Vaisakh Shaj

Resume

+91 9206022011
vaisakhs.shaj@gmail.com
https://github.com/vaisakh-shaj/

Education

2014–2016 **Indian Institute Of Space Science And Technology**,
M.Tech in Machine Learning and Computing, CGPA: ***8.4/10*** .

- Major: **Machine Learning**; Minor: **Mathematics**
- Key Courses: Pattern Recognition and Machine Learning, Reinforcement Learning, Neural Networks, Data Mining, Matrix Computations, Applied Statistics, Discrete Mathematics, Optimization Techniques, Computer Modeling and Simulations(Queuing Theory), Discrete Mathematics.

2009–2013 **T K M College Of Engineering, University Of Kerala.**,
B.Tech in Electrical Engineering, CGPA: ***8.1/10***.

- Major: **Electrical Engineering**; Minor: **Computer Engineering**
- Key Courses: Modern Operating Systems, Computer Networks, Microprocessors, Digital Electronics and Logic Design, Digital Signal Processing, Electrical Machines, Control Theory.

Experience

Industry

2017–2018 **McAfee**,
Role: Data Scientist, Location: Bangalore.

- Adversarial Machine Learning : Analysis of robustness of large deep learning models in adversarial settings, Network Anomaly Detection.
- **Finalist for CEOs Innovator of the Year Award(top 5 out of 2500 employees)**

2015–2017 **Intel**,
Role: Researcher(2016-17), Graduate Intern(2015-16), Location: Bangalore.

- Developed a Deep Neural Net Based Dynamic Malware Classication Engine for the Advanced Threat Defense Research Team, which is currently in production.
- Developed Sparse Machine Learning Algorithms For Audio Understanding. Applications included Audio Denoising, Source Separation and Classication.

Independent Course Work

2017 Deep Reinforcement Learning(UC Berkley Fall 2017)[Code]

2016 Deep Learning(Hugo Larochelle's Course, Udacity)[Code]

2015 Introduction to Mathematical Thinking[Certificate], R Programming[Certificate]

Publications

2017 **"Learning Sparse Adversarial Dictionaries For Multi Class Audio Classication " (Oral Paper - Oral Acceptance: 8.5%)[ArXiv]**,
IAPR Asian Conference on Pattern Recognition, Nanjing, China.,
Authors: Vaisakh Shaj, Puranjoy Bhattacharya .

2016 **"Edge PSO: A Recombination Operator Based Particle Swarm Algorithm for Solving TSP " (Won Best Paper Award)[Xplore]**,
International Conference on Advances in Computing, Communications and Informatics, Jaipur, India.,
Authors: Vaisakh Shaj, Akhil P M, Asharaf S .

Scholastic Achievements

2018 Top 5 Finalist from among 2500 Employees for **McAfee CEO's Innovator Of The Year Award 2018**.

2016 Won the **Best Paper Award** at ICACCI 2016, from among among 1474 submissions from authors round the globe.[Certificate]

2013 Qualied 2013 Graduate Aptitude Test In Engineering(**GATE**) and was placed at **98 percentile** amongst 152381 candidates.

2017 Received **Graduate Fellowship** from **Department of Space**, Government of India for pursuing graduate studies at IIST.

2017 Received a travel grant of 2000 USD from McAfee to present paper at the **2017 Asian Conference on Pattern Recognition**, Nanjing, China.

2017 Recieved The UK Engineering and Physical Sciences Research Council (**EPSRC**) and the Indian Department of Science and Technology (**DST**) **Travel Grant** to attend the Indo-UK Workshop on Conformal Prediction for Reliable Machine Learning, Hyderabad, India.

Relevant Projects

2018 **Deep Reinforcement Learning(Independent Work)** .

- A GitHub Repository For The Study and Analysis of Deep Reinforcement Learning Algorithms.
- Implemented and improved upon latest literature on Imitation Learning, Policy Gradients, Deep Q Learning, Model Based RL on standard simulated environments.

2016 **Learning Structured Dictionaries For Sparse Representation Based Monaural Source Separation And Pattern Classification (M.Tech Thesis) [Thesis Report]**,
Advisor: Dr. Puranjoy Bhattacharya(Intel) .

2018 **Adversarial Machine Learning: Measuring Robustness of Deep Learning Models in Security Sensitive Applications(McAfee)** ,
Advisor: Dr. Yonghong Huang .

- Research involved the understanding of the robustness of large deep learning models in adversarial settings.
- Using multiple open source libraries(eg: Cleverhans) created white-box and black-box attacks on a deep learning based malware classication engine of McAfee and brought the accuracy of the system to less than 10 percent.
- Devised a mechanism to detect adversarial samples.

2017 **Deep Neural Networks for Malware Detection and Classication (Intel)** .

- Developed a Deep Neural Net Based Dynamic Malware Classication Engine for the Advanced Threat Defense Research Team, which is currently in production.
- Leveraged Transfer and Multi Task Learning to accomplish this effectively.

2015 **Multi-Label Classication Using Struct SVM (IIST) [Report]**,
Advisors: Dr. Asharaf S, Dr. Sumitra S Nair, .

- We explored the scope of applying the struct-SVM algorithm for Multi-Label Classication 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 classication dataset yielding satisfactory results.

Languages

English	Advanced
Malayalam	Advanced
Hindi	Intermediate

Computer skills

Programming Languages Python, MATLAB, Java, R, C

Libraries TensorFlow, Scikit-Learn, OpenAI Gym

Writing Tools LaTeX, Open Office, MS Office