Shailja Thakur

Voice: (917) 283 1342
e-mail: st4920@nyu.edu
homepage: shailja-thakur.github.io

Research Interests

Langugae models, Cyber-physical systems, Secure and explainable AI, Safety-critical systems, Side-channel analysis, Anomaly detection, Time-series.

Education

University of Waterloo, Waterloo, ON Canada

Ph.D. Candidate, Electrical and Computer Engineering, April 2022

- Dissertation Topic: "Security and Interpretability in Automotive Systems"
- Advisor: Dr. Sebastian Fischmeister (Affiliations: University of Waterloo)

IIIT, Delhi, India

M.Tech, Computer Science, September 2012

- Dissertation Topic: "WattShare : detailed energy apportionment in shared living spaces within commercial buildings"
- Advisor: Dr. Amarjeet Singh (Affiliations: IIIT Delhi, UCLA)

GGSIPU, New Delhi, Delhi India

B.Tech., Computer Science, September 2008

Honors and Achievements

Post-Doctoral Fellowship in the NSF National AI Institute for Edge Computing Leveraging Next Generation Networks (Athena) 2022

Faculty of Engineering Award, University of Waterloo, 2020

International Doctoral Student Scholarship, University of Waterloo, 2017-2020

Graduate Research Scholarship, University of Waterloo, 2017-2020

Data Analytics Excellence Award, Compuware, 2016

UGC Sholarship for GATE qualified

GATE (Graduate Aptitude Test in ENgineering), Rank 1500, 2012

Academic Excellence Award, GGSIPU, 2008-2012

Recent Activities

Stanford Computer Forum - Graph Learning Workshop, Virtual, September 2021

Inria-DFKI European Summer School on AI (Trustworth AI), July 2021

UAI 2021, Virtual Conference

ICPR Conference, Milan, Italy, 2020

Expectation Teaching Assistant Workshop, Waterloo, 2019

Graduate Research Seminar, UWaterloo, 2019

Waterloo ML, Security, and Verification Workshop, 2019

Volunteer at CPS 2019, Montreal, 2019

TU Automotive Conference 2016, Michigan, 2016

Microsoft Azure ML Competition, 2016

Kaggle Competitions, 2015

Academic Experience

University of Waterloo, Waterloo, Ontario Canada

Graduate Student **May, 2017 - present**
Includes current Ph.D. research, Ph.D. level coursework and research/consulting projects.

Teaching Assistant **January - April, 2021**
Graduate-level course: Data knowledge and modeling analysis. Shared responsibility for lectures (lecture on machine learning interpretability), exams, homework assignments, grading, and office hours.

Teaching Assistant **September - December, 2020**
Course: System Programming and Concurrency Duties included shared administrative responsibilities with faculty instructor, fielding of all student inquiries, and oversight of graduate student teaching assistants and graders.

Teaching Assistant **September - December, 2019**
Undergrad level course Real-time and Safety-critical Embedded systems ECE(652/455). Duties included grading mid-term and finals, delivered special lecture on the application of machine learning for intrusion detection in real-time and safety-critical systems.

IIIT Delhi, Delhi, India

Teaching Assistant **May - September, 2012**
Undergrad level course Operating Systems. Duties included in-person tutorials, lab sessions, grading.

Research Associate **January, 2013 - April, 2013**
The tasks and responsibilities included customizing the data logging script for flyport nodes(wifi & ethernet module) to optimize module Power Consumption and network bandwidth for efficient data transfer over cloud. *Embedded Programming*

Publications

Shailja Thakur, Carlos Moreno, Sebastian Fischmeister,"CANOA: CAN Origin Authentication Through Power Side-Channel Monitoring", Transaction on Cyber-Physical Systems (**TCPS**), 2021, *Special issue on Automotive safet and security.*

Shailja Thakur, Sebastian Fischmeister, "A generalizable saliency map-based interpretation of model outcome", In Proceedings of International Conference on Pattern Recognition (**ICPR**). Milan, Italy, January 2021.

