

Table of Contents

Preface	i
Acknowledgements.....	iii
Table of Contents	v
List of Figures	xiv
List of Tables.....	xvii
List of Abbreviations.....	xviii
CHAPTER 1 INTRODUCTION.....	Error! Bookmark not defined.
1.1. BACKGROUND.....	1
1.2. MOTIVATION FOR THE WORK	2
1.3. OBJECTIVES OF THE THESIS	2
1.4. CONTRIBUTIONS	2
1.5. ORGANIZATION OF THE THESIS.....	3
CHAPTER 2 LITERATURE SURVEY.....	5
2.1. CLOUD COMPUTING.....	5
2.1.1. <i>Definitions of the Cloud Computing</i>	6
2.2. CLOUD COMPUTING MODELS	6
2.2.1. <i>Service Oriented Cloud Computing</i>	7
2.2.1.1. Software as a Service(SaaS)	7
2.2.1.2. Platform as a Service(SaaS).....	8

2.2.1.3. Infrastructure as a Service(SaaS)	9
2.2.2. <i>Cloud Computing Deployment Models</i>	9
2.2.2.1.Private Cloud.....	9
2.2.2.2. Public Cloud.....	9
2.2.2.3. Hybrid Cloud.....	9
2.2.2.4. Community Cloud.....	10
2.2. CLOUD COMPUTING ISSUES	10
2.3.1. <i>Security and Privacy</i>	10
2.3.2. <i>Availability</i>	11
2.3.3. <i>Virtualization</i>	11
2.3.4. <i>Bandwidth Cost</i>	12
2.4. CLOUD COMPUTING CHALLENGES	12
2.4.1. <i>Security and Privacy</i>	12
2.4.2. <i>Data Confidentiality</i>	13
2.4.3. <i>Data Integrity</i>	14
2.4.4. <i>Identity and Access Managementt</i>	15
2.4.5. <i>Trust</i>	16
2.4.5.1. Persistent Trust.....	17
2.4.5.1. Dynamic Trust	17
2.4.6. <i>Insider Access</i>	17
2.4.7. <i>Risk</i>	17

2.4.7.1. Disruptive Force.....	18
2.4.7.2. Lack of Transparency	18
2.4.7.3. Security and Compliance Concerns	18
2.4.7.4. Risk of Data Leakage.....	18
2.4.7.5. Cloud Service Provider Viability.....	18
2.4.8. <i>Risk Management</i>	18
2.4.9. <i>Identity Management</i>	19
2.4.9.1 Authentication.....	19
2.4.9.2. Access Control.....	19
2.4.10. <i>Software Isolation</i>	19
2.4.10.1. Hypervisor Complexity.....	20
2.4.10.2. Attack Vectors	20
2.4.11. <i>Data Protection</i>	20
2.4.11.1. Data-Isolation.....	20
2.4.11.2. Data Sanitization.....	21
2.4.11.3. Data Location.....	21
2.4.12. <i>Availability</i>	21
2.4.12.1. Temporary Breakdown	21
2.4.12.2. Prolonged and Permanent Outages	22
2.4.13. <i>Denial of Services</i>	22
2.5. ATTACKS IN CLOUD COMPUTING	22

2.5.1. XML Signature.....	22
2.5.2. Browser Security.....	23
2.5.3. Attacks on Browser-Based Cloud Authentication.....	23
2.5.4. Cloud Malware Injection Attack.....	23
2.5.5. Meta data Spoofing Attack.....	23
2.5.6. Flooding Attack.....	23
2.5.7. Direct Denial of Service Attack	24
2.5.8. Indirect Denial of Service Attack.....	24
2.6. COMPARATIVE ANALYSIS FOR STRENGTHS AND LIMITATIONS OF SOME OF THE EXISTING SECURITY SCHEME	24
CHAPTER 3 SECURE AND PRIVACY ENHANCED AUTHENTICATION FRAMEWORK FOR CLOUD COMPUTING.....	28
3.1. INTRODUCTION.....	28
3.2. CRYPTOGRAPHY	28
3.3. CRYPTOGRAPHIC ALGORITHMS.....	29
3.3.1. Conventional Cryptography.....	29
3.3.2. Public Key Cryptography	30
3.4. PROBLEM STATEMENT	31
3.5. EXISTING WORK	31
3.6. EXISTING METHODS	33
3.6.1. Kerberos.....	33
3.6.1.1. Components of the Kerberos	33

