# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>CHAPTER NO.</th>
<th>TITLE</th>
<th>PAGE NO.</th>
</tr>
</thead>
<tbody>
<tr>
<td>ABSTRACT</td>
<td></td>
<td>v</td>
</tr>
<tr>
<td>LIST OF TABLES</td>
<td></td>
<td>xvi</td>
</tr>
<tr>
<td>LIST OF FIGURES</td>
<td></td>
<td>xvii</td>
</tr>
<tr>
<td>LIST OF SYMBOLS AND ABBREVIATIONS</td>
<td></td>
<td>xix</td>
</tr>
</tbody>
</table>

1 INTRODUCTION 1

1.1 CLOUD COMPUTING: AN OVERVIEW 1
  1.1.1 Characteristics of Cloud Computing 2
  1.1.2 Service Models of Cloud Computing 3
  1.1.3 Deployment Models of Cloud Computing 5
  1.1.4 Key Benefits of Cloud Computing 6
  1.1.5 Barriers to Cloud Computing Adoption 6

1.2 CLOUD DATA SECURITY CHALLENGES 7
  1.2.1 International Data Corporation (IDC) 8
  1.2.2 Cloud Security Alliance (CSA) 9
  1.2.3 Amazon Web Services (AWS) 10

1.3 MOTIVATION 12

1.4 PROBLEM STATEMENT 13
  1.4.1 System Model 13
  1.4.2 Problem Definition 15
  1.4.3 Research Objectives 16
  1.4.4 Scope 17

1.5 CONTRIBUTIONS OF THE THESIS 17

1.6 ORGANIZATION OF THE THESIS 18
# 2 LITERATURE REVIEW

2.1 INTRODUCTION  
2.2 SYMMETRIC KEY ALGORITHMS  
2.3 PUBLIC KEY ALGORITHMS  
2.4 HASH ALGORITHMS  
2.5 ELLIPTIC CURVE CRYPTOGRAPHY ALGORITHM  
2.6 AUTHENTICATION AND ACCESS CONTROL  
2.7 DIGITAL MULTI-SIGNATURE  
2.8 PROVABLE DATA POSSESSION PROTOCOL  
2.9 OPENSTACK CLOUD OPERATING SYSTEM  
2.10 RESEARCH GAP  
2.11 SUMMARY

# 3 AN ADAPTIVE MULTILEVEL SECURITY FRAMEWORK TO SECURE CLOUD DATA

3.1 INTRODUCTION  
3.2 OUTSOURCING DATA TO CLOUD STORAGE  
3.3 SECURITY CHALLENGES TO DATA STORED IN CLOUD ENVIRONMENT  
3.4 SECURITY MEASURES TO PROTECT DATA OUTSOURCED TO CLOUD STORAGE  
3.4.1 Access Control  
3.4.2 Data Encryption  
3.4.3 Integrity Verification  
3.4.4 Log Analysis  
3.4.5 Data Classification  
3.4.5.1 Data Sensitivity  
3.4.5.2 Classification Plan  
3.4.5.3 Data Segmentation
3.5 AN ADAPTIVE MULTILEVEL SECURITY (AMLS) FRAMEWORK TO SECURE DATA STORED IN CLOUD ENVIRONMENT

3.5.1 Overview of Adaptive Multilevel Security Framework

3.5.1.1 Preprocessing Phase (P)

3.5.1.2 Setup Phase (S)

3.5.1.3 Data Accessing Phase (D)

3.5.1.4 Key Management Phase (K)

3.5.1.5 Data Integrity Verification Phase (I)

3.5.1.6 Log Analysis Phase (L)

3.5.1.7 Token Verification Phase (T)

3.5.2 High Security Scheme for High Sensitive Class I Data

3.5.3 Medium Level Security Scheme for Moderate Sensitive Class II Data

3.5.4 Base Level Security Scheme for Low Sensitive Class III Data

3.5.5 Security Analysis

3.6 IMPLEMENTATION AND RESULTS

3.6.1 OpenStack Private Cloud

3.6.2 Performance Analysis of Cryptographic Algorithms

3.7 CONCLUSION

4 ECC BASED ADAPTIVE AND SECURE ACCESS PROTOCOL FOR CLOUD DATA

4.1 INTRODUCTION
4.2 REVIEW OF LIN ET AL. AND ZHU ET AL.’S AUTHENTICATION SCHEME 65
4.3 ECC BASED ADAPTIVE AND SECURE ACCESS PROTOCOL (ECC-ASAP) 68
  4.3.1 Preliminaries 68
  4.3.2 Setup Phase 71
  4.3.3 Registration Phase 72
  4.3.4 Authentication Phase 73
  4.3.5 Token Distribution Phase 74
  4.3.6 Key Generation Phase 76
  4.3.7 Key Derivation Phase 76
4.4 SECURITY AND PERFORMANCE ANALYSIS 77
  4.4.1 Security Analysis 77
    4.4.1.1 Masquerade Attack 77
    4.4.1.2 Replay Attack 79
    4.4.1.3 Impersonation Attack 80
    4.4.1.4 Insider Attack 80
  4.4.2 Performance Analysis 82
4.5 CONCLUSION 83

5 EFFICIENT AND SECURE ECC BASED DIGITAL MULTI-SIGNATURE PROTOCOL 85
5.1 INTRODUCTION 85
5.2 ECC BASED DIGITAL MULTI-SIGNATURE (ECC-DMS) PROTOCOL 86
  5.2.1 Setup Phase 87
  5.2.2 Key Generation Phase 87
  5.2.3 Multi-Signature Generation Phase 88
  5.2.4 Multi-Signature Verification Phase 89
6 ECC BASED PROVABLE DATA POSSESSION PROTOCOL WITH DATA DYNAMICS FOR SECURE CLOUD DATA STORAGE

6.1 INTRODUCTION
6.2 SYSTEM MODEL
   6.2.1 Cloud Data Storage Overview
   6.2.2 Security Attacks
   6.2.3 Design Goals

6.3 EFFICIENT ECC BASED PROVABLE DATA POSSESSION (ECC-PDP) PROTOCOL WITH DATA DYNAMICS
   6.3.1 Pre-Processing Phase
   6.3.2 Key Generation Phase
   6.3.3 Tag Generation Phase
   6.3.4 Challenge Generation Phase
   6.3.5 Proof Generation Phase
   6.3.6 Proof Verification Phase

6.4 DATA DYNAMICS
   6.4.1 Block Insertion
   6.4.2 Block Modification
   6.4.3 Block Deletion
   6.4.4 Process Update Request

6.5 SECURITY AND PERFORMANCE ANALYSIS