

# PRABIN B. LAMICHHANE

[prabin.lamichhane@mastercard.com](mailto:prabin.lamichhane@mastercard.com)

*I am a Senior Data Scientist at Mastercard with working experience in Network Security, Anomaly Detection, Machine Learning, Data Mining, Graph Mining, Graph Embedding, and Graph Visualization.*

## **EDUCATION:**

**Tennessee Tech University**

Ph.D. (Computer Science), GPA: 4/4

Cookeville, TN

Aug, 2018 – Sep, 2022

**Tennessee State University**

M.S. (Comp. and Info. Sys. Engineering), GPA: 4/4

Nashville, TN

Jan, 2016 – May, 2018

**Tribhuvan University**

B.E. (Electronics & Comp. Engineering), GPA: 3.72/4

Kathmandu, Nepal

Jan, 2011 – Jan, 2015

## **EXPERIENCES:**

**Mastercard**

Senior Data Scientist

O'Fallon, MO

09/26/2022 – Present

- *Currently working on Merchant Data Quality project under which analyzed the mastercard's internal data and developed A.I. models to improve data quality. Later, these improved data will be used in various crucial fields like rewards programs, fraud detection, etc.*
  - *Performed Initial Data Analysis on merchant data,*
  - *Prepared Data for the PoC and the MVP models,*
  - *Developed the Deduplication PoC and MVP models,*
  - *Validated and Evaluated the PoC and the MVP models, and*
  - *Deployed the MVP model on Production etc.*

**Tennessee Tech University**

Graduate Teaching and Research Assistant

Cookeville, TN

08/15/2018 – 09/26/2022

- *Worked on research related to anomaly/fraud detection in streaming (dynamic) networks, such as Denial-of-Service attacks (DoS) in computer networks, social network impersonations, fake recommendations in e-commerce networks, etc., using graph-based techniques like probabilistic, embedding, and sketching.*
- Assisted Courses: *Data Structures and Algorithms, Discrete Structures for CSC, Foundation of CSC, Database Management Systems*

**Tennessee Tech University**

Internship (Research Assistant)

Cookeville, TN

05/15/2018 – 08/15/2018

- *Formally analyzed the transmission scheduling process of the WirelessHART networks using Satisfiability Modulo Theories (SMT). That is, this research formally models the WirelessHART network configuration and various constraints (like the number of channels and flow deadline) as inputs and verifies the schedulability of the packets under certain success specifications.*

**Tennessee State University**

Graduate Research Assistant

Nashville, TN

01/10/2016 – 05/15/2018

- *Performed research on network security: finding a stepping stone path towards the node with the highest impact on the network (i.e., the node whose exploitation causes the most significant loss to the organization). So that defenders can mitigate network attack problems by either changing any of the paths towards the node or sifting the node to the place where it will be more secure.*

## **TECHNICAL SKILLS:**

**Language:** Python, C, C++, MATLAB/Octave, SQL, LaTeX.  
**Software** Scikit-learn, Numpy, Scipy, Pandas, Matplotlib, Seaborn, Weka, Git/Github, Jupyter  
**Tools:** Notebook, SQL Developer, Gephi, Tiger Graph, NPView, Nmap, Wireshark.  
**Data Skill:** Anomaly/Fraud Detection, Machine Learning, Data Mining, Data Visualization, Data Cleaning, Graph Mining, Graph Embedding.  
**Database:** MySQL, Oracle, SQL/Impala.

## **PUBLICATIONS:**

2024 **P. B. Lamichhane**, Jacob Taylor, W. Eberle, "Effectiveness of Term Frequency-Inverse Graph Frequency (TF-IGF) Technique Against Various Cyber Attacks"(accepted in CSCI'24, will publish on Dec, 2024).  
2022 **P. B. Lamichhane** and W. Eberle, "Self-Organizing Map-Based Graph Clustering and Visualization on Streaming Graphs," 2022 IEEE International Conference on Data Mining Workshops (ICDMW), Orlando, FL, USA, 2022, doi: [10.1109/ICDMW58026.2022.00097](https://doi.org/10.1109/ICDMW58026.2022.00097).  
2022 **P. B. Lamichhane**, H. Mannering, W. Eberle, "Discovering Breach Patterns on the Internet of Health Things: A Graph and Machine Learning Anomaly Analysis." The International FLAIRS Conference Proceedings. 35, (May 2022), doi: [10.32473/flairs.v35i.130628](https://doi.org/10.32473/flairs.v35i.130628).  
2022 R. Manicavasagam, **P. B. Lamichhane**, P. Kandel, D. Talbert, "Drug Repurposing for Rare Orphan Diseases using Machine Learning Techniques". The International FLAIRS Conference Proceedings. 35, (May 2022), doi: [10.32473/flairs.v35i.130653](https://doi.org/10.32473/flairs.v35i.130653).  
2021 **P. B. Lamichhane**, W. Eberle, "Anomaly Detection in Edge Streams Using Term Frequency-Inverse Graph Frequency (TF-IGF) Concept," 2021 IEEE International Conference on Big Data (Big Data) 2021. pp. 661-667, doi: [10.1109/BigData52589.2021.9671424](https://doi.org/10.1109/BigData52589.2021.9671424).  
2018 **P. B. Lamichhane**, L. Hong and S. Shetty, "A Quantitative Risk Analysis Model and Simulation of Enterprise Networks," 2018 IEEE 9th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON), 2018, pp. 844-850, doi: [10.1109/IEMCON.2018.8615080](https://doi.org/10.1109/IEMCON.2018.8615080).  
Under Review **P. B. Lamichhane**, W. Eberle, "Anomaly Detection in Graph Structured Data: A Survey" (On arxiv: <https://arxiv.org/abs/2405.06172>)

## **PRESENTATIONS:**

- **Research Paper Presentation**, 2018 IEEE 9th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON), University of British Columbia, Canada.
- **Research Presentation**, on "Anomaly Detection in Edge Streams Using Term Frequency-Inverse Graph Frequency (TF-IGF) Concept", at the Graduate Student Seminar, 2021.
- **Research Paper Presentation**, 2021 IEEE International Conference on Big Data (IEEE BigData 2021), Orlando, Florida, USA.

## **RESEARCH INTERESTS:**

- Graph-based Anomaly Detection
- Graph Embedding and Sketching
- Cyber Security Data Analysis
- Anomaly/ Fraud Detection
- Machine Learning & Artificial Intelligence
- Network Security

## **CERTIFICATIONS:**

- Machine Learning
- Applied Data Science with Python

Stanford University  
University of Michigan