

CONTENTS

Chapter No	Title	Page No
1	Introduction	
	1.1 Introduction	1
	1.2 Zero-Day Attacks	3
	1.2.1 Lifecycle of Zero-Day Attack	4
	1.3 Zero-Day Attacks in Cloud Environment	5
	1.3.1 Why Zero-day Attacks are Especially Dangerous in Cloud Environments	5
	1.3.2 Common Zero-day Attack Vectors in Cloud	6
	1.3.3 Preventing and Detecting Zero-Day Attacks in Cloud	6
	1.3.4 Classifications of Zero-day Attack	7
	1.3.5 Extended Scope of Zero-Day Attacks beyond Software	9
	1.3.6 Recent Statistics of Zero-day Attacks	10
	1.4 Zero-Day Attack Handling Mechanisms	12
	1.5 Motivation and Justification	14
	1.6 Problem Statement	15
	1.7 Research Questions	15
	1.8 Research Objectives	16
	1.9 Significant Contributions of the Thesis	17
	1.10 Justification based on Proposed Methodology	18
	1.10.1 Justification for Multi-Phase Execution	18
	1.10.2 Justification for Using Quantitative Measures as Expected Outcomes	19
	1.10.3 Application and Attack Discovery Justification	19
	1.10.4 How Attacks Are Detected Across Phases	20
	1.11 Thesis Organization	21
	1.12 Chapter Summary	23
2	Review of Literature	
	2.1 Introduction	24
	2.2 Review of Cloud Attacks	24

Chapter No	Title	Page No
	2.3 Review of Zero-Day Attacks	30
	2.3.1 Review of Zero-day Attacks in Path Identification	31
	2.3.2 Review of Zero-day Attacks in Prediction	35
	2.3.3 Review of Zero-day Attacks in Detection	40
	2.3.4 Review of Methods applied to Enhance zero-Day Attack Analysis	43
	2.4 Observations due to Literature	48
	2.5 Research Challenges and Gaps Identified	49
	2.6 Phase-Wise Literature Mapping and Comparison	51
	2.7 Chapter Summary	53
3	Research Methodology	
	3.1 Introduction	54
	3.2 Steps Involved in the Proposed Methodology	55
	3.3 Research Design	58
	3.3.1 Contribution 1: Zero-Day Attack Path Identification using Enhanced BPNN with CloudSim	60
	3.3.2 Contribution 2: Zero-Day Attack Prediction Using Game Theory	60
	3.3.3 Contribution 3: Zero-Day Attack Prediction and Detection using ResNet50 with Bi-LSTM	61
	3.3.4 Contribution 4: Comparative Analysis on Prediction of Zero-Day Attack	61
	3.4 Thesis Order Justification	62
	3.5 Chapter Summary	62
4	Dataset Description	
	4.1 Introduction	64
	4.2 Dataset 1: Path Dataset	64
	4.2.1 Description	64
	4.2.2 Path Dataset Simulation Details	65
	4.3 Dataset 2: Attack Dataset	66
	4.3.1 Description	66

Chapter No	Title	Page No
	4.3.2 Dataset Generation Process	67
	4.4 Justification for Using Both Datasets	69
5	Zero-Day Attack Path Identification Using Probabilistic and Graph Approach-Based Back Propagation Neural Network in Cloud	
	5.1 Introduction	71
	5.2 Dataset Justification and Simulation Approach	72
	5.3 Key Defense Measures	73
	5.4 Ground Works On Zero-Day Path Identification	75
	5.5 Proposed Methodology	75
	5.5.1 Algorithms	78
	5.5.2 High Probability Tuning Parameter (Threshold)	88
	5.6 Experimental Setup and Results	89
	5.6.1 Simulated Experiment	89
	5.6.2 Performance Metrics	90
	5.6.3 Percentage Improvement of Proposed Work	92
	5.7 Chapter Summary	94
6	Enhancing Zero-Day Attack Prediction a Hybrid Gam Theory Approach with Neural Networks	
	6.1 Introduction	95
	6.2 Proposed Methodology	96
	6.2.1 Zero-Day Attack Prediction	99
	6.2.2 Dataset Description	101
	6.2.3 Autoencoder for Feature Compression	102
	6.2.4 Modified Bi-LSTM for Attack Path Prediction	103
	6.2.5 Hybrid Game-Theoretic Modeling for Zero-Day Defense	108
	6.2.6 Hybrid Integration Strategy	114
	6.3 Experimental Setup and Results	117
	6.3.1 Simulated Experiment	117
	6.3.2 Comparison with Existing Methods for Zero-Day Attack Prediction	126

Chapter No	Title	Page No
	6.3.3 Performance Metrics	126
	6.3.4 Analysis of Results and Discussions	127
	6.3.5 Performance Improvement Table – Proposed Vs Existing Methods	131
	6.3.6 Justification for Modified Bi-LSTM and Hybrid Game Theory with Autoencoder	134
	6.4 Chapter Summary	135
7	ResNet50 Based Deep Convolutional Neural Network for Zero-Day Attack Prediction and Detection	
	7.1 Introduction	136
	7.2 Proposed Methodology	138
	7.2.1 Robustness against Adversarial Evasion	140
	7.2.2 Zero-Day Attack Prediction and Detection	140
	7.2.3 Justification of Methods used in Prediction and Detection Process	143
	7.2.4 Data Pre-Processing	143
	7.2.5 Feature Engineering Module	144
	7.2.6 Training with LSTM and ResNet50	146
	7.2.7 Applying with ResNet	148
	7.2.8 Classifications using ML	150
	7.2.9 Final Prediction and Detection using DC-nZDASN	152
	7.3 Experimental Setup and Results	152
	7.3.1 Simulated Experiment	154
	7.3.2 Performance Metrics	155
	7.3.3 Analysis of Results and Discussions	158
	7.4 Computational Expenses	164
	7.5 Chapter Summary	165
8	Enhancing Cyber Defense against Zero-Day Attacks using Ensemble Neural Networks	
	8.1 Introduction	167
	8.2 Proposed Methodology	168

Chapter No	Title	Page No
	8.2.1 Datasets Description	169
	8.2.2 Data Preprocessing and Feature Engineering	169
	8.2.3 Zero-Day Attack Prediction Model	170
	8.2.4 Hybrid Ensemble Framework	171
	8.2.5 Comparative Analysis of ZDA Prediction using Optimization	176
	8.2.6 Integration of Models for Enhanced Cyber Defence	179
	8.3 Experimental Setup and Results	181
	8.3.1 Performance Metrics	181
	8.3.2 Results and Analysis	182
	8.4 Comparison of Existing Works	190
	8.5 Chapter Summary	192
9	Summary And Conclusion	
	9.1 Summary of Contributions	193
	9.1.1 Phase 1 Zero-Day Attack Path Identification	193
	9.1.2 Phase 2 Zero-Day Attack Prediction	193
	9.1.3 Phase 3 Prediction and Detection of ZDA in Real-Time	194
	9.1.4 Phase 4 Optimization of Detection Accuracy	194
	9.2 Overall Summary	194
	9.3 Conclusion	195
10	Future Research Directions	
	10.1 Future Research Directions	196
	Bibliography	198
	Publications	
	Plagiarism Report	
