Table of Content

CHAPTER NO	TITLE	PAGE NO
	ABSTRACT	
	LIST OF TABLES	
	LIST OF FIGURES	
	LIST OF ABBREVIATIONS AND SYMBOLS	
1	**INTRODUCTION**	**1**
	1.1. CLOUD FORENSICS	2
	1.1.1. Digital Forensics	4
	1.2. CLOUD FORENSIC INVESTIGATION	6
	1.3. PROCESS OF CLOUD FORENSICS INVESTIGATION	7
	1.3.1. Identification	8
	1.3.2. Collection & Preservation	8
	1.3.3. Examination	8
	1.3.4. Analysis	8
	1.3.5. Reporting & Presentation	8
	1.4. FORENSIC ACQUISITION AND ANALYSIS SYSTEM	9
	1.4.1. Forensic Acquisition and Analysis System for IaaS	9
	1.5. CLOUD COMPUTING EVIDENCE ACQUISITION	11
	1.6. FORENSIC CHALLENGES FACED BY DIGITAL INVESTIGATORS	14
	1.6.1. Data Identification	14
	1.6.2. Time Mismatch	14
	1.6.3. Multi-tenancy	15
	1.6.4. Owner of Data	15
	1.6.5. Live Forensics	15
	1.6.6. Privacy	15
	1.6.7. Multiple Cloud Service Providers	16
	1.7. PROBLEM DEFINITION	16
	1.8. PROPOSAL WORK	17
	1.9. ORGANISATION OF THE THESIS	18
	1.10. SUMMARY	19

2	**LITERATURE REVIEW**	**20**
	2.1. INTRODUCTION	20
	2.2. DIGITAL FORENSIC INVESTIGATION TECHNIQUES	20
	2.3. DATA INVESTIGATION TECHNIQUES IN CLOUD FORENSICS	22
	2.4. IDENTIFICATION OF MALICIOUS ATTACKS	27
	2.5. FORENSICS ANALYSIS TECHNIQUES	29
	2.6. SECURITY ENHANCEMENT TECHNIQUES IN CLOUD FORENSICS	31
	2.7. FAULT TOLERANCE TECHNIQUES IN CLOUD FORENSICS	35
	2.8. CLOUD FORENSICS IN VARIOUS APPLICATIONS	36
	2.9. RESEARCH GAP	38
	2.10. RESEARCH CONTRIBUTIONS	40
3	**SPATIO-TEMPORAL BASED FORENSIC DATA COLLECTION AND ISOLATION IN CLOUD**	**42**
	3.1. INTRODUCTION	42
	3.2. FORENSIC ACQUISITION AND ANALYSIS SYTEM (FAAS)	43
	3.3. SECURE-LOGGING-AS-A-SERVICE (SecLaaS) SCHEME	44
	3.4. MULTI-TENANTS FORENSIC DATA COLLECTION AND ISOLATION USING STFDC-LF TECHNIQUE	45
	3.4.1 Collection of Cloud Log Files from Different Sources	47
	3.4.1.1. Spatio- Temporal Data Collector	48
	3.4.1.2. Event Activity Time Synchronization method	50
	3.4.1.2.1. Event Activity Time Synchronization with External and Internal Time Resources	51
	3.4.2. Multi Tenant Log Data Isolation	53
	3.5. EXPERIMENTAL EVALUATION OF STFDC-LF TECHNIQUE	56
	3.6. RESULTS ANALYSIS OF STFDC-LF TECHNIQUE	56
	3.6.1. Performance Analysis of Investigation Accuracy	56
	3.6.2. Performance Analysis of Investigation Time	58
	3.6.3. Performance Analysis of Filtering Efficiency	60
	3.6.4. Performance Analysis of Isolation Speed	61
	3.7. SUMMARY	63

