NARASARAOPETA ENGINEERING COLLEGE (AUTONOMOUS)

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

2024-2025

Batch Number	AG7
Team Members	Bojja Sobharani (21471A0509) Gattu Thanuja (21471A0522) Thalapaneni Suma Durga (21471A0564)
Guide	Mothe Sathyam Reddy
Title	Enhancing Cloud Security with Deep Learning - An ANN Approach for Cyber Threat Detection
Domain/Technology	DEEP LEARNING
Base Paper Link	https://www.sciencedirect.com/science/article/pii/S1877050923021671
Dataset Link	https://www.kaggle.com/datasets/mrwellsdavid/unsw-nb15
Software Requirements	Operating System : Windows 11 Coding Language : PYTHON, HTML, CSS, JS, FLASK IDE : Python 2.7.15
Hardware Requirements	SystemType: 64-bit operating system RAM: 8 GB Hard disk:4MB Cache Memory:4GB
Abstract	Due to the increasing role of cloud computing in the growth of trustable digital services, secure and efficient solutions will be a must in the mitigation of cyber risks. This paper presents an approach to the enhancement of cloud security through the application of deep learning, focusing on Artificial Neural Networks. Moderate segments of ANN algorithms have been performed that are Levenberg-Marquardt(LM), Scaled Conjugate Gradient(SCG) and Bayesian Regularization(BR), to build an enhanced threat detection system which has the capability of detecting highly complex attacking patterns in the cloud.The paper also looks at the problem of various types of cyber threat detection - malware, phishing, distributed denial of service (DDos) attacks etc. Finally, it can be concluded that employing the knowledge of ANN, and other, deep learning approaches, can facilitate the development of persistent cyber defense structures in the cloud. The research shows how ANN models can contribute to a faster and easier detection of new, unclassified threats, therefore increasing the overall security of cloud related activities.

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