3.6.2. <i>Working of the Kerberos</i>	34
3.6.2.1. Authentication.....	34
3.6.3. <i>Pretty Good Privacy (PGP)</i>	35
3.6.3.1. Working of PGP	35
3.6.3.2. PGP Keys and Key Rings	36
3.6.4. <i>Authentication by PGP</i>	37
3.7. PROPOSED METHOD.....	38
3.7.1. <i>Working of Proposed Method</i>	39
3.7.1.1. Authentication and Integrity	40
3.7.1.2. Confidentiality	41
3.7.1.3. Non repudiation	42
3.8. SECURITY ANALYSIS.....	43
3.8.1. <i>Automated Validation of Internet Security Protocol and Application (AVISPA)</i>	43
3.8.1.1. The IF.....	44
3.8.2. <i>Experimental Analysis</i>	44
3.8.2.1. Protocol Simulation With AVISPA	47
3.8.3. <i>Analysis</i>	49
3.8.3.1. Security Against Brute Force Attack	50
3.8.3.2. Mathematical Attack.....	50
3.8.3.3. User Privacy.....	50

3.8.3.4. Identity Management.....	50
3.8.3.5. Session Key Agreement.....	51
3.9. TECHNICAL COMPARISON OF THE VARIOUS AUTHENTICATION MODES	51
3.10. IMPLIMENTATION	52
3.11. CONCLUSION.....	58
CHAPTER 4 ACCESS CONTROL USING MOBILE VERIFICATION SYSTEM FOR CLOUD	59
4.1. INTRODUCTION.....	59
4.2. SMS BASED OTP PASSWORD.....	59
4.2.1. Parties Involved in SMS OTP.....	60
4.3. ARCHITECTURE OF ACCESS CONTROL MECHANISM USING MOBILE VERIFICATION	60
4.4. ACCESS CONTROL OF DATA AND APPLICATION	62
4.5. SIMULATION AND EXPERIMENTAL ANALYSIS.....	63
4.6. SECURITY EVALUATION OF THE MOBILE AUTHENTICATION MECHANISM	64
4.6.1. Key Logging Attacks	64
4.6.2. Lost or Stolen List of OTPs.....	65
4.6.3. Shoulder Surfing	65
4.6.4 Lost or Stolen Mobile Device.	65
4.7. IMPORTANT OBSERVATIONS	65
4.8. CONCLUSION	66
CHAPTER 5 MULTIFACTOR AUTHENTICATION IN CLOUD COMPUTING.....	67

5.1. INTRODUCTION.....	67
5.2. TRADITIONAL AUTHENTICATION TECHNIQUES	67
5.3. COMMON MULTI-FACTOR AUTHENTICATION METHODS.....	68
5.3.1. BIOMETRIC AUTHENTICATION	68
5.3.2. <i>SMS-Based One-Time Multi-Factor Authentication</i>	69
5.3.3. <i>Software-Based Certificate Multi-Factor Authentication</i>	69
5.3.4. <i>Internet Protocol Address (IPA) Location and Geo Location</i>	69
5.4. PROBLEM STATEMENT.....	69
5.5. MULTIFACTOR AUTHENTICATION MECHANISM FOR ACCESS CONTROL IN CLOUD COMPUTING.....	70
5.5.1. <i>Biometrics</i>	70
5.5.1.1. Fingerprint Recognition	70
5.5.1.2. Voice Recognition	71
5.5.1.3. Signature Recognition	71
5.5.1.4. Retinal Recognition	71
5.5.1.5. Iris Recognition	71
5.5.1.6. Palm Recognition	72
5.5.1.7. Face Recognition	72
5.5.2. <i>Biometrics for Cloud Security</i>	72
5.6. Mode of Operation of Biometric System.....	73
5.6.1. <i>Verification Mode</i>	73

5.6.2. <i>Identification Mode</i>	74
5.7. COMPONENTS OF BIOMETRIC SYSTEM	74
5.7.1. <i>Sensor module</i>	74
5.7.2. <i>Pre-processing</i>	75
5.7.3. <i>Feature Extraction</i>	75
5.7.4. <i>Matching Process</i>	75
5.7.5. <i>Decision Process</i>	75
5.8. IMPLEMENTATION OF BIOMETRIC SYSTEM FOR CLOUD SECURITY	76
5.8.1. <i>Stage I: New User Registration</i>	76
5.8.2. <i>Stage II: Assignment of User-Id and Password</i>	77
5.9. OUT OF BAND AUTHENTICATION.....	78
5.9.1. <i>Steps to Generating OTP</i>	78
5.9.2. <i>The OTP Server and Authentication Protocol</i>	78
5.10. METHOD FOR NEW USER REGISTRATION IN THE CLOUD	79
5.11. PROPOSED METHOD FOR ACCESS SERVICES FROM A CLOUD SERVICE PROVIDER	80
5.12. SECURITY ANALYSIS.....	81
5.12.1. <i>Robust Security</i>	81
5.12.2. <i>Identity Management</i>	81
5.12.3. <i>Mutual Authentication</i>	81
5.12.4. <i>Replay Attack</i>	82
5.12.5. <i>Password Guessing Attack</i>	82

