

## TABLE OF CONTENTS

CHAPTER NO.	TITLE	PAGE NO.
	<b>ABSTRACT</b>	iii
	<b>LIST OF TABLES</b>	xiii
	<b>LIST OF FIGURES</b>	xiv
	<b>LIST OF ABBREVIATIONS</b>	xviii
<b>1.</b>	<b>INTRODUCTION</b>	<b>1</b>
1.1	CLOUD COMPUTING	1
1.2	CLOUD ARCHITECTURE	1
1.2.1	Cloud Computing Service Architecture	1
1.2.2	Cloud Security	3
1.3	MOTIVATION BEHIND RESEARCH	4
1.4	IMPORTANCE OF RELIABLE ARCHITECTURE	5
1.5	PROBLEMS AND HYPOTHESIS	6
1.6	LITERATURE SURVEY	7
1.6.1	Security Issues in Cloud Model	10
1.6.2	Security Issues in Saas	13
1.6.2.1	Data security	16
1.6.2.2	Network security	17
1.6.2.3	Data locality	18
1.6.2.4	Data integrity	18
1.6.2.5	Data segregation	20
1.6.2.6	Data access	20
1.6.2.7	Authentication and authorization	21
1.6.2.8	Data confidentiality issue	22



<b>CHAPTER NO.</b>	<b>TITLE</b>	<b>PAGE NO.</b>
	1.6.4.5 Amazon web services meets spamhaus	43
	1.6.4.6 Internal breaches	45
	1.6.4.7 Configuration errors	46
1.6.5	Security Issues in PaaS	46
	1.6.5.1 Default application configurations	48
	1.6.5.2 SSL protocol and implementation flaws	49
	1.6.5.3 Insecure permissions on cloud data	49
	1.6.5.4 Authentication, access control and authorization	50
1.6.6	Security Issues in IaaS	52
	1.6.6.1 Impact of deployment model	55
1.6.7	Related Works and Current Security Solutions	57
	1.6.7.1 Application and data transmission security	57
	1.6.7.2 Data storage security	62
1.7	OBJECTIVE OF THE THESIS	63
1.8	ORGANIZATION OF THESIS	67
<b>2.</b>	<b>BASICS OF CLOUD COMPUTING</b>	<b>69</b>
2.1	CLOUD COMPUTING	69
2.2	CORE CONCEPTS OF CLOUD COMPUTING	70
	2.2.1 Service Models	71

<b>CHAPTER NO.</b>	<b>TITLE</b>	<b>PAGE NO.</b>
	2.2.2 Deployment Models	73
2.3	CLOUD COMPUTING DRIVERS	74
2.4	CLOUD COMPUTING BARRIERS	75
2.5	CLOUD COMPUTING Vs OTHER TECHNOLOGIES	76
	2.5.1 Cloud Computing and SOA	77
	2.5.2 Cloud Computing and Grid Computing	77
2.6	SERVICE LEVEL AGREEMENTS	79
2.7	MULTI TENANCY	80
2.8	SECURITY IN CLOUD COMPUTING	81
<b>3.</b>	<b>MULTI-TIER FRAMEWORK FOR PROVIDING APPLICATION SECURITY IN CLOUD ENVIRONMENT</b>	<b>84</b>
3.1	INTRODUCTION	84
3.2	MULTI-TIER SECURITY FRAMEWORK	85
3.3	DYNAMIC TIERS	96
3.4	DEDICATED AND PRIVATE SECURITY	97
3.5	SECURITY OF CLIENT VERSUS SERVICE	99
3.6	DEPLOYMENT	100
<b>4.</b>	<b>IMPLEMENTATION AND RESULTS OF MULTI-TIER FRAMEWORK FOR APPLICATION SECURITY</b>	<b>101</b>
4.1	EXPERIMENTAL SETUP	101
4.2	RESULTS AND DISCUSSION	102
	4.2.1 Positive Tests	102
	4.2.2 Negative Tests	109

<b>CHAPTER NO.</b>	<b>TITLE</b>	<b>PAGE NO.</b>
	4.2.3 Multi-Tier Security Framework vs Current Day Cloud Environment	113
<b>5.</b>	<b>META DATA BASED STORAGE MODEL FOR DATA SECURITY</b>	117
5.1	INTRODUCTION	117
5.2	DISTRIBUTED DATABASE AND FRAGMENTATION	118
5.3	METADATA BASED DATA STORAGE MODEL	120
5.4	THE METHODOLOGY	122
<b>6.</b>	<b>IMPLEMENTATION AND RESULTS OF META DATA BASED STORAGE MODEL FOR DATA SECURITY</b>	131
6.1	IMPLEMENTATION AND COST	131
6.2	RESULTS AND DISCUSSIONS	134
6.3	LIMITATIONS AND CONSIDERATIONS	136
<b>7.</b>	<b>CONCLUSION AND FUTURE WORK</b>	138
7.1	SUMMARY	138
7.2	CONCLUSION	139
7.3	FUTURE WORK	141
	<b>REFERENCES</b>	142
	<b>LIST OF PUBLICATIONS</b>	149
	<b>CURRICULUM VITAE</b>	150

