NARASARAOPETA ENGINEERING COLLEGE (AUTONOMOUS)

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

2025-2026

Batch Number	DG2
Team Members	T.DurgaBhavani (22471A05O6) Sk.Y.Khajabi (22471A05O3) G.Kavya (22471A05M4) A.DeepthiPriya (23475A0513)
Guide	DR.K.Suresh Babu M.Tech
Title	Detecting Unbalanced Network Traffic Intrusion With Deep Learning
Domain/Technology	DEEP LEARNING
Base Paper Link	https://ieeexplore.ieee.org/document/1053823 2
Dataset Link	https://www.kaggle.com/datasets/naveengill/cicids2017-dataset/code
Software Requirements	Browser: Any latest browser like Chrome Operating System: Windows 7 Server or later Python (COLAB)
Hardware Requirements	SystemType: Intel Core i5 or above RAM: 8 GB Number of cores:5 Number of Threads: 4
Abstract	Intrusion detection systems (IDS) face challenges in detecting malicious network traffic due to class imbalance, where normal traffic overshadows rare attacks. This paper proposes a deep learning-based IDS to address this issue using advanced techniques like focal loss, cost-sensitive learning, and Generative Adversarial Networks (GANs) for generating minority class samples. A Random Forest Regressor is used for feature importance estimation, reducing computational complexity. Transformer-based architectures, such as Vision Transformer and Time-Series Transformer, along with DenseNet and EfficientNet, enhance feature extraction. The system effectively detects both known and novel attacks. Experimental results show improved accuracy and robustness in imbalanced traffic scenarios. This approach offers a promising solution for modern IDS challenges.

Signature of the student(s)   **Signature of the Guide**   **Signature of the project coordinator**