

# Somesh Singh

website | singhksomesh@gmail.com | 9140827410 | LinkedIn | GitHub | Twitter

## EXPERIENCE

### COMMERCEIQ, BANGALORE | DATA SCIENTIST (INTERN)

July 2021 – Current

- Working on advertisement optimization on e-commerce platforms such as Amazon and Walmart.

### MIDAS LABS, IIIT DELHI | RESEARCH INTERN

May 2020 – Current | Delhi, India

- Research: Gradient estimation based white-box **adversarial attacks** and black box attacks on Automatic Essay Scoring (AES) systems with customized policies using Tensorflow and Pytorch.
- Worked on generating data free adversaries, investigating dataset bias and worked on post-hoc protection mechanisms against adversarial attacks.
- Supervised by** Prof. Rajiv Ratn Shah (Dept. of CSE & HCD, IIIT Delhi).

### MYSMARTPRICE WEB TECHNOLOGY | DATA ANALYST AND SOFTWARE DEVELOPMENT INTERN

May 2020 – July 2020 | Hyderabad, India

- Built Knowledge-based active and passive **recommendation systems** using Bayesian and Non-Bayesian methods using Java, Python, Django and RESTful APIs.
- Built and deployed overall **Social Media Crawling** tools utilizing Docker container using Java, Python and Selenium integrated with cloud and parallel computing.

## PROJECTS

### CODE-SOUP | OPEN-SOURCE

- Collection of easy to understand Algorithms in "Adversarial Deep Learning" written by Dr. Di Jin, Dr. Yifang Yin, Yaman Kumar, and Dr. Rajiv Ratn Shah, and its tutorials.
- URL:** Code-Soup

### DECEPTICONLP | OPEN SOURCE PROJECT, LEAD DEVELOPER

March 2020 - Present

- DecepticoNLP is a Python based PyTorch Wrapper for robustness monitoring and adversarial debugging of NLP models powered by Travis CI.
- DecepticoNLP has implementations of various character & word level adversarial perturbations for text.  
<https://github.com/SforAiDL/decepticonlp>

### FLAIREDIT | MACHINE LEARNING WEBAPP

April 2020

- Built a complete text classification web-app using Python and PyTorch and deployed it on Heroku which scrapes data from Reddit, pre processes and classifies its flair tag.  
**URL:** <https://github.com/someshsingh22/FlaiReddit-MIDAS>

## EDUCATION

### BIRLA INSTITUTE OF TECHNOLOGY AND SCIENCE, PILANI

B.E. (HONS.) IN COMPUTER SCIENCE,  
MINOR IN DATA SCIENCE

Expected July 2022 | Goa, India

CGPA - Minor: 9/10, Overall: 7.86/10

## PUBLICATIONS

### SEMEVAL-2020

BPGC at SemEval-2020 Task 11:  
Propaganda Detection in News  
Articles with Multi-Granularity  
Knowledge Sharing and Linguistic  
Features based Ensemble Learning

### ICDM-2021

MINIMAL: Mining Models for Universal  
Adversarial Triggers (Review)

### CIKM-2021

Automatic Essay Scoring Systems Are  
Both Overstable And Oversensitive:  
Explaining Why And Proposing  
Protection Mechanisms (Review)

### AAAI-2021

Improving adversarial robustness of NLP  
Systems using mutual information and  
sub-network training. (Review)

## SKILLS

Python, C/C++, Java,  
Tensorflow/PyTorch, AWS, Django/Flask

## COURSEWORK

### GRADUATE

Meta Learning

### UNDERGRADUATE

Machine Learning, Natural Language  
Processing, Information Retrieval,  
Computer Programming (*Teaching  
Assistant*) Data Structures & Algorithms,  
Deep Learning, Applied Statistical  
Methods, Artificial Intelligence,  
Foundations of Data Science, Database  
Systems, Operating System,

## SOCIETIES

Events Head, PoR, CTE, Core member,  
SAiDL, Head of Duties, LRG