**LIST OF TABLES**

<b>TABLE NO</b>	<b>TITLE</b>	<b>PAGE NO</b>
1.1	Security Challenges in Identity Management (IdM) and Sign-on Process	32
1.2	Cloud Service Deployment Model	56
2.1	Cloud Computing Drivers	75
2.2	Cloud Computing Barriers	76
3.1	Security Levels	91
4.1	Test Setup	101
4.2	Performance data of the multi-tier security framework with different number of tiers and different sizes of data	107
4.3	Advantages of Multi-tier Application Security Framework over Conventional Cloud Security	116
5.1	Metadata information	125
5.2	Metadata information after fragmentation	126
5.3	Segregated Schema	127
5.4	DME_MAPPER Table	129

## LIST OF FIGURES

FIGURE NO	TITLE	PAGE NO
1.1	Cloud Computing Architecture	3
1.2	Complexity of Security in Cloud Environment	9
1.3	Security for the SaaS stack	14
1.4	Example of the separation of security concerns between a PaaS customer and provider. Note that there is some overlap where the two meet	33
1.5	Code snippet with a well-defined interface between the cloud customer and cloud provider	34
2.1	Cloud Computing Types Based on Capability and Access	71
2.2	Multi-tenancy in private cloud	80
2.3	Multi-tenancy in public cloud	81
3.1	Security Framework	85
3.2	Establishing connection between client and service based on security demand	87
3.3	Communication cycle between client and service using the multi-tier framework (based on the example discussed)	93
4.1	Happy path traces – 1 (Configuration and Connection of Clients with the Applications)	103
4.2	Happy path traces -2 (Signature and Checksum checking of the data by every tier involved in the communication)	104

<b>FIGURE NO</b>	<b>TITLE</b>	<b>PAGE NO</b>
4.3	Happy path traces - 3 (Detection of Security level and subsequently elevating the Security levels)	105
4.4	Happy path traces - 4 (Reconfiguring Client and Application with the elevated security levels)	106
4.5	Performance graph for multitier environment with different number of tiers and data sizes	108
4.6	Metasploit attacks – 1 (Hosting an Exploit with a pay load on the secure session)	109
4.7	Metasploit attacks – 2 (Execution of Exploits on the secure session to create negative scenarios for testing the framework)	110
4.8	Metasploit attacks – 3 (Creating an exploit to do a Man in the Middle Attack on the communication, which provides a negative scenario to the test the framework)	111
4.9	Traces showing the detection of Intrusion created by the Man in the Middle attack hosted by Metasploit	112
4.10	Application Security – Security requirement vs Security provision between present day cloud and multi tier framework	114
4.11	Application Security – % of Users in a group requiring % of Security	115
4.12	Application Security – Costs between present security in cloud and proposed security in cloud	115



<b>FIGURE NO</b>	<b>TITLE</b>	<b>PAGE NO</b>
5.1	Data Fragmentation	121
6.1	Performance between normal and fragmented environment	136

## LIST OF ABBREVIATIONS

ACID	-	Atomicity, Consistency, Isolation and Durability
AD	-	Active Directory
ADRW	-	Adaptive data replication algorithm
Amazon EC2	-	Amazon Elastic Compute Cloud
API	-	Application programming interfaces
AWS	-	Amazon Web Services
BEP	-	Bureau of Engraving and Printing
BPaaS	-	Business Process as a Service
CBK	-	Common Body of Knowledge
CIA	-	Confidentiality, integrity and availability
CISSP	-	Certified Information System Security Professional
CoD	-	Computing on Demand
CRM	-	Customer Relationship Management
CSA	-	Cloud Security Alliance
CSRF	-	Cross Site Request Forgery
DDos	-	Distributed Denial of Service
DR	-	Disaster Recovery
ECPA	-	Electronic Communications Privacy Act
ESB	-	Enterprise Service Bus
FISMA	-	Federal Information Security Management Act
HIP	-	Host Intrusion Prevention
HTTP	-	Hyper Text Transfer Protocol
HTTPS	-	Hyper Text Transfer Protocol Secure
IaaS	-	Infrastructure as Service
ISO	-	International Organization for Standardization
LDAP	-	Lightweight Directory Access Protocol
MITM	-	Man-In-The-Middle
NIST	-	National Institute of Standards and Technology

OWASP	-	Open Web Application Security Project
PaaS	-	Platform as a Service
PCI DSS	-	Payment Card Industry – Data Security Standards
POR	-	Proof of retrievability
RBAC	-	Role based Access Control
REST	-	REpresentational State Transfer
S3	-	Simple Storage Service
SaaS	-	Software as a Service
SAS 70	-	Service Organization Auditing Standards 70
SecaaS	-	Security as a Service
SES	-	Simple Email Service
SETI	-	Search for Extraterrestrial Intelligence
SLA	-	Service Level Agreement
SMB	-	Small and Medium Business
SOA	-	Service Oriented Architecture
SOAP	-	Simple Object Access Protocol
SQL	-	Structured Query Language
SSL	-	Secure Socket Layer
TLS	-	Transport Layer Security
VMM	-	Virtual Machine Monitor