Shailja Thakur, Manaswi Saha, Amarjeet Singh, Yuvraj Agarwal, "WattShare: Detailed Energy Apportionment in Shared Living Spaces within Commercial Buildings", In Proc. of First ACM International Conference on Embedded Systems for Energy-Efficient Buildings (**ACM BuildSys**). Memphis, TN, USA, November 2014 (Acceptance Rate: 27%)

Manaswi Saha, **Shailja Thakur**, Amarjeet Singh, Yuvraj Agarwal, "EnergyLens: Combining Smartphones with Electricity Meter for Accurate Activity Detection and User Annotation", In Proc. of Fifth International Conference on Future Energy Systems (**ACM e-Energy**). Cambridge, UK, June 2014 (Acceptance Rate: 20%)

Nipun Batra, Manoj Gulati, Amarjeet Singh, Mani Srivastava, "It's Different: Insights into home energy consumption in India". In Proc. of Fifth ACM Workshop On Embedded Systems For Energy-Efficient Buildings, Rome, Italy, November 2013.`https://github.com/nipunbatra/Home_Deployment`

Paper under review

Shailja Thakur, Sebastian Fischmeister, "TiME: Time-series based model outcome explanation", Transaction on Knowledge and Data Engineering (TKDE), 2022.

Professional Experience

MAGNA International, Remote

Student Staff **February, 2021 - Present**

Participating in a project in collaboration with MAGNA international. The project aims at developing and interpreting driver behavior analysis models using LiDAR, CAN logs, and VLT data captured from a study consisting of several trips by participating drivers in the area of Waterloo, ON, Canada, comprising of trips from highways, countrysides, high traffic intersection points.
Time-Series Analysis, Driving Behavior Analysis, Time to Collision detection, LSTMs, Explainability

Acerta Analytics, Waterloo, Canada

Data Science Intern **September, 2017 - December, 2017**

Worked on projects including anomaly detection from Engine, Transmission, Anti-Lock Brake Systems on Chrysler data. Detection of the anomaly using acoustic sensor data from windmill by ZF Manufacturers. Tyre category classification using acoustic data from sensors mounted across the tire at specific positions.
Time-Series Analysis, Variational Autoencoders, Data Analysis, Anomaly Detection

Compuware, Gurgaon, India

Data Science Consultant **August, 2015 - March, 2017**

Participated in several consulting projects in collaboration with GM, Chrysler, and Fiat, including anomaly detection for fault detection and diagnosis, usage based insurance by scoring driving behavior using features captured by Onboard diagnostic (OBD) tool. I also participated in public data competitions such as Kaggle, Microsoft.
Time-Series Analysis, Autoencoders, Regression, Anomaly Detection

U2opia Mobile, Gurgaon, India

Software Engineer **August, 2014 - July, 2015**

USSD based twitter app implementation in java, tweets analysis for user recommendation, sentiment analysis, and performance tuning.
Twitter APIs, development, Sentiment analysis

IIIT Delhi, India

Research Intern **May, 2013 - July, 2013**

Developed an android application for data collection from various interfaces for indoor localization and user context analysis.
Speech Processing, Localization & Location Profiling, stochastic Bayesian models

Projects

Language model for less popular programming languages

New York University **March, 2022 - Present**

Large language models have demonstrated text generation capabilities at par with the human level. One of the widely used applications is for code completion across programming languages such as C, C++, Python, JAVA, dotNet. However, the quality of generations is poor for low-resource programming languages such as Verilog. To address the data hunger for language models, we prepare a text corpus comprising Verilog-based text and source code available from various sources such as public datasets, books, and specifications, and fine-tune the pre-trained language model. We evaluate the correctness of generated code across language models of varying complexity. We further explore the quality of synthesis for bugs, quality, and vulnerabilities.