4	**MULTI-OBJECTIVE FUNCTIONS BASED GENE OPTIMIZATION FOR MALICIOUS USER DETECTION IN CLOUD FORENSIC SERVICES**	**65**
	4.1. INTRODUCTION	65
	4.2. FORENSIC OPEN-STACK TOOLS (FROST) ON OPENSTACK CLOUD PLATFORM	66
	4.3. IMPROVING CONFIDENTIALITY ON CLOUD DATA BY USING SECURE LOGGING-AS-A-SERVICE (SECLAAS) SCHEME	67
	4.4. REPORTING ACCEPTABLE EVIDENVCE OF SUSPECT BY USING GENE OPTIMIZED MULTI-OBJECTIVE PROOF ACCUMULATOR	67
	4.4.1. Analysis of Multi Objective Function	69
	4.4.1.1. Proof of Integrity	70
	4.4.1.2. Provable Data Possession (PDP)	70
	4.4.1.3. Data Provenance Information	71
	4.4.1.4. Time Stamp Analysis	73
	4.4.2. Gene based Approach	74
	4.5. EXPERIMENTAL EVALUATION OF GOMOPA TECHNIQUE	77
	4.6. RESULT ANALYSIS OF GOMOPA TECHNIQUE	78
	4.6.1. Performance Analysis of Investigation Accuracy	78
	4.6.2. Performance Analysis of Processing Time	80
	4.6.3. Performance Analysis of Confidentiality Rate	82
	4.7. SUMMARY	83
5	**SPATIOTEMPORAL FORENSIC DATA COLLECTION AND ISOLATION BASED PARTICLE SWARM OPTIMIZATION FOR SECURED CLOUD SERVICES**	**85**
	5.1. INTRODUCTION	85
	5.2. SECURE PROVENANCE SCHEME	86
	5.3. SECURITY AS A SERVICE MODEL	87
	5.4. SECURE-LOGGING-AS-A-SERVICE (SecLaaS) SCHEME	87
	5.5. SPATIOTEMPORAL FORENSIC DATA COLLECTOR AND SWARM OPTIMIZED MULTI-OBJECTIVE PROOACCUMULATOR (SFDC-SOMOPA) TECHNIQUE	88

	5.5.1. Collection of Cloud Log Files from Various Sources	90
	5.5.1.1. Spatiotemporal Forensic Data Collector	90
	5.5.1.2. Fault Tolerant Time Synchronization	91
	5.5.2. Isolation of Cloud Log Files	94
	5.5.3. Submission of Admissible Evidence	97
	5.5.3.1. Analysis of Multi Objective Functions	97
	5.5.3.2. Identification of Malicious User	98
	5.6. EXPERIMENTAL EVALUATION SFDC-SOMOPA TECHNIQUE	101
	5.7. RESULT ANALYSIS OF SFDC-SOMOPA TECHNIQUE	101
	5.7.1. Performance Analysis of investigation Accuracy	101
	5.7.2. Performance Analysis of Investigation Time	104
	5.7.3. Performance Analysis of Filtering Efficiency	105
	5.7.4. Performance Analysis of Processing Time	107
	5.7.5. Performance Analysis of Confidentiality Rate	109
	5.8. SUMMARY	110
6	**PERFORMANCE OF CLOUD FORENSIC ANALYSIS FOR SECURED FILE TRANSMISSION IN GOVERNMENT SECTORS**	**112**
	6.1. INTRODUCTION	112
	6.2. PERFORMANCE ANALYSIS FOR PROPOSED STFDC-LF, GOMOPA AND SFDC-SOMOPA TECHNIQUES	116
	6.2.1. Performance Analysis of Investigation Accuracy	116
	6.2.2. Performance Analysis of Investigation Time	119
	6.2.3. Performance Analysis of filtering Efficiency	122
	6.2.4. Performance Analysis of Confidentiality Rate	124
	6.2.5. Performance Analysis of Processing Time	127
	6.3. SUMMARY	129
7	**CONCLUSION AND FUTURE WORK**	**130**
	7.1. CONCLUSION	130
	7.2. LIMITATIONS AND FUTURE WORK	132
	REFERENCES	**132**

List of Tables

TABLE NO	TITLE	PAGE NO
3.1.	Tabulation for Investigation Accuracy	57
3.2.	Tabulation for Investigation Time	58
3.3.	Tabulation for Filtering Efficiency	60
3.4.	Tabulation for Isolation Speed	62
4.1.	Representation of Provenance Information	73
4.2.	Tabulation for Investigation Accuracy	78
4.3.	Tabulation for Processing Time	80
4.4.	Tabulation for Confidentiality Rate	82
5.1.	Tabulation for Investigation Accuracy	102
5.2.	Tabulation for Investigation Time	104
5.3.	Tabulation for Filtering Efficiency	106
5.4.	Tabulation for Processing Time	107
5.5.	Tabulation for Confidentiality Rate	109
6.1.	Tabulation for Investigation Accuracy	117
6.2.	Tabulation for Investigation Time	120
6.3.	Tabulation for Filtering Efficiency	122
6.4.	Tabulation for Confidentiality Rate	125
6.5.	Tabulation for Processing Time	127

