# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>CHAPTER NO.</th>
<th>TITLE</th>
<th>PAGE NO</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>ABSTRACT</td>
<td>iii</td>
</tr>
<tr>
<td></td>
<td>LIST OF TABLES</td>
<td>xiii</td>
</tr>
<tr>
<td></td>
<td>LIST OF FIGURES</td>
<td>xiv</td>
</tr>
<tr>
<td></td>
<td>LIST OF SYMBOLS AND ABBREVIATIONS</td>
<td>xix</td>
</tr>
<tr>
<td>1</td>
<td>INTRODUCTION</td>
<td>1</td>
</tr>
<tr>
<td>1.1</td>
<td>CLOUD COMPUTING</td>
<td>1</td>
</tr>
<tr>
<td>1.1.1</td>
<td>Introduction to Cloud Computing</td>
<td>1</td>
</tr>
<tr>
<td>1.1.2</td>
<td>Cloud Characteristics</td>
<td>5</td>
</tr>
<tr>
<td>1.1.3</td>
<td>Cloud Service Models</td>
<td>6</td>
</tr>
<tr>
<td>1.1.4</td>
<td>Cloud Deployment Models</td>
<td>6</td>
</tr>
<tr>
<td>1.1.5</td>
<td>Virtualization and Hypervisor</td>
<td>7</td>
</tr>
<tr>
<td>1.1.6</td>
<td>Cloud Architecture</td>
<td>9</td>
</tr>
<tr>
<td>1.1.7</td>
<td>Advantages of Cloud Computing in the Current Scenario</td>
<td>10</td>
</tr>
<tr>
<td>1.2</td>
<td>PROBLEMS IN CLOUD COMPUTING</td>
<td>11</td>
</tr>
<tr>
<td>1.3</td>
<td>CLOUD SECURITY – A CURRENT SCENARIO</td>
<td>12</td>
</tr>
<tr>
<td>1.3.1</td>
<td>Security Scenarios</td>
<td>12</td>
</tr>
<tr>
<td>1.3.2</td>
<td>Regulations</td>
<td>13</td>
</tr>
<tr>
<td>1.3.3</td>
<td>Security Controls</td>
<td>13</td>
</tr>
<tr>
<td>1.3.4</td>
<td>Service Automation</td>
<td>15</td>
</tr>
<tr>
<td>1.4</td>
<td>MOTIVATION FOR THIS RESEARCH WORK</td>
<td>15</td>
</tr>
</tbody>
</table>
1.4 SUMMARY

2 LITERATURE SURVEY

2.1 IMPORTANCE OF SECURITY IN CLOUD COMPUTING

2.2 STATE-OF-THE-ART CLOUD COMPUTING SECURITY TAXONOMIES

2.2.1 Taxonomy#1: Logical Storage Segregation & Multi-tenancy Security Issues

2.2.2 Taxonomy#2: Identity Management Issues

2.2.3 Taxonomy#3: Insider Attacks

2.2.4 Taxonomy#4: Virtualization Issues

2.2.5 Taxonomy#5: Cryptography and Key Management

2.2.6 Taxonomy#6: Governance and Regulatory Compliance Gaps

2.2.7 Taxonomy#7: Insecure APIs

2.2.8 Taxonomy#8: Cloud & CSP Migration Issues

2.2.9 Taxonomy#9: SLA & Trust Management Gaps

2.2.10 Conclusion: State-of-the-art Cloud Computing Security Taxonomies

2.3 CLOUD ARCHITECTURE DESIGN – SECURITY PERSPECTIVES
2.3.1 Data Center or Physical Security 36
2.3.2 Server Security 36
2.3.3 Network Security 37
2.3.4 Application and Platform Security 39
2.3.5 Encryption and Key Management 40
2.3.6 Infrastructure Security 42

