NARASARAOPETA ENGINEERING COLLEGE (AUTONOMOUS)

DEPARTMENTOFCOMPUTERSCIENCEANDENGINEERING

2025-2026

Batch Number	AG6
Team Members	GADDAM MEGHANA (22471A0518) DARLA DIVYA (22471A0515) GADDIPATI KEERTHANA DIVYA (22471A0520)
Guide	Dr. K. Suresh Babu ,M.Tech., Ph.D.,
Title	Effectiveness of an Adaptive Deep Learning-Based Intrusion Detection System
Domain/Technology	DEEP LEARNING
Base Paper Link	https://ieeexplore.ieee.org/document/10778531
Dataset Link	https://www.kaggle.com/datasets/sampadab17/network-intrusion-detection https://www.kaggle.com/datasets/ericanacletoribeiro/cicids2017-cleaned-and-preprocessed
Software Requirements	Browser: Any latest browser like Chrome Operating System: Windows 7 Server or later Python (COLAB)
Hardware Requirements	System Type: Intel Core i5 or above RAM: 8GB Number of cores:6 Number of Threads: 12

Abstract	Cybersecurity is characterized by its dynamism and complexity, with malicious actors continually developing new strategies to evade traditional intrusion detection systems. These systems, while once robust, now often need help to adapt to evolving threat tactics, resulting in a high incidence of false positives and inadequate response capabilities. This scenario presents a critical challenge: how can defenders stay one step ahead of threats without compromising operational efficiency and security effectiveness? The problem is the need for intrusion detection systems that react to known threats and anticipate and adapt to emerging threats in real-time. This work examines the implementation and effectiveness of an adaptive intrusion detection system using deep learning algorithms to strengthen cybersecurity. The research focused on evaluating the system's ability to identify and neutralize cyber threats more efficiently and accurately than traditional methods. Quantitative analysis showed that AIDS significantly improved in several key metrics: precision increased by 12.5%, reaching 90%, while recall enhanced by 13.3%, reaching 85%. Furthermore, the F1-score experienced an increase of 12.9%, settling at 87.5%. Qualitative evaluations complemented these results through case studies and testimonials from IT staff, which corroborated the improvement in the detection and response to security incidents. The results reveal that the adaptive intrusion detection system, with its machine learning approach, not only improves threat detection and management but also optimizes operational efficiency, reducing false positives and accelerating response times.

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