5.12.6. <i>Insider Attack</i>	82
5.13. IMPORTANT OBSERVATIONS.....	82
5.14. IMPLIMENTATIONS.....	84
5.14.1. <i>Server Side</i>	84
5.15. CONCLUSION.....	89
CHAPTER 6 CONCLUSION AND SCOPE FOR FUTURE WORK.....	90
6.1. CONCLUDING REMARKS.....	90
6.2. SCOPE FOR FUTURE WORK.....	92
References	93
Appendix A- Implementation Codes	106

List of Figures

FIGURE 2.1: NIST STACK OF CLOUD COMPUTING.....	6
FIGURE 2.2 : LAYERED STACK OF SAAS.....	8
FIGURE 2.3 : IDC SURVEY ON CLOUD COMPUTING ISSUES AND CHALLENGES.	11
FIGURE 3.1 : WORKING OF SHARED KEY CRYPTOGRAPHY.....	29
FIGURE 3.2 : OVERVIEW OF PUBLIC KEY CRYPTOGRAPHY.....	30
FIGURE 3.3 : AUTHENTICATION.....	34
FIGURE 3.4 : PGP ENCRYPTION.....	36
FIGURE 3.5 : PGP DECRYPTION.....	36
FIGURE 3.6 : PROPOSED METHOD FOR CLOUD COMPUTING.....	38
FIGURE 3.7 : KERBEROS AUTHENTICATION IN CLOUD COMPUTING.....	39
FIGURE 3.8 : AUTHENTICATION BY PROPOSED FRAMEWORK.....	40
FIGURE 3.9 : CONFIDENTIALITY BY PROPOSED FRAMEWORK.....	42
FIGURE 3.10 : NON REPUDIATION PROPOSED FRAMEWORK.....	42
FIGURE 3.11 : AVISPA TOOL ARCHITECTURE.....	44
FIGURE 3.12 : TLS VISUALIZATION USING AVISPA.....	45
FIGURE 3.13 : TLS INTRUDER SIMULATION.....	45
FIGURE 3.14 : PROTOCOL SIMULATION(MESSAGE SEQUENCE CHART) RESULT.....	48
FIGURE 3.15 : EXISTING PROTOCOLS VS. KERB-PGP (EXECUTION TIME).....	50
FIGURE 3.16 : RESULT COMPARISION.....	51

FIGURE 3.17 : CLIENT REGISTRATION	53
FIGURE 3.18 : LOGIN - BY ENTERING USERNAME AND PASSWORD	54
FIGURE 3.19 : SEND REQUEST TO AUTHENTICATION SERVER FOR SERVICE.....	54
FIGURE 3.20 : PUBLIC KEY GENERATION	55
FIGURE 3.21 : TICKET GENERATION	56
FIGURE 3.22 : SERVICE REQUEST TO CSP	57
FIGURE 3.23 : NON REPUDIATION	57
FIGURE 4.1 : SMS OTP EXAMPLE IN FORM OF A MOBILE TAN.....	60
FIGURE 4.2 : USER AUTHENTICATION ARCHITECTURE USING MOBILE SMS	61
FIGURE 4.3 : WORKING OF OTP USING MOBILE AUTHENTICATION MECHANISM.....	61
FIGURE 4.4: GROUP AND PERMISSION BASED ACCESS CONTROL	62
FIGURE 4.5: OFMC RESULT OF OTP PROTOCOL	63
FIGURE 4.6: MSC FOR OTP PROTOCOL SIMULATION	64
FIGURE 4.7: SECURITY RISK AGAINST VARIOUS ATTACK	65
FIGURE 5.1 : MULTIFACTOR AUTHENTICATION OVERVIEW	70
FIGURE 5.2:BIOMETRIC CHARACTERISTICS: PHYSIOLOGICAL CHARACTERISTICS AND BEHAVIOURAL CHARACTERISTICS	73
FIGURE 5.3 : BLOCK DIAGRAM OF A GENERAL BIOMETRICS RECOGNITION SYSTEM.....	74
FIGURE 5.4 : NEW USER REGISTRATION IN CLOUD USING GENERIC BIOMETRIC SYSTEM	76
FIGURE 5.5 : REGISTERED USER REGISTRATION IN CLOUD USING GENERIC BIOMETRICS RECOGNITION SYSTEM.....	77
FIGURE 5.6 : NEW USER REGISTRATION IN CLOUD	79

