Dipkamal Bhusal

✉ db1702@rit.edu Google Scholar Github Webpage in LinkedIn

Summary

Extensive theoretical and practical background in machine learning with experience in quantitative and qualitative research, experiment design, and result analysis. Experience in launching and working in ML startups. .

Research Interests: Explainable Machine Learning, Adversarial Machine Learning, Computer Vision, ML in Healthcare, Natural Language Processing.

Education

Ph.D. 2021–Present
Rochester Institute of Technology, Rochester, NY, USA,
Concentration – Computing and Information Science
Advisor – Dr. Nidhi Rastogi .

M.Sc. 2019–2021
Tribhuvan University, Institute of Engineering, Pulchowk Campus Lalitpur, Nepal,
Concentration – Information and Communication Engineering
Advisor – Dr. Sanjeeb Prasad Panday.

B.E. 2012–2016
Tribhuvan University, Institute of Engineering, Pulchowk Campus Lalitpur, Nepal,
Electronics and Communication Engineering .

Publications

[1] **Dipkamal Bhusal**, Md Tanvirul Alam, Monish Kumar Manikya Veerabhadran, Michael Clifford, Sara Rampazzi and Nidhi Rastogi. "PASA: Attack Agnostic Unsupervised Adversarial Detection using Prediction & Attribution Sensitivity Analysis" at 9th IEEE European Symposium on Security and Privacy (2024)
[2] **Dipkamal Bhusal**, Rosalyn Shin, Ajay Ashok Shewale, Monish Kumar Manikya Veerabhadran, Michael Clifford, Sara Rampazzi and Nidhi Rastogi. "SoK: Modeling Explainability in Security Analytics for Interpretability, Trustworthiness, and Usability." at 18th International Conference on Availability, Reliability and Security (2023)
[3] Tanvirul Alam, **Dipkamal Bhusal**, Youngja Park, and Nidhi Rastogi, "Looking Beyond IoCs: Automatically Extracting Attack Patterns from CTI". 26th International Symposium on Research in Attacks, Intrusions and Defenses (2023)
[4] Md Tanvirul Alam, **Dipkamal Bhusal**, Youngja Park, Nidhi Rastogi, "CyNER: A Python Library for Cybersecurity Named Entity Recognition". on arXiv

Under Review
[1] **Dipkamal Bhusal**, Monish Kumar Manikya Veerabhadran, Michael Clifford, Sara Rampazzi and Nidhi Rastogi, "On the connection between model robustness and saliency map interpretability".
[2] **Dipkamal Bhusal**, Nidhi Rastogi, "Adversarial Patterns: Building Robust Android Malware Classifiers".
[3] **Dipkamal Bhusal**, Sanjeeb Prasad Panday, "Multi-Label Classification of Thoracic Diseases using Dense Convolutional Network on Chest Radiographs"

Poster & Presentation

Presentation
[1] Guest talk on "Understanding black box models: A review of explainable AI", RIT DataFest, March 24, 2023,
[2] Presented our paper "SoK: Modeling Explainability in Security Analytics for Interpretability, Trustworthiness, and Usability." at ARES'2023 held at Benevento, Italy, August 29 -September 1, 2023

Poster
[1] Poster presentation, "**Dipkamal Bhusal**, Nidhi Rastogi, Analyzing anomalous events using context and explainability", RIT AI Summit, October 24 2022.

Experience

August 2021–Present **Graduate Research Assistant**, *Rochester Institute of Technology*.

As a research assistant in the lab "AI for Security," I work at the intersection of machine learning and security. Primarily, my research focuses on developing reliable and actional explainable AI, but I have also been involved in projects involving knowledge graphs and adversarial machine learning. My research goals and activities can be enlisted in three major points: study of existing explanation methods in deep learning to understand their shortcomings in various applications, propose design changes to existing explanation methods to improve the reliability of explanations and propose a new framework that handles the shortcomings of existing methods and provides reliable and actionable explanations. My research goal is to improve post-hoc explanation methods for black box models by understanding the relationship between model robustness and attributional robustness to obtain concise, stable, and faithful explanations that can assist decision-making in various applications.

Dec 2016–June 2021 **Co-founder/Software Engineer**, *Paaila Technology*.

