

CONTENTS

Chapter No.	Title	Page No.
1	Introduction	1
	1.1 Key Aspects of Mobile Devices	2
	1.2 Research Motivation	3
	1.3 Mobile Device and Data Security Challenges	3
	1.4 Threats and Vulnerabilities	4
	1.5 Defensive Mechanisms	9
	1.6 Problem Statement	9
	1.7 Proposed Approaches	10
	1.7.1 Authentication	10
	1.7.2 Malicious Applications	11
	1.7.3 Data Storage	11
	1.7.4 Data Retrieval	11
	1.8 Objectives of the Thesis	12
	1.9 Significant Contributions of the Thesis	12
	1.10 Organization of the Thesis	14
	1.11 Chapter Summary	15
2	Literature Review	16
	2.1 Security Challenges in Mobile Devices	17
	2.2 Defensive Mechanisms	19
	2.2.1 Iris Biometric Authentication	20
	2.2.2 Malware Detection	22
	2.2.3 Outsourcing Data to Cloud Storage	24
	2.2.4 Retrieval of Outsourced Encrypted Data	26
	2.3 Observations due to Literature	28
	2.4 Chapter Summary	29

Chapter No.	Title	Page No.
3	Proposed Methodology	30
	3.1 Steps involved in the Proposed Methodology	31
	3.2 Specific Contributions of the Thesis	34
	3.3 Chapter Summary	37
4	Enhanced Biometric Iris Authentication in Low Powered Resource Constrained Mobile Devices using the Proposed PCA-SVMED Method	38
	4.1 Introduction	39
	4.2 Steps of the Proposed Contribution PCA-SVMED Method	40
	4.2.1 Acquisition and Preprocessing	41
	4.2.1.1 Integro-Differential Operator	41
	4.2.1.2 Rubber-Sheet Model	41
	4.2.2 Feature Extraction and Reduction	42
	4.2.2.1 Color Based Zero Crossing Extraction	42
	4.2.2.2 Principal Component Analysis	44
	4.2.3 Detection and Classification	45
	4.2.3.1 Support Vector Machine with Euclidean Distance	45
	4.3 Flow diagram of the Proposed Contribution One - PCA-SVMED Method	46
	4.4 Steps involved in the Proposed PCA-SVMED Method	48
	4.5 Pseudo Code of PCA-SVMED Method	49
	4.6 Experimental Setup and Results	50
	4.7 Chapter Summary	56
5	Enhanced Permission Based Malware Detection in Mobile Devices Using the Proposed MSGP-MS Method	57
	5.1 Introduction	58

Chapter No.	Title	Page No.
5.2	Steps of the Proposed Contribution Two - MSGP-MS Method	58
5.2.1	Data Collection	60
5.2.2	Permission Extraction and Selection	60
5.2.3	Classification Techniques for Malware Detection	62
5.2.3.1	K-Means Clustering	63
5.2.3.2	J48	63
5.2.3.3	Classification and Regression Tree	64
5.2.3.4	Random Forest	64
5.2.4	Optimization Techniques for Malware Detection	65
5.2.4.1	Genetic Algorithm	65
5.2.4.2	Particle Swarm Optimization	66
5.3	Flow Diagram of the Proposed Contribution Two - MSGP-MS Method	66
5.4	Steps involved in the Proposed MSGP-MS Method	68
5.5	Pseudo Code of MSGP-MS Method	68
5.6	Experimental Setup and Results	71
5.7	Chapter Summary	75
6	Secured Cryptographic Approach for the Outsourced Mobile Device Data over Cloud Storage using the Proposed MSAES Method	76
6.1	Introduction	77
6.2	Steps of the Proposed Contribution Three MSAES Method	77
6.2.1	MSAES Encryption for Uploading Process	78
6.2.1.1	Symmetric Advanced Encryption Standard Algorithm	79
6.2.1.2	Asymmetric Elliptic Curve Cryptography Algorithm	80
6.2.1.3	Asymmetric Rivest Shamir Adleman Algorithm	81

Chapter No.	Title	Page No.
	6.2.1.4 Digital Signature Message Digest Algorithm	82
	6.2.2 MSAES Decryption for Downloading Process	83
	6.3 Flow Diagram of the Proposed Contribution Three - MSAES Method	84
	6.4 Steps involved in the Proposed MSAES Method	86
	6.5 Pseudo Code of MSAES Method	86
	6.6 Experimental Setup and Results	88
	6.7 Chapter Summary	95
7	Efficient Secured Search over Outsourced Encrypted Mobile Device Data in Cloud using the Proposed RFMKS Method	96
	7.1 Introduction	97
	7.2 Steps of the Proposed Contribution Four - RFMKS Method	97
	7.2.1 Pre-Framework phase	98
	7.2.1.1 System Model	99
	7.2.1.2 Threat Model	100
	7.2.1.3 Design Goals	100
	7.2.2 Retrieval Phase	101
	7.2.2.1 Build Index	101
	7.2.2.2 Fuzzy Multi-Keyword Search	101
	7.2.2.3 Rank Retrieval	102
	7.3 Flow Diagram of the Proposed Contribution Four - RFMKS Method	102
	7.4 Steps involved in the Proposed RFMKS Method	104
	7.5 Pseudo Code of RFMKS Method	104
	7.6 Experimental Setup and Results	106
	7.7 Chapter Summary	110

Chapter No.	Title	Page No.
8	Conclusion	111
	8.1 Summary and Conclusions	112
9	Future Directions	114
	9.1 Future Research Directions	115
	References	116
	Annexures	129
	Annexure I	129
	Annexure II	132
	Annexure III	140
	Annexure IV	142
	Publications	143
	Profile	145