FIGURE 5.7 : MULTI- FACTOR AUTHENTICATION AND SUCCESSFUL AUTHORIZATION.....	80
FIGURE 5.8 : SERVER SIDE REGISTRATION.....	84
FIGURE 5.9 : LOGIN.....	85
FIGURE 5.10 : OTP AS A PASSWORD.....	85
FIGURE 5.11 : BIOMETRIC AUTHENTICATION.....	86
FIGURE 5.12 : FACE CAPTURING AND AUTHENTICATION.....	86
FIGURE 5.13 : VERIFICATION/AUTHENTICATION.....	87
FIGURE 5.14 : SERVICE ACCESS REQUEST.....	87
FIGURE 5.15 : VALIDATION OF THE REQUEST.....	88
FIGURE 5.16 : ACCESS GRANTED.....	88

List of Tables

TABLE 2.1 : COMPARATIVE ANALYSIS FOR STRENGTHS AND LIMITATIONS OF SOME OF THE EXISTING SECURITY SCHEME..... 24

TABLE 3.1 : TLS PROTOCOL ANALYSIS. 46

TABLE 3.2 : KERBEROS PGP PROTOCOL ANALYSIS.....48

TABLE 3.3 : COMPARATIVE ANALYSIS OF THE PROPOSED METHOD WITH EXISTING PROTOCOL ... 49

TABLE 3.4 : TECHNICAL COMPARISON OF THE VARIOUS AUTHENTICATION MODES..... 51

List of Abbreviations

ACPS	Advanced Cloud Protection system
AES	Advanced Encryption Standard
APIs	Application Programming Interfaces
ATM	Automated Teller Machine
AS	Authentication Server Usually, it includes KDC and TGS
AWS	Amazon Web Services
CAST	Algorithm- Carlisle Adams and Stafford Tavares Algorithm
CPU	Central Processing Unit
CRM	Customer Relationship Management
CSP	Cloud Service Provider
CRUD	Create, Remove, Update, Delete
DES	Data Encryption Standard
DOM	Document Object Model
DoS	Denial of Service
DDoS	Direct Denial of Service
DH	Deffi-Hellman
DHT	Digital High Technology
EC2	Elastic Compute Cloud
ERM	Enterprise Risk Management
ESB	Enterprise Service Bus

FBI	Federal Bureau of Investigation
FIM	Federated Identity Management
FUDD	Fear, Uncertainty, Doubt, and Disinformation
GoogleApps	Google Applications
HIPAA	Health Insurance Portability and Accountability Act
HTTP	Hypertext Transfer Protocol
IaaS	Infrastructure as a Service
ICT	Information and Communication Technology
IDEA	International Data Encryption Algorithm
IDC	International Data Corporation
IT	Information Technology
KDC	Key Distribution Centre
KVM	Kernel-based Virtual Machine
LDAP	Lightweight Directory Access Protocol
MAC	Message Authentication Codes
NIST	National Institute of Standards and Technology
OAuth protocol	Open Authentication Protocol
OS	Operating System
OTP	One Time Pass Code
PaaS	Platform as a Service
PGP	Pretty Good Privacy

PIN	Personnel Identification Number
PKI	Public Key Infrastructure
QoS	Quality of Service
RBT	Rigorous Binary Tree
REST	Representational State Transfer
RSA	Rivest-Shamir-Adleman Algorithm
S3	Amazon's Simple Storage Service
SaaS	Software as a Service
SAML	Security Assertion Mark-up Language
SLA	Service Level Agreement
SIM	Subscriber Identity Module
SOA	Service-Oriented Architecture
SOAP	Simple Object Access Protocol
SSO	Single Sign On
TAN	Transaction Authorization Number
TC	Trusted Computing
TGS	Ticket Granting Servers
TLS	Transport Layer Security
TPM	Trusted Platform Module
TTP	Trusted Third Party
TGT	ticket-granting ticket

UDDI	Universal Description, Discovery, and Integration
VM	Virtual Machine
VMs	Virtual Machines
VMM	Virtual Machine Monitor
WS	Web Service
WSDL	Web Services Description Language
XACML	eXtensible Access Control Mark-up Language
XML	Extensible Mark-up Language
XOR	exclusive OR