+1 404 786-1767
sahiti@jhu.edu
https://www.linkedin.com/in/bsahiti/
https://b-sahiti.github.io/

Sahiti Bommareddy

Education

2019– now **Ph.D., Computer Science**, *Johns Hopkins University*, Baltimore, USA
Advisor: Dr. Yair Amir (https://www.cs.jhu.edu/∼ yairamir/)

2017–2019 **M.S., Computer Science**, *Duke University*, Durham, NC

2007–2011 **B.Tech, ECE**, *Jawaharlal Nehru Technological University*, Hyderabad, India

Technical Skills

Languages Python, C, Java, SQL

Tools &Frameworks PyTorch,TensorFlow, NumPy, Pandas, Hugging Face, HP LoadRunner, HP Performance Center, Mininet, Spark

Systems *NIX (CentOS, Ubuntu, Kali, Alma), Windows

Dev Tools Vim, Git, VS Code

Research and Publications

My research focuses on the dependability, resiliency, and security of distributed systems and networks, particularly in the context of critical infrastructure. I specialize in designing and developing intrusion-tolerant systems that maintain operational continuity and required performance levels in the face of faults, cyber-attacks, and intrusions. By integrating advanced machine learning techniques for intrusion detection and situational awareness, I aim to enhance system reliability and performance. Ultimately, my goal is to contribute to the development of resilient critical infrastructure that effectively addresses the evolving challenges of cybersecurity and operational resilience.

Research & Publications @ lab's website: https://jhu-dsn.github.io

- Tolerating Compound Threats in Critical Infrastructure Control Systems, SRDS 2024. *Best Paper*
- ByzSec — A Multi-layered Byzantine Resilient Architecture for Bulk Power System Protective Relays, IEEE Power & Energy Society General Meeting (PESGM) 2024.
- Real-Time Byzantine Resilient Power Grid Infrastructure: Evaluation and Trade-offs, RTSS-W 2022.
- Real-Time Byzantine Resilience for Power Grid Substations, SRDS 2022.
- Data-Centric Analysis of Compound Threats to Critical Infrastructure Control Systems, DSN-W 2021.

Professional Experience

Jan 2013–Dec 2015 **Software Engineer**, *Aktrix Technologies Pvt Ltd*, Hyderabad,India

- Led and expanded a team of 9 performance engineers, overseeing test strategies, coordinating resources, managing risks, and providing training and guidance to new engineers across diverse client projects.
- Pioneered the development of an automated performance monitoring system for multi-cloud environments, enhancing data mining and machine learning analysis. Achieved up to 2x to 5x latency improvement and significantly reduced maintenance costs and Root Cause Analysis (RCA) time in multiple projects.
- Developed and deployed ML-based prediction systems for system load and resource utilization. Built and maintained data pipelines for extracting and cleaning data from cloud monitoring tools and logs. Engaged in feature engineering, model training, and performance monitoring.
- Applied various ML models, including Time Series Models (ARIMA, SARIMA), Regression Models (Decision Trees, Random Forests, XGBoost), and Deep Learning Models

May 2011–Nov 2012 **Performance Engineering Analyst**, *Deloitte*, Hyderabad,India

- Ensured optimal performance across geo-distributed systems by evaluating application performance, analyzing network traffic, and implementing optimizations to enhance system efficiency.
- Led performance testing for 7 Deloitte projects, collaborating with product owners to gather requirements. Developed and executed approximately 40 performance test plans using HP LoadRunner and Performance Center.
- Built and maintained data pipelines, and performed comprehensive data analysis on server monitoring data, network traffic, and resource utilization to identify and address critical performance bottlenecks.
- Collaborated with application development, database, and infrastructure teams to achieve significant reductions in application transaction latency, ensuring compliance with Service Level Agreements (SLAs) through targeted issue resolution and performance tuning.
- Received the Applause Award at Deloitte for outstanding contributions to application performance optimization.

