



FONSAC 2023

University Auditorium,
IBB University, Lapai,
Niger State.
16th -19th October, 2023

FACULTY OF NATURAL SCIENCES
IBRAHIM BADAMASI BABANGIDA UNIVERSITY LAPAI

3rd FACULTY OF NATURAL SCIENCES ANNUAL CONFERENCE



— *Theme* —

**Scientific Research for Smart,
Secure and Sustainable Future**

*Book of
Abstracts*

**DISTRIBUTED DENIAL OF SERVICE ATTACK DETECTION
TECHNIQUE BASE ON ARTIFICIAL NEURAL NETWORKS:
SYSTEMATIC LITERATURE REVIEW**

Abdul-karim Baba Oshoma, Morufu Olalere, Ismaila Idris, Joseph Adebayo Ojeniyi,
Abdulkadir Onivehu Isah
Department of Cyber Security science, Federal University of Technology, Minna

Abstract

Distributed Denial of Service attacks (DDoS) are one of the biggest security problems facing the Internet. Detecting and mitigating such attacks is challenging to users and cyber security researcher that requires effective techniques which can accurately identify the attack traffic and distinguish it from legitimate traffic. Artificial Neural Network is among the most popular techniques for preventing distributed denial-of-service (DDoS) attacks on any kind of network. To reach out the objective, we conducted a systematic literature review based on the method use to provide the best performances and evidence in artificial neural network technique applications which includes an analysis of the preparation techniques, advantages, and different types of attacks used in various datasets and also looked for publications that used artificial neural network (ANN) approaches to identify DDoS attacks. To search the contemporary literature, we have extensively utilized a number of digital libraries (including IEEE, ACM, Springer, and other digital libraries) and one academic search engine (Google Scholar). The result show that, the accuracy rate reported in much of the literature is over 99%. Because the majority of these studies assessed their models using offline data analysis for evaluation and comparison. We conclude from this review that the most commonly used ANN techniques are RNN 99%, CNN 89% - 90%, LSTMs 85.19%, FNN 80%, GAN 75% and SOM 70% for data analysis and evaluation. Another conclusion of this review relates to performance metrics. Of the reviewed studies, 29 employed accuracy measurements for evaluating their techniques, compared to 22 studies each using the precision, recall, and F1-score metrics and six studies each using the FPR and AUC metrics. Thus, the paper is expected to benefit academicians and researchers in developing an efficient solution for the artificial neural network mentioned above in detecting DDoS attacks.