Model outcome explanation for time-series

University of Waterloo **December, 2020 - Present**

Due to the criticality of decision-making in safety-critical systems, there is a need for an explanation algorithm for deep learning-based classifiers. Proposed an explanation algorithm for a time-series-

based classification algorithm. The approach is a refined version of the perturbation-based interpretation. The algorithm's objective is to assign a relevance score to every time point in the input sequence. The approach empirically determines a sequence of relevance scores for the input sequence such that the time-points (or the segments of time-points) significant for the target class are assigned scores (greater than a threshold) greater than the time-points that are not significant. A rigorous evaluation of the approach across a wide range of models and across the domain of medicine and automotive for verification, accuracy, and the scalability of the approach using a set of metrics shows that the technique is effective in providing an interpretation of time-series-based model outcomes.

Model outcome explanation for images

University of Waterloo **April, 2019 - Present**

Proposed a perturbation-based explanation technique by optimizing the input with respect to the class-specific confidence score. The approach empirically update a randomly initialized mask by turning pixels on and off and assigning weights to the pixels according to the output class attribution score. The resultant saliency mask highlight the regions of the input that are significant in classifying the input to the output. In addition, the approach identifies alternative sets of input samples for the significant regions of the input using a generative model such that the difference in the class attribution with and without the substitution is less than a pre-defined threshold.

Intrusion Detection system for Automotive Systems

University of Waterloo **January, 2018 - Present**

Proposed a sender authentication technique for CAN (Controller Area Network) - bus communication protocol using power consumption measurements of the ECUs (Electronic Control Units) as the characteristics of the transmission and non-transmissions. The approach has been designed to work in real-time and safety-critical systems. The approach has been tested in a real-world setting on different kinds of automotive systems (such as trucks, heavy-duty vehicles, lab prototype ECUs) for the robustness and the reliability of the technique.

Anomaly Detection using power consumption measurements

University of Waterloo **May - December, 2017**

Anomaly detection in vehicles is a challenging task both in terms of security and safety. Any fault and failure should be detected and reported in real-time and under a resource constraint environment for precaution measures. Therefore, I developed an anomaly detection technique using denoising autoencoders and power consumption measurements as the characteristics of the normal behavior (not anomalous) of the component of interest. The anomalous events are the events that have power consumption characteristics of the component absent from the input data distribution. The encoding is available in the latent space of the autoencoder. The implementation has been deployed and tested in real-world field trials for detecting anomalies.

Brain Signal Decoding - Azure Competition

Lochbridge **May - June, 2016**

Microsoft organized the competition. The objective of the competition was to build a machine learning model to decode perceptions of human subjects from the brain, specifically Electrocorticographic (ECoG) signals from Microsoft Cortana Intelligence Suite. The task of the model was to predict whether the human subject saw a house image (stimulus class 1) or a face image (stimulus class 2) from the ECoG signals collected from the subtemporal cortical surfaces of four seizure patients.
Secured leaderboard rank 21 from 11500 worldwide submissions.

Anomaly Detection Using Simulated Data

Lochbridge **January - April, 2015**

Developed several prognostics and diagnostics models using a simulator that captures scenarios applicable to our use case. Use Cases - Automotive engine oil efficiency by detecting time to failure

prediction. Identifying anomalous behavior in the engine RPM. Technique used includes point anomaly detection, Collective Anomaly detection using 2D kernel density estimation, random forest.

Predict Usage-Based Insurance using Driving Behavior

Lochbridge **September - December, 2015**

Designed and implemented a unique approach to predict driver scores using a fusion of multiple data sources such as the trip summary (hard accelerations, brakes, mileage driven, and duration of the trip), the weather during the trip, road condition, road visibility, and crime factor. The driver score acts as a premium calculation factor/validation factor. We also detected driving patterns per individual by accumulating the driver score over a period of time. The driving pattern is taken as feedback to tune the future score.

