division) Chicago, Illinois

Research Aide *June 2026 -August 2026*

- Research and Education Networks (RENs) like ESnet are the backbone of our distributed research infrastructure. We aim to develop fast models that can simulate an predict the activities of the networks, enabling rapid design space exploration and near real-time digital twins. This project will explore creating AI models of REN components, such as switches, and develop integrated network-level models of these components.

Virginia Tech Washington DC

Graduate Teaching Assistant *August 2020 -August 2021*

- ECE 5424/CS 5824 - Advanced Machine Learning, ECE 4424/CS 4824 Machine Learning

Accenture AI India

Senior Software Developer(Machine Learning) *2017 - 2018*

- Worked on various client projects and implemented statistical ML and DL algorithms in production systems. We developed a B2B marketing strategy with scalable and interpretative product recommendations using co-clustering and collaborative filtering. We used decision trees and ARM rules to provide interpretability to our product recommendation system.

Accenture Digital India

Software Developer *2015 - 2016*

- While working as a software engineer (data analytics) in a financial services domain, we developed microservices for various kinds of data extraction from cloud platforms. We built a similar product inspired from MS Vault that deployed many microservices for various independent works like storing all access and security-related information for our third parties on cloud using RestApi calls built on Flask architecture with end-to-end CI/CD pipelines. Previosuly, worked as an automation engineer (shell scripting and python) to automate deployments and environment health checks across platforms.

Coursework

Advanced Machine Learning, Deep Learning, Applied Machine Learning, Theory of Algorithms, R and D Methods for Engineers, Intro to Urban Computing, Data Analytics, Optimization Techniques, Intro to Deep Learning, Robust Estimation and Filtering, Signal Processing.

Extracurricular Activities

Innovation Campus Fellow: As an innovation campus fellow, my role was to collaborate with Virginia Tech leadership and offer input, share perspectives, act as advisors, and participate in events as the Innovation Campus plans move forward.