

# CONTENTS

<b>Chapter No</b>	<b>Title</b>	<b>Page No.</b>
	Abbreviations	xvii
	Abstract	xix
<b>1</b>	<b>Introduction</b>	<b>1</b>
	1.1 Security	1
	1.2 Cyber Security Challenges	2
	1.3 Types of Attacks	3
	1.4 Denial of Service Attacks	4
	1.5 Distributed Denial of Service Attacks	4
	1.5.1 DDoS Attack Types	6
	1.5.1.1 Flooding/Volume-Based Attacks	6
	1.5.1.2 Protocol-Based Attacks	7
	1.5.1.3 Attacks at the Application Layer	7
	1.5.2 DDoS Attack Vector Classification	8
	1.5.2.1 Single Vector DDoS Flooding attack	9
	1.5.2.2. Multi Vector DDoS Flooding Attack	9
	1.6 Methods to handle Cyber Attacks	10
	1.6.1 Intrusion Detection System	11
	1.6.1.1 Signature-based IDS (SIDS)	12
	1.6.1.2 Anomaly-based IDS (AIDS)	12
	1.6.1.3 Deployment Based IDS	12
	1.6.1.4 IDS based on hosts	12
	1.6.1.5 IDS based on networks	13
	1.6.2 Hybrid Deep Learning Detection Method	13
	1.7 Motivation and Justification	13
	1.8 Problem Statement	17
	1.9 Research Questions	17
	1.10 Objectives of Thesis	17
	1.11 Significant Thesis Contributions	18

<b>Chapter No</b>	<b>Title</b>	<b>Page No.</b>
	1.12 Organization of Thesis	20
	1.13 Chapter Summary	21
<b>2</b>	<b>Literature Review</b>	23
	2.1 Introduction	23
	2.2 Literature on various approaches in DDOS detection	23
	2.3 Literature on various IDS in Intrusion Detection	27
	2.4 Literature on Various Datasets used in Intrusion detection	30
	2.5 Literature on various Feature Selection (FS) Methods	32
	2.6 Literature on various Computational Intelligence Techniques in Intrusion Detection	36
	2.7 Observations and Critical Analysis Based on Literature	40
	2.8 Chapter Summary	42
<b>3</b>	<b>Proposed Methodology</b>	43
	3.1 Introduction	43
	3.2 Steps Involved in the Proposed Methodology	43
	3.3 Research Design	50
	3.4 Chapter Summary	51
<b>4</b>	<b>Ensemble Based Combined Filter for Feature Selection (CFFS) With Decision Tree (DT) Classifier for Single Vector DDoS Flooding Attacks Detection</b>	52
	4.1 Introduction	52
	4.2 Proposed Methodology in Phase I	53
	4.2.1 Benchmark Dataset	55
	4.2.2 Data Pre-Processing	55
	4.2.3 Ensemble-based Combined Filter for Feature Selection	56
	4.2.3.1 Information Gain (IG)	57
	4.2.3.2 Gain Ratio	57
	4.2.3.3 Chi-Square	58
	4.2.3.4 ReliefF	58
	4.2.3.5 Pseudocode for proposed combined filter for feature selection method	59
	4.3 Steps involved in Proposed Approach	60
	4.3.1 Pseudocode for Decision Tree and SVM Classifier	60

<b>Chapter No</b>	<b>Title</b>	<b>Page No.</b>
	4.4 Experimental Results and Discussion	63
	4.5 Chapter Summary	74
<b>5</b>	<b>Feature Engineering Techniques with Hybridization of Improved Dragonfly Optimization Algorithm (IDOA) And Decision Tree Classification (DT) For Multi-Vector DDoS Flooding Attacks Detection</b>	76
	5.1 Introduction	76
	5.2 Proposed Framework and Approach	77
	5.2.1 Data Set	79
	5.2.2 Enhanced Feature Engineering and Extraction using Improved Dragonfly Optimization Algorithm (DOA)	80
	5.2.2.1 Improved Dragonfly Optimization Algorithm	84
	5.3 Decision Tree Classifiers for Training and Testing	86
	5.4 Validation	87
	5.4.1 Performance Evaluation	88
	5.5 Experimental Results and Discussion	88
	5.6 Chapter Summary	99
<b>6</b>	<b>Panthera Leo Optimized Multilayer Feed Forward Learning for Multiple DDoS Attack Detection</b>	101
	6.1 Introduction	101
	6.2 Proposed Framework and approach	102
	6.2.1 Dataset	104
	6.2.2 Feature Extraction (Panthera Leo Optimization technique – PLO)	104
	6.2.3 Proposed Model Training and Testing	109
	6.3 Experimental Setup	110
	6.4 Experimental Results and Discussion	110
	6.5 Chapter Summary	120
<b>7</b>	<b>Attention Enabled Gated Recurrent Network (AEGRN) and Deep Feed Forward Networks for Detecting DDoS Attacks In Multiple Datasets</b>	121
	7.1 Introduction	121
	7.2 Proposed Methodology	122
	7.3 Materials and Methods	124

<b>Chapter No</b>	<b>Title</b>	<b>Page No.</b>
	7.4 Data Reorganizing	124
	7.5 Self-Attention Gated Recurrent Networks for Feature Extraction	125
	7.5.1 Gated Recurrent Units	125
	7.5.2 Self-Awareness Maps	126
	7.5.3 Feature Extraction Proposal	126
	7.5.4 Deep Feed Forward Network	127
	7.6 Experimentation Details	130
	7.7 Performance Metrics	130
	7.8 Results and Discussion	131
	7.9 Chapter Summary	139
8	<b>Statistical Validation and Proposed Model Comparison in DDoS Attack Detection</b>	140
9	<b>Summary, Conclusion and Future Work</b>	150
	9.1 Summary and Conclusion	150
	9.2 Future Scope	153
	9.3 Real-World Applicability: Case Studies and Practical Insights	153a
	<b>References</b>	154
	<b>Publications</b>	169
	<b>Plagiarism Report</b>	170