ANUP KUMAR GUPTA

☎ +91-8800764516 | ✉ msrphd2105101002@iiti.ac.in | ⌨ AnupKumarGupta

EDUCATION

Indian Institute of Technology Indore *Aug. 2021 - Present*
Ph.D. in Computer Science and Engineering

Indian Institute of Technology Indore *Aug. 2019 - Aug. 2021*
M.S.(Research) in Computer Science and Engineering *CPI: 10/10*

Dr. A.P.J. Abdul Kalam Technical University, Lucknow *Aug. 2013 - Jul. 2017*
B.Tech. in Computer Science and Engineering *Score: 78.42%*

Navals National Academy, Gorakhpur *May 2012*
All Senior School Certificate Examination *Score: 84.6%*

Kendriya Vidyalaya Duliajan, Duliajan *May 2010*
All India Secondary School Examination *CGPA: 9.2*

RESEARCH

Adversarial Attacks on Medical Image Segmentation Models *Aug. 2021 - Present*
– Devised a novel attack architecture that selects the best surrogate loss function to perform attacks on medical image segmentation models while adding minimum adversarial perturbations.
– The architecture was able to fool the state-of-the-art medical image segmentation models with an attack success rate of more than 99%.

Defence against Adversarial Attacks on NLP Models *Jan. 2021 - Jun. 2021*
– Devised two novel transformation based defences that can circumvent state-of-the-art attacks.
– The proposed defence overcome the drawbacks of the existing spelling correction based defences.

Adversarial Attacks on Audio-Visual Speech Recognition Models *May. 2020 - Nov. 2020*
– Devised a novel attack to breach the state-of-the-art AVSR models by simultaneously deceiving the detection algorithm, with an attack success rate of 100%.

Adversarial Attacks on Visual Speech Recognition Models *Dec. 2019 - Apr. 2020*
– Devised a novel algorithm to perform an attack on the state-of-the-art VSR models with a 100% attack success rate.
– The algorithm was able to circumvent popular defences with an attack success rate of more than 99%.

PUBLICATIONS

– **Anup Kumar Gupta**, Puneet Gupta, and Esa Rahtu. "DARE: Deceiving Audio–visual speech Recognition model." *Applied Intelligence (2021)*, DOI: https://doi.org/10.1007/s10489-021-02846-w.

– Saumya Mishra, **Anup Kumar Gupta**, and Puneet Gupta. "FATALRead – Fooling visual speech recognition models." *Knowledge-Based Systems (2021)*, DOI: https://doi.org/10.1016/j.knosys.2021.107503.

PROJECTS

Next Word Prediction *Sep. 2019 - Nov. 2019*

Course Project

- An LSTM based deep neural network capable of predicting next word based on previous words inputted by the user.
- Framework: TensorFlow, Language: Python

Automatic Text Summarization *Jul. 2016 - Apr. 2017*

Major Project

- A Deep Neural Network capable of producing a summary of a larger piece of text using the abstract summarization technique.
- Framework: TensorFlow, Language: Python

Biometric Attendance System *Dec. 2015 - Apr. 2016*

Departmental Responsibility

- Deployed as an attendance system for more than 600 faculty and staff members of Ajay Kumar Garg Engineering College.
- Frameworks: ASP.NET, SQL Server , Language: C#

WORK EXPERIENCE

Kwench Global Technologies Pvt. Ltd. Noida, Uttar Pradesh

Software Engineer *Oct. 2017 - Apr. 2018*

- Developed Workplace Bots in a team that is Product Partner of Workplace, an enterprise connectivity platform by Facebook.
- Worked on the Reward and Recognition Platform that is trusted by over 500 companies across 63 countries.
- Developed rules for the Reward Platform, which helps provide the clients with numerous configurations of the Reward System of their choice with no change in the code.

Novoinvent Softwares Pvt. Ltd. Noida, Uttar Pradesh

Software Engineer *Jul. 2017 - Sep. 2017*

- Worked on a US government insurance project for the state of Maryland, "Maryland Health Connection" which is the state's official health insurance marketplace for individuals and families to compare and enrol in health insurance.

Software Development Centre (Software Incubator) Ghaziabad, Uttar Pradesh

Student Co-ordinator/ Software Engineer *Aug. 2014 - May 2017*

- Developed a Biometric Attendance System for the faculty and staff of Ajay Kumar Garg Engineering College (AKGEC), Ghaziabad.
- Developed and maintained more than 10 portals, websites and platforms related to AKGEC.
- Web Team Member, Event Organiser: Tech Trishna'15, the annual national technical festival of AKGEC, which saw a footfall of 1500+ participants.
- Developed an online registration and slot booking portal in the Blood Donation Camp, 2016 & 2017.

My Own Space Research Consultancy Ghaziabad, Uttar Pradesh

Student Intern *Jun. 2016 - Jul. 2016*

- Designed and developed a website that provides an easy solution to buyers for accessing reviews for any property and helps them make the correct decision.

Sarvodya Ventures Ghaziabad, Uttar Pradesh

Student Intern *Jun. 2015*

– Worked on a live portal that connects transporters, truck drivers, customers and other related entities.

EXTRACURRICULAR ACTIVITIES & ACHIEVEMENTS

– **Student Placement Manager**, Training and Placement Cell, IIT Indore, Sep. 2019 - Aug. 2021

– **Member**, Postgraduate Academic Council, IIT Indore, Nov. 2020 - Feb. 2021

– **Instructor**, in **Rashtriya Avishkar Abhiyan**, an initiative by **Ministry of Education**, Aug. 2019

– **Student Co-ordinator**, Software Development Center (R&D center of college), Aug. 2014 - May 2017

– **2nd Runner-up**, Coding event conducted by Codechef Campus Chapter of college, Apr. 2017

– **Finalist**, Technical Quiz, "QuizUp" in Tryst, IIT Delhi, Feb. 2017

– **Winner**, Anti-Ragging Poster Making Competition, Aug. 2015

– **Winner**, Techno-managerial event, "The Last Strike", Feb. 2015

– **Co-ordinator**, Workshops on WordPress and classes on Python, ASP.Net, Aug. 2014 - May 2017