




# Kumarakrishna Valeti

 kumarakrishnav@gmail.com    Kumarakrishna Valeti    Kumarakrishna Valeti

## Education

**B.E. Computer Science, Minor in Data Science** 2021 – 2025  
*Birla Institute of Technology And Science - Pilani*  
CGPA: 9.12 | Minor CGPA: 9.6

## Work Experience

**TELUS Digital** Jan 2025 – present  
*Machine Learning Intern*

- **Fine-tuned** all-mpnet-base-v2 for mapping job titles, degrees, and majors to predefined lists, achieving **>98% accuracy**
- **Optimized inference** for a fine-tuned LLaMA 8B Instruct model using bits-and-bytes **quantization**, **speculative decoding**, structured outputs, and prefix caching with **vLLM**

**MASTH (UltraHive Healthcare Pvt Ltd)** May 2023 – Jul 2023  
*Machine Learning Intern*

- Developed machine learning and deep learning based models to **detect emotions** from text journal entries, achieving a maximum **accuracy of 97%** using GloVe embeddings and TF-IDF vectoriser
- Created **Flask APIs** and a mock app using Android Studio for testing before integration into the MASTH app

## Projects

**Adversarially Robust ML-Based Android Malware Detector** Aug 2023 – Oct 2024

- Developed 28 Android malware detectors using permissions and intents extracted from AndroidManifest.xml, achieving a maximum **accuracy of 96%**, under the guidance of Dr. Hemant Rathore
- Proposed GBKPA, an **evasion attack** causing an average **misclassification rate** of 77%
- Proposed **'AuxShield' defence** strategy reducing the misclassification rate from 77% **to 3.25%**, enhancing robustness

**Analysis of Memory Safety Guarantees of Rust Integrations** Aug 2023 – Dec 2023

- Integrated **Rust** with a C-based TCP/IP stack, exploring conditional **memory safety guarantees**, and conducted performance and memory benchmarks for Rust integrations into the C codebase
- Used **perf** and **Valgrind** suite for benchmarking the Rust integrated codebase


**Linear Decision Trees: A Comparative Study** Apr 2024 – Jul 2024


- Studied **Linear Decision Trees** against neural networks, decision trees, and random forests on synthetic and real-world datasets with varying **noise** and **complexity**

**Deep Q-Network based Malware Dataset Expansion** Oct 2024 – Jan 2025

- Developed ExpanQN, a **Deep Q-Network-based attack** that expands existing malware datasets by generating adversarial variants, achieving a **55.16 expansion ratio** for five malware families with 94% similarity to source samples
- Generated highly **transferable** adversarial malware samples, with **71%** evading detection across **10 classifiers**
- Improved **robustness** to **>95%** by adversarially **retraining** the models using the expanded dataset
- **Paper accepted** at International Joint Conference on Neural Networks (IJCNN) 2025

## Publications

**GBKPA and AuxShield: Addressing Adversarial Robustness and Transferability in Android Malware Detection**   
*Kumarakrishna Valeti, Hemant Rathore* | Forensic Science International: Digital Investigation (Elsevier) | October 2024

**Linear Decision Trees: A Comparative Study with Insights on ReLU Neural Networks**   
Nirmal Govindaraj†, *Kumarakrishna Valeti*†, Siddhant Kulkarni†, Nandan Surani†, Hemant Rathore | 2025 IEEE 22nd Consumer Communications & Networking Conference (CCNC) | January 2025 | † Equal Contribution

## Teaching Experience

**Teaching Assistant - BITS Pilani** Aug 2023 – Dec 2024

- Responsible for conducting tutorials and programming labs as part of **Relational Databases, Operating Systems, Computer Architecture and Logic in Computer Science**

## Awards

Best Paper Award - DFRWS APAC 2024 Conference	Winner – Vimarsh 5G Hackathon conducted by BPR&D, TCoE and Ministry of Home Affairs	SOLVE grant by BITS Goa Innovation, Incubation & Entrepreneurship Society	IEEE Computational Intelligence Society (CIS) Travel Grant
---	---	---	--