Twitter Application, User Engagement, Notifications

U2opia Mobile **August - November, 2015**

Developed a Twitter application for USSD based phones capable of handling huge traffic. Analyzed the tweets and the traffic for sentiment analysis using user specific hidden patterns to recommend subscriptions to potential users.

Personal Energy Usage Monitoring in Commercial and Residential Settings

IIIT Delhi **May - November, 2014**

The primary objective of this research was to explore the combined potential of using smartphones with smart electricity meters in commercial buildings. I designed and developed a system, WattShare, motivated by our previous project called, EnegyLens, a system for apportioning energy usage to individual users in residential buildings, for monitoring the appliance usage events in shared setting and attributing them to the room in which the event occurred, thereby apportioning the usage at room level.

Uncovering Contextual Insights with UbiComp Dataset

IIIT Delhi **April - May, 2014**

The objective was to find useful context about the user and phone i.e. the users behavior on the usage of the phone. The most important factor for determining the behavior of phone usage is to determine the battery consumption behavior of user and the reasons behind the abrupt drop of the battery. Developed a regression model to predict an estimate of the time to 5% battery level and measures to preserve the remaining battery life by reporting the services with maximum battery consumption and provide recommendations for charging locations using location data.

Indoor localization using mobile sensors and static sensors

IIIT Delhi **March - May, 2013**

Designed and developed (i) an android application for collecting wifi signal strength from nearby APs, audio samples, accelerometer events. (ii) Customised a Flyport node to collect light, PIR, temperature data periodically. The data from the two sources used to get indoor occupancy achieved high accuracy, which cannot be otherwise achieved in isolation from one another. `http://energy.iiitd.edu.in/`

Middleware Application for Android

IIIT Delhi **March - May, 2012**

Developed a user interface on the mobile platform for a middleware-SensorAct for sensing and actuation of sensors in building management systems. `http://www.sensoract.iiitd.edu.in/`

Computer Skills

- Python, R, Octave, Unix shell scripts, SLURM
- C/C++, Java, Android, Matlab
- Applications: github, Emacs, LaTeX, Overleaf

- GitHub Copilot, HuggingFace, Transformers,
- Tensorflow (GPU/CPU, Tensorboard), PyTorch, Jupyter, HPCs
- Operating Systems: Ubuntu, Fedora, Mac

COURSES

- Machine Learning: Statistical and Computational Foundations (*UWaterloo*)
- Statistics in Engineering (*UWaterloo*)
- Statistical Signal Processing (*UWaterloo*)
- Methods and Principles of Safety-critical Embedded Software (*UWaterloo*)
- Data and Knowledge Modelling and Analysis (*UWaterloo*)
- Statistical Computing (*IIITD*)
- Cryptography (*IIITD*)
- Mobile and Ubiquitous Computing ((IIITD))
- Advanced Mobile Computing (*IIITD*)
- Embedded Systems (*IIITD*)
- Database and System Implementation (*IIITD*)
- Distributed Systems (*IIITD*)
- Learning From Data(*Edx.org*)
- Statistical Inference(*Coursera.org*)
- Regression Models(*Coursera.org*)
- Data Scientist Toolbox(*Coursera.org*)
- Machine Learning(*Coursera.org*)

Referees

Dr. Sebastian Fischmeister
Associate Professor, Department of Electrical and Computer & Engineering
University of Waterloo
✉ sebastian.fischmeister@uwaterloo.ca

Dr. Mark Crowley
Assistant Professor, Department of Electrical and Computer & Engineering
University of Waterloo
✉ mark.crowley@uwaterloo.ca

Dr. Hiren Patel
Professor, Department of Electrical and Computer & Engineering
University of Waterloo
✉ hdpatel@uwaterloo.ca

Dr. Carlos Moreno
Senior Research Associate, Department of Electrical and Computer & Engineering
University of Waterloo
✉ carlos.moreno@uwaterloo.ca