List of Figures

FIG NO.	TITLE	PAGE NO
1.1.	Cloud Forensics Diagram	2
1.2.	Cloud Forensic Three-Dimensional Model	3
1.3.	Four Steps for Forensic Investigation in Cloud Environments	6
1.4.	Cloud Forensics investigation process	7
1.5.	Data Acquisition within an IaaS	9
1.6.	Relationship between both the Dead and Alive System	12
3.1.	Overview of Logging Scheme with Privacy Preservation on Cloud Forensic Framework	46
3.2.	Architectural Diagram of the Proposed STFDC-LF Technique in Cloud Forensic Framework	47
3.3.	Event Activity Time Synchronization with External Source	51
3.4.	Event Activity Time Synchronization with Internal Source	52
3.5.	Multi Tenant Forensic log Filter Process	53
3.6.	Forensic Log Filter Process	54
3.7.	Measurement of Investigation Accuracy	57
3.8.	Measurement of Investigation Time	59
3.9.	Measurement of Filtering Efficiency	61
3.10.	Measurement of Isolation Speed	63
4.1.	Architectural Diagram of the Gene Optimized Multi-Objective Proof ACCUMULATOR Technique	68
4.2	Cloud Forensic Models For Crime Investigation	69
4.3.	Data Provenance in Cloud	72
4.4.	Crossover Process	75
4.5.	Mutation	76
4.6.	Measure of Investigation Accuracy	79
4.7.	Measure of Processing Time	81
4.8.	Measure of Confidentiality Rate	83
5.1.	Architecture Diagram of the Spatiotemporal Forensic Data Collector and Swarm Optimized Multi-objective Proof Accumulator	89
5.2.	Fault Tolerant in Cloud Environment	92

5.3.	Processing Diagram of the Adaptive Fault Tolerance	93
5.4.	Process of Watermarked Forensic Logging FILTER	95
5.5.	Measure of Investigation Accuracy	103
5.6.	Measure of Investigation Time	105
5.7.	Measure of Filtering Efficiency	106
5.8	Measure of Processing Time	108
5.9	Measure of Confidentiality Rate	110
6.1.	Cloud Forensic Analysis for Secured Cloud Services	114
6.2.	Measure of Investigation Accuracy	118
6.3.	Measure of Investigation Time	121
6.4.	Measure of Filtering Efficiency	124
6.5.	Measure of Confidentiality Rate	126
6.6.	Measure of Processing Time	128

List of Abbreviation and Symbols

ABBREVIATIONS	DESCRIPTION
ABS	Attribute-based Signature Technique
API	Application Programming Interface
APT	Advanced Persistent Threat
ARM	Adaptive Resource Management
AWS	Amazon Web Service
CC	Cloud Controller
CLF	Cloud Log Forensics
C-NFMS	Current Network Forensics Methods
CSP	Cloud Service Provider
FAAS	Forensic Acquisition and Analysis System
FLF	Forensic Logging Filter
FMP	Forensic Monitoring Plane
FROST	Forensic Open-Stack Tools
FVM	Forensic Virtual Machine
GOMOPA	Multi-objective Proof Accumulator
HBST	Host Based Security Tools
HDFS	Hadoop distributed file system
IaaS	Infrastructure as a Service
LC	Log Chain
MCC	Mobile cloud computing
MHT	Merkle Hash Tree
NC	Node Controller
NFFs	Network Forensic Frameworks
NGS	Next Generation Sequencing
NLP	Natural Language processing
NTP	Network Time Protocol
PaaS	Platform as a Service
PDP	Provable Data Possession
PPL	Proof of Past Log
PSO	Particle Swarm Optimization
SaaS	Software as a Service
SCARF	SCAlable Realtime Forensics

SecLaaS	Secure-Logging-as-a-Service
SFDC-SOMOPA	Spatiotemporal Forensic Data Collector and Swarm Optimized Multi-Objective Proof Accumulator
SIEM	security Information and Event Management
SLA	Service Level Agreement
SOMOPA	Swarm Optimized Multi-objective Proof Accumulator
SPAD	Service Provider Attack Detection
STFDC-LF	Spatio-Temporal Forensic Data Collector and Logging filter
TCB	Trusted Computing Base
TPA	Third Party Auditor
TSAD	Tenant Specific Attack Detection
UTC	Universal Coordinated Time
UTM	Unified Threat Management
VDI	virtual Desktop Infrastructure
VM	Virtual Machine
WFLF	Watershed Forensic Logging Filter
‘L’	Location
‘ CU_i’	Cloud User
W_o	Initial Weighted Vector of the Cloud Users
V_i	Temporal and Spatial Uncorrelated Data
W_l^G	Global Weighted Vector
μ	Positive Step Size
$W_{i,l}^N$	Updated Weight Vector
D_i^N	data with multiple users
u_i^T	users login time
‘r’	Pearson correlation coefficient
$Sign_{PK}$	Private Key of the CSP
‘d_i’	Two Events of Tenants
$P_i{}^k$	Position of Particle
$V_i{}^{k+1}$	Adjusted velocity
W_t	Weight Factor