SHAURYA PUROHIT

Ames, IA | 515-817-3915 | shaurya1@iastate.edu | linkedin.com/in/shaurya-purohit/

PROFESSIONAL SUMMARY

I am proficient and have good hands-on experience in the fields of Machine learning, Federated Learning, Cyber-security, Data Analysis and Full Stack Development. My research focuses on developing advanced Artificial Intelligence and Cybersecurity solutions for Anomaly and Intrusion Detection systems using state-of-the-art techniques such as Machine Learning, Federated Learning, and Game Theory. My research involves investigating the application of these techniques to various use cases, including Self-driving cars, EV charging infrastructure, DER Communication with the goal of enhancing their reliability and security.

EDUCATION

Pursuing **PhD** in **Computer Engineering** — August 2019 – Fall 2024 *(Expected)*
Iowa State University - Ames, Iowa
CGPA: 3.86/4.00

Master of Engineering in **Computer Engineering (Minor in Statistics)** — August 2019 - May 2022
Iowa State University - Ames, Iowa
CGPA: 3.84/4.00

Bachelor of Technology in **Information Technology**
Manipal University Jaipur - Jaipur, India — August 2015 - May 2019
CGPA: 9.58/10.00

PROFESSIONAL EXPERIENCE

Iowa State University - Ames, Iowa
Graduate Research Assistant — May 2020 – Present

- Starting Spring 2024, started working on two projects in collaboration with Argonne National Lab
  - The first project enhances real-time operations of distributed energy resources, providing cost-effective, real-time cybersecurity for individual DERs within an aggregation pool through Reinforcement learning and Game theory.
  - The second aims to bolster grid cybersecurity through a novel Machine and Federated Learning methodology. The project underscores a commitment to integrating Machine Learning to address complex energy and security challenges.
- Worked on Cybersecurity of DER communication protocols and EV Charging using Federated Learning.
  - Developed federated learning models enhancing data privacy and cybersecurity in DER and EV charging networks, achieving high accuracy and reduced loss.
- Had the honor of being **selected as a senior PhD student to serve on a panel at the CAE-R Symposium 2023**, where I presented both my research and poster.
- Worked on Game-theoretic Optimization of Cybersecurity Investment Strategies for EV Charging Stations using Attack Defense Trees.
  - This framework integrates the CIA triad and MITRE ATT&CK framework to analyze attack paths, optimize resource allocation, and formulate robust defense strategies
- Worked on cybersecurity of autonomous vehicles using Machine Learning & Deep Neural Networks
  - Developed a Hybrid Anomaly detection system for preventing cyber-attacks on intra-vehicular communication networks with the help of rule based and machine learning techniques. Achieved an accuracy of around 95%.
  - Submitted the enhanced journal version of this work using Deep Neural Networks and variety of databases. Achieved an accuracy of more than 97% and better latency.
- Worked on a project titled Cloud-based multi-sensor remote data acquisition system.

Mutual of Omaha – Nebraska, USA — May 2022 – December 2022
Information Technology Intern

- Worked as an I/S intern with Security and Data Communication team.
  - Worked on Deep Neural Networks for Forcepoint Framework.
  - Worked on complete automation and full stack management of an in-house project titled "Moonet" using Jenkins CI/CD pipeline architecture.

Iowa State University - Ames, Iowa
Graduate Teaching Assistant — August 2021 - December 2021

- Working as a TA for a 500-level course: Real-Time systems (**CPR E 558**)
- Responsibilities included: one-to-one interaction with students for solving queries, helping students in their final course project, providing feedback by grading assignments, quizzes, and exams.

Graduate Teaching Assistant August 2019 - May 2020

- Worked as a TA for courses: Introduction to Computer Engineering and Problem Solving (**CPR E 185**) & Problem Solving in Software Engineering (**S E 185**).
- Responsible for conducting labs every week to help students write programs in C, helping students in their final course project, holding office hours to facilitate one-to-one interaction for resolving queries, grading homework, lab reports, exams and providing appropriate feedback.

ValueLabs – Hyderabad, India January 2019 - April 2019
Software Engineer Intern

- Worked as a Full-Stack Developer on a real time client project titled MfExpert (Micro- Finance Expert) and designed a web application using Angular 7, Node.js and PostgreSQL.

IIT BHU – Varanasi, India May 2018 - July 2018
Machine Learning Intern

- Worked on a project titled Autonomous Car Detection using Deep Learning under the guidance of Dr. Tanima Dutta.
- Implemented Car Detection in images and videos using Machine Learning and Deep Learning.

CERTIFICATIONS

- Machine Learning
  Issued by: Stanford University (via Coursera)
- Cybersecurity Specialization
  Issued by: IBM (via Coursera)
- Cybersecurity Fundamentals
  Issued by: IBM
- AWS Machine Learning
  Issued by: Amazon Web Services (via Coursera)
- Programming in Java
  Issued by: NIIT Technologies

PUBLICATIONS

- S. Purohit and M. Govindarasu, "ML-based Anomaly Detection for Intra-Vehicular CAN-bus Networks," 2022 IEEE International Conference on Cyber Security and Resilience (CSR), Rhodes, Greece, 2022, pp. 233-238, doi: 10.1109/CSR54599.2022.9850292. (***Published***)
- S. Purohit and M. Govindarasu, "Cybersecurity Investment Analysis for Electric Vehicle Charging Infrastructures," 2023 Resilience Week (RWS), National Harbor, MD, USA, 2023, pp. 1-6, doi: 10.1109/RWS58133.2023.10284670. (***Published***)
- S. Purohit and M. Govindarasu, "Federated Learning based Anomaly Detection for DER Communication" IEEE PES GM 2024. (***Accepted***)
- S. Purohit and M. Govindarasu, "FL-EVCS: Federated Learning based Anomaly Detection for EV Charging Ecosystem" ICCCN 2024. (***Accepted***)
- B. Blakely, S. Purohit, K. Ogbuefi, I. Prieto, and M. Govindarasu. "A Federated Intrusion Response Network for Grids (FIRNet-G)." IECON 2024. (***Accepted***)
- S. Purohit and M. Govindarasu, "HAVEN: A Hybrid Anomaly Detection System for Intra-Vehicular CAN-bus Communication using Rule-based and Neural Networks" , IEEE TDSC Journal . (***Accepted***)
- S. Purohit, M. Govindarasu and B. Blakely, "FL-ADS: Federated Learning Anomaly Detection System for Distributed Energy Resource Networks", IET CPS Journal. (***Submitted- Under Review***)

TECHNICAL SKILLS

- **Programming Languages:** Python, Java, C, R
- **Web Based Technologies:** HTML, CSS, Angular, Node.js, PHP, JavaScript, jQuery, Ajax, XML, DHTML
- **ML Frameworks:** Tenser flow, Keras, Sckit-learn, Py Torch, Flower
- **Databases:** MySQL, PostgreSQL

ACHIEVEMENTS & AWARDS

- Secured **1st Rank in B. Tech (IT) 3rd year** & **4th year** for the academic year 2017-18 and 2018-19 respectively.
- Secured **Statewide Ranking 1st** & **India Wide Ranking 3rd** in the Wheebox Employability Skills Test in 2017.
- Published article for e-magazine **EasyShiksha** in 2018.