PRABIN B. LAMICHHANE

pblamichha42@tntech.edu

I am a Ph.D. Candidate in Computer Science with five years of working experience in Network Security, Anomaly Detection, Machine Learning, Data Science, and Graph Mining. Currently, I am working on research related to anomaly/fraud detection in dynamic networks using graph-based techniques.

EDUCATION:

Tennessee Tech University   *Cookeville, TN*
Ph.D. (Computer Science)   *2018 – Present*
GPA: 4/4

Tennessee State University   *Nashville, TN*
M.S. (Computer and Information Sys. Engineering)   *2016 – 2018*
GPA: 4/4

Tribhuvan University   *Kathmandu, Nepal*
B.E. (Electronics & Computer Engineering)   *2011 – 2015*
GPA: 3.72/4

EXPERIENCES:

Tennessee Tech University   *Cookeville, TN*
Graduate Teaching and Research Assistant   *2018 – Present*

- *Currently working on research related to anomaly/fraud detection in streaming (dynamic) networks such as Denial-of-Service attacks (DoS) in computer networks, social networks impersonations, or fake recommendations in e-commerce networks, etc. using graph-based techniques like probabilistic, embedding, and sketching.*

- <u>*Assisted Courses*</u>: *Data Structures and Algorithms, Discrete Structures for CSC, Foundation of CSC, Database Management Systems*

Tennessee Tech University   *Cookeville, TN*
Internship (Research Assistant)   *May 2018 – Aug 2018*

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

Tennessee State University   *Nashville, TN*
Graduate Research Assistant   *2016 – 2018*

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

TECHNICAL SKILLS:

Language: Python, C, C++, MATLAB/Octave, SQL, LaTeX.

Software Tools: Tensorflow, Keras, Scikit-learn, Numpy, Scipy, Pandas, Matplotlib, Seaborn, Plotly, Tableau, Weka, Git/Github, Jupyter Notebook, NPView, Nmap, OPNET, Wireshark, NS2, Network Simulator.

Data Skill: Anomaly/Fraud Detection, Machine Learning, Data Mining, Data Visualization, Data Cleaning, Graph Mining, Time-series Analysis.

Database: MySQL, Oracle, SQL Server.

PUBLICATIONS:

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, 10.1109/IEMCON.2018.8615080

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 (IEEE BigData 2021).

Under Process **P. B. Lamichhane**, W. Eberle, "A Self-Organizing Map Based Graph Similarity Detection Approach on Streaming Graphs". (Target date: end of January, 2022)

Under Process H. Mannering, **P. B. Lamichhane**, W. Eberle, "Discovering Breach Patterns on the Internet of Health Things: A Graph and Machine Learning Anomaly Analysis" (Target date: end of January, 2022)

Under Process R. Manicavasagam, **P. B. Lamichhane**, P. Kandel, D. Talbert, "Drug Repurposing Using Machine Learning Techniques" (Target date: end of January, 2022)

Under Process **P. B. Lamichhane**, W. Eberle, "Anomaly Detection in Graph Structured Data: A Survey" (Target date: end of February, 2022)

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   *Stanford University*
- Applied Data Science with Python   *University of Michigan*