Teaching Experience

Fall 2024	Machine Learning (JHU EN.601.675), *Teaching Assistant*
Spring 2022	Advanced Distributed Systems (JHU EN.601.675), *Teaching Assistant*
Fall 2021	Distributed Systems (JHU EN.601.417/617), *Special Help*
Spring 2021	Software for Resilient Communities (JHU EN.601.310), *Special Help*
Fall 2020	Intermediate Programming (JHU EN.601.220), *Special Help*
Fall 2019	Distributed Systems (JHU EN.601.417/617), *Teaching Assistant*
Spring 2019	Introduction to Artificial Intelligence (Duke CS270), *Teaching Assistant*

Open Source Contributions

Spire: Spire is an open-source intrusion-tolerant Supervisory Control And Data Acquisition (SCADA) system for the power grid. It is engineered to withstand attacks and compromises at both the system level and the network level, while meeting the timeliness requirements of power grid monitoring and control systems (on the order of 100-200ms update latency).
Version 1.3 (Dec 2021): Optimized transaction latency to 30ms (3x improvement) and integrated a Machine Learning-based network intrusion detection system.
Version 2.0 (Jan 2023): Developed the first Byzantine-resilient system for power grid substations with real-time latency constraints (4ms). The system is deployed at PNNL, Siemens, GE, and Hitachi Energy, and has successfully withstood red teaming exercises conducted by hackers from Sandia National Labs.
Spire 2.1 (Feb 2024): Added reconfiguration capabilities to enhance operational continuity and resilience against cyber threats and natural disasters (compound threats).

Web page: https://jhu-dsn.github.io/spire/

Spines: Many applications including critical infrastructure require high demanding combinations of latency, reliability, resilience, and processing even in presence of malicious actors at network level. To support such applications, new overlay dissemination protocols are developed and used to provide the necessary timeliness and reliability. Spines is a generic messaging infrastructure, that provides automatic reconfiguration and network flexibility required for research and production deployments.

Web page: https://spines-org.github.io/

Select Academic Projects

NLP Projects: In these projects I focused on the development and evaluation of advanced Natural Language Processing (NLP) models for text classification and generation tasks. These projects involved designing experiments to assess the impact of various features and algorithms, including traditional methods and cutting-edge techniques. A key component was the fine-tuning of large language models (LLMs) such as BERT and using the Hugging Face Transformers.

Loosely Coupled Key-Value Store with Fault Tolerance: Engineered a sharded, replicated key-value store that utilizes the Raft consensus protocol. The objective of this project was to study the tradeoffs offered by the CAP theorem and implications of data distribution schemes. The prototype built was Consistent, but not Available, under

a network partition.

Fair Decision Making using Privacy-Protected Data: This research investigates if fairness and privacy are fundamentally incompatible, and if there exists some differentially private mechanism which can preserve fairness, or if fairness can only be preserved in some cases. This project extends previous work by exploring new privacy mechanisms, and by designing a new fairness metric. Different privacy preserving mechanisms are explored to reduce error and increase fairness while preserving privacy.

Cracking a Home Router: Conducted a comprehensive security audit of a home router, meticulously probing its vulnerabilities through a battery of known attack vectors. From password cracking to DoS assaults, and from Evil twin exploits to MITM stratagems, the router's defenses were systematically dismantled and scrutinized. This hands-on exploration sheds invaluable light on the myriad security pitfalls lurking in networked systems, fostering a deeper understanding of cybersecurity imperatives.

Performance Evaluation of Fat-Tree: In a bid to unravel the performance nuances of network topologies, this project meticulously crafted and evaluated a Fat-Tree architecture on the Mininet network emulator. By subjecting it to rigorous testing against a conventional tree topology, the project elucidates the impact of application distribution, scheduling schemes, and topology on performance SLAs and Bandwidth Utilization. Results revealed performance differentials spanning from 0.5x to 3x, underscoring the critical role of topology optimization in network efficiency.

Haptic Aid for the Visually Challenged: I spearheaded the development of a prototype computational navigational aid, meticulously crafted to facilitate indoor navigation for the visually impaired. This innovative solution harnesses the power of ultrasonic sensors to perceptively analyze the surroundings, coupled with a micro-controller for real-time data processing. Leveraging this technology, our system delivers intuitive haptic feedback through precision actuators, empowering individuals with visual impairments to navigate with confidence and independence.