I co-founded an AI startup in December 2016 (Kathmandu) to work on robotics and AI projects. From December 2016 to November 2018, I worked as a developer and project manager for the manufacture of service robots, Pari, Pari 2.0, and Ginger. All of these robots were designed and manufactured in Nepal. I also contributed as a machine learning engineer for developing ML models for specific tasks of the robot like speech synthesis, and recognition. I took the position of Managing Director in December 2018, was involved in handling planning and managerial activities, and was responsible for the overall growth of the startup. I resigned in July 2021 to pursue PhD in the USA.

Sept 2020–Aug 2021 **Lecturer**, *IIMS College*.

As a lecturer in the Computer Science department, I taught two BSc. IT undergraduate courses: Introduction to Python and Machine Learning. In addition to teaching, I organized various data science camps and Python training sessions.

Skills

Languages	Python, C/C++
Frameworks	PyTorch, Keras, TensorFlow
Libraries	NumPy, Pandas, Scikit-learn, OpenCV, Matplotlib, BeautifulSoup, LIME, SHAP
Utilities	Jupyter Notebook, Visual Studio, Git, Latex

Graduate Courses

Quantitative Foundations, Deep Learning, Statistical Machine Learning, Foundation of Algorithms, Software Engineering, Neural Network, Image Processing, Big Data.

Selected Projects

2021 **Multi-label classification of thoracic diseases**, *Python*.

- Developed a concurrent multi-class detection of fourteen clinically important pathologies in chest radiographs
- Architecture: DenseNet
- Test case explanation of diagnosis model prediction using GRADCAM
- Explored variational auto-encoder as a representation learning model for extracting disentangled features of X-ray images

2019 **Brain tumor auto-segmentation for magnetic resonance imaging**, *Python*.

- Built a neural network to automatically segment tumor regions in the brain, using MRI scans and visualize the segmentation

2019 **Sentiment Analysis of Tweets using PySpark**, *PySpark, Python* .

- Implemented sentiment analysis on a dataset of 1.6 million tweets using the Spark Machine Learning library

2019 **Business assistant robot, Pari 2.0**, *Python, C++*.

- Designed and developed a business assistant robot for the State Bank of India, Nepal
- Developed face recognition for a robot for identifying registered faces of employees and facilitating registration of new faces

2018 **Automation at Naulo restaurant**, *Java, Python, C++*.

- Naulo restaurant is a fully automated robotics restaurant developed by our team at Paaila Technology.
- Contributed to the development of face recognition for waiter robots (Ginger) and the digital technology of the restaurant, including digital tables and applications for order and delivery of food

Honors and achievements

Scholarship Financial Support for Ph.D. in Computer Science at RIT, 2021-Present.

Training Conducted two-week training in Python and Data Science at IIMS College, Kathmandu, 2021.

Award National ICT Innovation Award by Ministry of Communication and Information Technology (Nepal Government) for Paaila Technology, 2019 .

Scholarship Full scholarship for Masters in Information Engineering at Pulchowk Campus, Tribhuvan University, 2019.

Contest Most Creative Business of Nepal by Antarprena. Represented Team Nepal at global finals in Copenhagen, Denmark, 2018.

Contest Winner of Object Oriented Programming Competition by FlipKarma at Pulchowk Campus, 2014.

Scholarship Full scholarship for bachelor in engineering at Pulchowk Campus, Tribhuvan University, 2012.

Scholarship Full Scholarship at Balkumari College, Chitwan (10+2 college equivalent to junior and senior high school level in US) + College Topper + First Position at final examinations in the whole district.

Selected Certifications

1. AI for Medical Treatment, Medical Diagnosis, and Medical Prognosis by deeplearning.ai on Coursera. Certificate earned at June, 2020.
2. Deep Learning Specialization by deeplearning.ai on Coursera. Certificate earned in June 2020. Courses include Neural Networks and Deep Learning, Improving Deep Neural Networks: Hyperparameter tuning, Regularization and Optimization, Structuring Machine Learning Projects, Convolutional Neural Networks and Sequence Models..
3. IBM Data Science Specialization by IBM on Coursera. Certificate earned in May 2020. Courses include: What is Data Science?, Tools for Data Science, Data Science Methodology, Python for Data Science and AI, Databases and SQL for Data Science, Data Analysis with Python, Data Visualization with Python, Machine Learning with Python and Applied Data Science Capstone..
4. Project Management Principles and Practices Specialization by University of California, Irvine-The Paul Merage School of Business on Coursera. Certificate earned at May 2020.
5. Mathematics for Machine Learning: Linear Algebra and Multivariate Calculus by Imperial College London on Coursera. Certificate earned at April 2020..