2.4 IDENTITY MANAGEMENT IN PRESENT INDUSTRY PERSPECTIVE 43

2.5 ESSENTIALS OF INTRUSION DETECTION SYSTEMS IN DATA AND SYSTEM SECURITY 50

2.6 CLOUD SECURITY AT PRESENT 54
2.6.1 Investigations at NASA 54
2.6.2 Investigations at Intel 56
2.6.3 Investigations at CSA 57
2.6.4 Investigations at HP 58
2.6.5 Investigations at TCS 59
2.6.6 Investigations at Accenture 60

2.7 SUMMARY 61

3 PROBLEM FORMULATION 63
3.1 MAIN OBJECTIVE 63
3.2 SPECIFIC OBJECTIVES 63
3.2.1 eCloudIDS Objective 1: Logical storage segregation and multi-tenancy security issues 64
3.2.2 eCloudIDS Objective 2: Identity management issues 65
3.2.3 eCloudIDS Objective 3: Insider attacks 65
3.2.4 eCloudIDS Objective 4: Virtualization issues 66
3.2.5 eCloudIDS Objective 5: Cloud VM auditor management issues 66
3.2.6 eCloudIDS Objective 6: Hacker attacks 66
3.2.7 eCloudIDS Objective 7: Signature based attacks caused by Worms, Viruses, Trojans, etc. 67

3.3 SUMMARY 67

4 METHODOLOGY 68
4.1 INTRUSION DETECTION SYSTEM 68
  4.1.1 Types of IDS 74
  4.1.2 Role of IDS in Infrastructure Security 77
  4.1.3 Attacks Commonly Detected by IDSs 78
  4.1.4 Limitations of Intrusion Detection System 78
4.2 MACHINE LEARNING 80
  4.2.1 Types of Machine Learning Algorithms 83
  4.2.2 Supervised Machine Learning Algorithms 86
  4.2.3 Unsupervised Machine Learning Algorithms 89
4.3 IDENTITY MANAGEMENT 92
  4.3.1 Digital Identity Lifecycle 92
  4.3.2 Access-Control Lists 94
4.3.3  Components of Identity Management  96
4.3.4  Identity Management Objectives 97
4.3.5  Role of Identity Management in Cloud Environment 98

4.4  SUMMARY 100

5  eCloudIDS GENERIC CLOUD SECURITY FRAMEWORK 101
5.1  INTRODUCTION 101
5.2  NEED FOR THIS INVESTIGATION 103
5.3  ESSENTIALS OF THIS SYSTEM ARCHITECTURE 104
5.4  eCloudIDS – SYSTEM ARCHITECTURE 105
   5.4.1  eCloudIDS C3 Subsystem 106
   5.4.2  CIM Subsystem 107
   5.4.3  H-log-H Subsystem 107
   5.4.4  Audit Log Preprocessor (ALP) Subsystem 108
   5.4.5  eCloudIDS uX-Engine Tier-1 109
   5.4.6  eCloudIDS sX-Engine Tier-2 113
   5.4.7  Warning Level Generator (WLG) Subsystem 115
   5.4.8  Alert System 116
5.5  SUMMARY 117
6 EXPERIMENTATIONS AND RESULTS

6.1 INTRODUCTION

6.2 EXPERIMENTAL SETUP

6.3 PHASE-I EXPERIMENTATION

6.3.1 Syslog Preprocessing

6.3.2 Daemon Log Preprocessing

6.3.3 Xbel Log Preprocessing

6.3.4 Auth Log Preprocessing

6.3.5 ALP’s myfinal.log Preprocessing

6.3.6 Numerical Conversion – Phase-I

6.3.7 Selection Criteria for uX-Engine’s

Unsupervised Machine Learning Algorithm

6.3.8 uX-Engine Experimentation with SOM

6.4 PHASE-II EXPERIMENTATION

6.4.1 Selection Criteria for SVM

6.4.2 Auth Log Preprocessing

6.4.3 Daemon Log Preprocessing

6.4.4 Database Log Preprocessing

6.4.5 Numerical Conversion – Phase-II

6.4.6 sX-Engine Training Phase using SVM in

Phase-II of eCloudIDS

6.4.7 sX-Engine Testing Phase using SVM in

Phase-II of eCloudIDS

6.4.8 Analyzing SVM for Performance and

Operational Efficiency of sX-Engine