Vaisakh S

Curriculum Vitae

PERSONAL DETAILS

Birth	May 30, 1992
Address	Geetham, Paraoor, Kollam, India
Contact	Mail: `vaisakhs.shaj@gmail.com` • Phone: (+91) 8848570189

EDUCATION

M Tech. Machine Learning And Computing 2014-2016

Department Of Mathematics
Indian Institute Of Space Science And Technology(IIST), Trivandrum
***CGPA**: 8.36/10*
***Thesis Project**: Learning Structured Dictionaries For Sparse Representation Based Monaural Source Separation And Pattern Classification, **Thesis GPA**: 9/10*

B Tech. Electrical And Electronics 2009-2013

Department Of Electrical And Electronics Engineering
University Of Kerala(TKMCE)
***CGPA:** 8.1/10*
***Thesis Project**: Computer Aided Heart Sound Analysis, **Thesis GPA**: 9/10*

WORK EXPERIENCE

McAfee 2017-present

Data Scientist *Location: Bangalore*

Working on two projects currently 1) Adversarial Machine Learning for Evasion Attacks on Deep Learning Models, 2) Network Anomaly Detection.

Intel Security 2016-2017

Security Researcher *Location: Bangalore*

Developed and patented a Deep Neural Net Based Dynamic Malware Classification Engine for the Advanced Threat Defense Research Team.

Intel 2015-2016

Graduate Intern *Location: Bangalore*

Developed Sparse Machine Learning For Audio Understanding. Application included Audio Denoising, Source Separation and Classification.

PUBLICATIONS

Learning Sparse Adversarial Dictionaries For Multi Class Audio Classification (Oral Paper) 2017

*Asian Conference On Pattern Recognition(ACPR), Nanjing, China.(**Oral Acceptance: 8.5%**)*
Authors: Vaisakh Shaj, Puranjoy Bhattacharya
***Link:** http://arxiv.org/abs/1712.00640*

Edge PSO: A Recombination Operator Based PSO Algorithm For Solving TSP(Won the Best Paper Award) 2016

*International Conference on Advances in Computing Communications And Informatics, Jaipur, India.(**Oral Acceptance: 16%)***
Authors: Vaisakh Shaj, Akhil P M, Asharaf S
***Link 1:** http://ieeexplore.ieee.org/document/7732022/* ***Link 2:** https://goo.gl/KbvKt3*

PATENTS

Memory Efficient Deep Learning Model For File Independent Dynamic Malware Analysis(Filed) 2018
Inventors: Vaisakh Shaj, Ashish Mishra

ACADEMIC PROJECTS

Learning Structured Dictionaries For Sparse Representation Based Monaural Source Separation And Pattern Classification (M-Tech Thesis) 2015-16
Advisor: Dr Puranjoy Bhattacharya
***Link**: https://goo.gl/Dvfj7M*

Multi-Label Classification Using Struct SVM 2015
Advisor: Dr Sumitra S Nair, Dr Asharaf S
***Link**: https://goo.gl/gTec2K*

Carried out as part of course mini-project, where we explored the scope of applying the struct-SVM algorithm for Multi-Label Classification Problems. A suitable loss function(hamming distance) and joint input output feature map representation using tensor products was formulated in accordance with the problem. Testing and training were done on a semantic scene classification dataset yielding satisfactory results.

Edge PSO: A Recombination Operator based PSO Algorithm For Solving TSP 2015
Advisor: Dr Asharaf S
***Link**: https://goo.gl/Eyioto*

Carried out as a part of Evolutionary and Natural Computing Course. We proposed a novel approach for solving TSP using discrete PSO, namely edge- PSO by intelligent use of enhanced edge recombination Operator.

Sequential Minimal Optimization for SVMs 2015
Advisor: Dr Sumitra S Nair

Carried out as a part of the Pattern Recognition and Machine Learning Course at IIST where a soft margin SVM classifier was designed from scratch using MATLAB. Involved understanding literature and implementing the sequential minimal optimization algorithm for solving the dual of the SVM objective function.

INDUSTRIAL PROJECTS

Adversarial Machine Learning: Evading Deep Learning Models of McAfee Anti Malware Products By Crafting Adversarial Samples 2017
McAfee

* With the assumption that we have knowledge of the feature vector used, we created adversarial samples using Fast Gradient Sign Method(FGSM) and Jacobian Saliency Map based Approach(JSMA).

* Was able to successfully evade this matured deep neural net and bring down the detection rate to near zero on a test set of sample size 1000.

* Currently investigating at possible defense mechanisms against these attacks.

Network Anomaly Detection on Cloud Workloads 2017

McAfee

* The data includes flow logs from cloud services like AWS and Azure.

* Over fixed time windows extracted features based on connection graphs which was fed to an SVM classifier.

* Currently investigating at adding spectral features and/or graph kernels for better predictions.

Deep Neural Net for Malware Detection and Classification 2016

Intel Security

Developed a dynamic malware analysis engine for the Advanced Threat Defense Team at Intel Security for detecting and classifying malware into higher and lower level families. The family classification system was designed to learn two tasks simultaneously, for which a multi-task learning framework was used which gave much better results compared to two single task learning networks.

OTHER PROJECTS

- Dimentationality Reduction Using Kohonen Self Organzing Maps(MATLAB) - MA613: Data Mining
- Improved K-means clustering using Genetic Algorithms(MATLAB) - MA616: Evolutionary and Natural Computing
- Convolutional Neural Network based Histopathological Image Analysis(Python) - MA820: Neural Networks
- CBOW and skipgram word vector analysis on Windows API calls(Intel Security)

ACHIEVEMENTS AND ACTIVITIES

- Won Best Paper Award at ICACCI 2016, from among among 1474 submissions from authors round the globe.
- McAfee Excellent Achievement Award from Senior Principal Engineer Dr. Celeste Fralick for the work in Adversarial Machine Learning.
- Received a grant of 1500 USD from McAfee to present paper at the 2017 Asian Conference on Pattern Recognition.
- Gained verified certificates for successfully completing(with distinction) the **Introduction To Mathematical Thinking**, **Python Data Structures**, **R Programming**. MOOC courses offered through Coursera.
- Qualified 2013 Graduate Aptitude Test In Engineering(GATE) and was placed at 98 percentile amongst 152381 candidates
- Received Graduate Fellowship from Department of Space, Government of India for pursuing graduate studies at IIST.
- Recieved EPSRC-DST grant to attend the Indo-UK Workshop on Conformal Prediction for Reliable Machine Learning, Hyderabad, India.

SKILLS

Programming Languages	Python,Matlab,Octave,C,C++,R
ML-Libraries	Tensorflow, scikit learn, NLTK, SparseLab
Documentation Tools	LaTeX, Open Office, MS Office