NARASARAOPETA ENGINEERING COLLEGE (AUTONOMOUS)

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

2025 - 2026

Batch Number	**DG1**
Team Members	G. Keerthana Lazarus(22471A05M5) G. Lakshmi Thirupathamma (22471A05M1) B. JayaBharathi(22471A05L5) Ch. John Wesly(22471A05L8)
Guide	**Dr. R. Sathees Kumar**
Title	**A blockchain based federated deep learning model for secured data Transmission in healthcare IOT networks.**
Domain/Technology	DEEP LEARNING
Base Paper Link	**https://doi.org/10.1016/j.measen.2024.101176**
Dataset Link	**https://www.kaggle.com/datasets/faisalmalik/iot-healthcare-security-dataset**
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: 8 GB Number of cores:5 Number of Threads: 4
Abstract	**The wide use of sensors in healthcare applications has made it necessary to have secure communication in healthcare Internet of Things (IoT) networks. The sensor data is sensitive, and can contain extremely confidential information such as medical diagnosis, clinical records, vital signs and health data of patients. The emergence of blockchain as a technology ensures consensus and trust among systems, and is now considered to be a new trend used to achieve high scalability, data integrity and privacy. Federated learning is a new technology based on distributed learning that exploits the concept of trust. In federated learning, each user builds an individual distributed model to help a central server that is accessible only to a trusted user group. This paper harnesses the potential of these approaches and proposes an attack detection model to discern normal user behaviours from that of adversaries in an IoT network. This model is called the Blockchain enabled Federated Learning model for secured communication in healthcare IoT (BFL-hIoT), to secure data in healthcare IoT networks. This model is trained and tested on a standard dataset and demonstrates the highest classification accuracy of 97.16 % for normal, 0.9546 for backdoors, 0.9618 for XSS etc., outperforming other blockchain and deep learning models.**

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