

TABLE OF CONTENTS

CHAPTER NO	TITLE	PAGE NO
	Abstract	
1	Introduction	1
1.1	Introduction to Insider Threat	2
	1.1.1 Insider	2
	1.1.2 Insider Threat	3
	1.1.3 Classification of Insider Threat	4
1.2	Attack Indicators	9
1.3	Analysis of Different Types of Insider Threat	10
1.4	Potential Consequences of Insiders	11
	1.4.1 Potential Consequences of Intentional Insiders	12
	1.4.2 Potential Consequences of Unintentional Insiders	13
1.5	Problem Justification	15
1.6	Application area of Insider threat Detection and Mitigation	16
1.7	Problem Statement	17
1.8	Objectives of the Thesis	17
1.9	Significant Contributions of the Thesis	17
1.10	Organization of the Thesis	18
1.11	Chapter Summary	19
2	Review of Literature	20
2.1	Introduction	21
2.2	Significant Review on Insider Threat Detection	21
2.3	Significant Review on Insider Threat Mitigation	52
2.4	Research Gaps Identified	69
2.5	Chapter Summary	70
3	Methodology	71
3.1	Introduction	72
3.2	Problem Specification	72

CHAPTER NO	TITLE	PAGE NO
3.3	Overall Methodology	72
	3.3.1 Preprocessing & Insider Detection (P&ID)	74
	3.3.2 Unintentional Insider Mitigation (UIM)	74
	3.3.3 Intentional Insider Mitigation (IIM)	76
3.4	Techniques Proposed & Outcome Achieved	76
3.5	Dataset Used	77
3.6	Tools Used	77
3.7	Chapter Summary	78
4	Phase I-Preprocessing and Insider Detection (P&ID)	79
4.1	Introduction	80
4.2	P&ID Methodology Overview	80
	4.2.1 Dataset	81
	4.2.2 Preprocessing and Insider Detection (P&ID)	86
4.3	Experimental Results	110
	4.3.1 Performance metrics for B-SVM	110
	4.3.2 Elaborative Result Analysis of the P&ID Phase	112
	4.3.3 Comparison of proposed B-SVM with existing methods	118
	4.3.4 Insider Detection using B-SVM	120
4.4	Outcome of Phase I	121
4.5	Limitation of Phase I	121
4.6	Chapter Summary	122
5	Phase II-Unintentional Insider Mitigation (UIM)	123
5.1	Introduction	124
5.2	UIM Methodology Overview	124
	5.2.1 Dataset	126
	5.2.2 Unintentional Insider Mitigation (UIM)	130
5.3	Experimental Results	145
	5.3.1 Performance metrics for DBN	145

CHAPTER NO	TITLE	PAGE NO
	5.3.2 Elaborative result analysis of UIM phase	146
	5.3.3 Comparison of proposed CKPCA-DBN with existing methods	158
	5.3.4 Unintentional Insider Authentication using CKPCA-DBN	159
5.4	Outcome of Phase II	160
5.5	Limitation of Phase II	160
5.6	Chapter Summary	161
6	Phase III-Intentional Insider Mitigation (IIM)	162
6.1	Introduction	163
6.2	IIM Methodology Overview	163
	6.2.1 Dataset preparation	164
	6.2.2 Intentional Insider Mitigation (IIM)	168
6.3	Experimental Results	175
	6.3.1 Performance Metrics for Decision Tree	175
	6.3.2 Elaborative Result Analysis of IIM phase	176
6.4	Outcome of Phase III	182
6.5	Chapter Summary	182
7	Conclusion	183
7.1	Summary and Conclusion	184
8	Future Research Directions	187
8.1	Future Research Directions	188
	References	189
	Annexure I	
	Publications	
	Plagiarism Report	