CVR COLLEGE OF ENGINEERING

(An UGC Autonomous Institute, Accredited by NAAC with 'A' Grade)

Department of Computer Science and Engineering

List of Journals Referred Relevant to Seminar Topic

Name of the Student : RAYARAKULA VISHNUVARDHAN

Section: CSE - B

Roll Number : 20B81A05B9

Date: 12.12.2023

S. No	Journal Details	
1	Title of Journal	Distributed Denial of Service Attack Detection for the Internet of Things Using Hybrid Deep Learning Model
	Publisher	IEEE
	Web Site	https://ieeexplore.ieee.org/document/10295488
	Electronic ISSN	2169-3536

Signature of the student

CVR COLLEGE OF ENGINEERING

(An UGC Autonomous Institute, Accredited by NAAC with 'A' Grade)

Department of Computer Science and Engineering

Area: Deep Learning

Abstract

Title**: Distributed Denial of Service Attack Detection for the Internet of Things Using Hybrid Deep Learning Model**

Deep learning is a subset of machine learning which uses deep neural networks to understand and make sense of complex data, excelling in tasks like image recognition and language understanding.

This study focuses on the critical issue of DDoS attacks in the Internet of Things (IoT) environment, proposing a novel approach for detection. The focus is on leveraging a hybrid deep learning model, incorporating Convolutional Neural Networks (CNN), Long Short-Term Memory (LSTM), and Autoencoder to enhance detection capabilities.

The study explores related works in the field, highlighting a novel sub-model structure that incorporates 2D CNNs, LSTM, and autoencoders. The training process involves iterative refinement, aiming to detect low-frequency and closely similar attacks efficiently. The proposed model is benchmarked against well-known classifiers, showcasing superior True Positive Rates and global metrics.

The model utilizes a combination of deep neural networks, including CNN, LSTM, and autoencoder, to exploit their diverse characteristics for effective DDoS detection. The proposed training algorithm iteratively refines sub-models, enhancing the capability to detect specific attack types that are challenging to identify.

Future work involves exploring hyperparameter optimization and feature selection to further enhance the performance of the proposed model. Additionally, transfer learning is considered for model updating, ensuring adaptability to evolving attack scenarios. The study demonstrates not only superior detection rates but also reasonable processing times, enabling real-time DDoS attack detection in IoT environments.

Name: Rayarakula Vishnuvardhan

Section: CSE-B

Roll No: 20B81A05B9