Avinashilingam Institute for Home Science and Higher Education for Women
(Deemed to be University Estd. u/s 3 of UGC Act 1956, Category A by MHRD)
Re-accredited with 'A++' Grade by NAAC.CGPA 3.65/4, Category I by UGC
Coimbatore – 641 043, Tamil Nadu, India

PLAGIARISM CHECK REPORT (THESES)

1.	Name of the Research Scholar	M. Kalaivani
2.	Roll No. and Year of Registration	18PHCSP005, 2018
3.	Department	Computer Science
4.	Name of the Research Guide	Dr. G. Padmavathi
5.	Title of the Thesis / Dissertation	Complexity Aware Intelligent Intrusion Detection for DDoS Attacks
6.	Similarity Content (%) Identified	**5%**
7.	Software Used	Turnitin
8.	Date of Verification	18-01-2025

Note : The report is excluding 14 Consecutive words, Review of Literature and Quoted Materials.

Checked by :

18/1/25
Information Scientist

18/1/25
Research Scholar

18.01.25
Assistant Librarian

18/1/25
Research Guide

Date: 18-01-2025

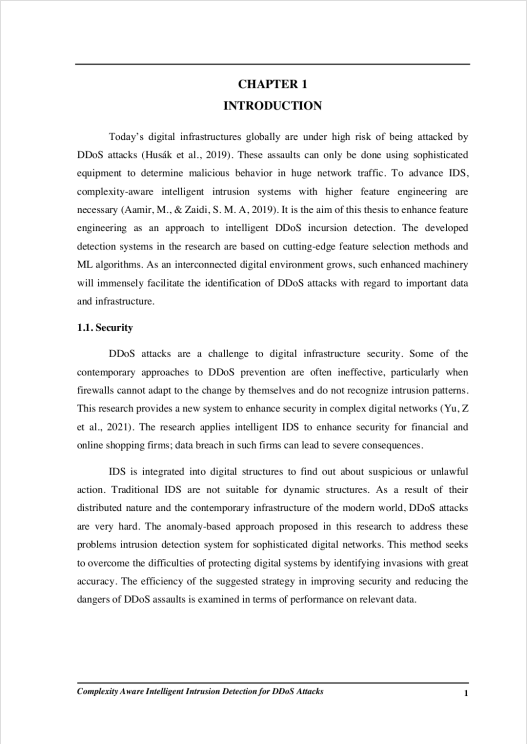
Dr. G.PADMAVATHI
M.Sc.,M.Phil.,Ph.D.,MISTE.,MCSI.,
Dean, School of Physical Science and Computational Sciences
Avinashilingam Institute for Home Science and Higher Education for Women
(Deemed to be University)
Coimbatore - 641 043

Digital Receipt

This receipt acknowledges that Turnitin received your paper. Below you will find the receipt information regarding your submission.

The first page of your submissions is displayed below.

Submission author:	Central Library Avinashilingam
Assignment title:	Paper 2024
Submission title:	Complexity Aware Intelligent Intrusion Detection for DDoS A...
File name:	exity_Aware_Intelligent_Intrusion_Detection_for_DDoS_Attack...
File size:	5.64M
Page count:	125
Word count:	26,096
Character count:	149,495
Submission date:	18-Jan-2025 02:48PM (UTC+0530)
Submission ID:	2333625884



CHAPTER 1
INTRODUCTION

Today's digital infrastructures globally are under high risk of being attacked by DDoS attacks (Husák et al., 2019). These assaults can only be done using sophisticated equipment to determine malicious behavior in huge network traffic. To advance IDS, complexity-aware intelligent intrusion systems with higher feature engineering are necessary (Aamir, M., & Zaidi, S. M. A, 2019). It is the aim of this thesis to enhance feature engineering as an approach to intelligent DDoS incursion detection. The developed detection systems in the research are based on cutting-edge feature selection methods and ML algorithms. As an interconnected digital environment grows, such enhanced machinery will immensely facilitate the identification of DDoS attacks with regard to important data and infrastructure.

1.1. Security

DDoS attacks are a challenge to digital infrastructure security. Some of the contemporary approaches to DDoS prevention are often ineffective, particularly when firewalls cannot adapt to the change by themselves and do not recognize intrusion patterns. This research provides a new system to enhance security in complex digital networks (Yu, Z et al., 2021). The research applies intelligent IDS to enhance security for financial and online shopping firms; data breach in such firms can lead to severe consequences.

IDS is integrated into digital structures to find out about suspicious or unlawful action. Traditional IDS are not suitable for dynamic structures. As a result of their distributed nature and the contemporary infrastructure of the modern world, DDoS attacks are very hard. The anomaly-based approach proposed in this research to address these problems intrusion detection system for sophisticated digital networks. This method seeks to overcome the difficulties of protecting digital systems by identifying invasions with great accuracy. The efficiency of the suggested strategy in improving security and reducing the dangers of DDoS assaults is examined in terms of performance on relevant data.

Complexity Aware Intelligent Intrusion Detection for DDoS Attacks 1

Complexity Aware Intelligent Intrusion Detection for DDoS Attacks

by Central Library Avinashilingam

Submission date: 18-Jan-2025 02:48PM (UTC+0530)
Submission ID: 2333625884
File name: exity_Aware_Intelligent_Intrusion_Detection_for_DDoS_Attacks.doc (5.64M)
Word count: 26096
Character count: 149495

Complexity Aware Intelligent Intrusion Detection for DDoS Attacks

ORIGINALITY REPORT

5%	3%	4%	1%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	jwcn-eurasipjournals.springeropen.com Internet Source	<1%
2	thesai.org Internet Source	<1%
3	link.springer.com Internet Source	<1%
4	M. Kalaivani, G. Padmavathi. "Panthera Leo Optimized Multilayer Feed Forward Learning-Based Intrusion Detection Model for Cloud", SN Computer Science, 2023 Publication	<1%
5	www.frontiersin.org Internet Source	<1%
6	eitca.org Internet Source	<1%
7	www.hdpublication.com Internet Source	<1%
8	doaj.org Internet Source	