SECURE CLOUD STORAGE MODEL TO PRESERVE CONFIDENTIALITY AND INTEGRITY

SARFRAZ NAWAZ BROHI

A thesis submitted in fulfilment of the
requirements for the award of the degree of
Doctor of Software Engineering

Advanced Informatics School
Universiti Teknologi Malaysia

JANUARY 2015

To

my supportive parents,

and

beloved siblings

ACKNOWLEDGEMENT

First of All, I thank ALLAH (SWT), the God Almighty, for granting me the health, knowledge, strength, ability, and patience to accomplish this research, and for blessing me with sympathetic and supportive supervisors as well as family members.

I am glad to express tremendous gratitude to my supervisor Dr Suriayati Chuprat for her compassionate character, knowledge sharing, ideas and continuous support from the first until the last day of this study. Her sincere behaviour and constructive feedback enabled me to achieve significant research milestones within the required time-frame.

I would also like to thank my external supervisor Dr Jamalul-lail Ab Manan for enriching me with innovative ideas and skills by sharing his expertise and knowledge in the field of cloud computing security. Due to his unlimited support for reviewing, improving and evaluating my research, I was able to publish several high quality research papers.

At various stages during this study, I faced several undesirable challenges which overburdened me with mental and physical stress. However, this never stopped me from progressing further due to encouraging, moral as well as financial support from my father Dr Muhammad Nawaz Brohi. I am extremely thankful to him for his understanding, kindness, believe, and trust on me.

I also wish to express deepest appreciation to my mother for her prayers regarding my success during this entire study. I will always remember my *late* grandmother in prayers. This research would have never been possible without her wishes for my success.

ABSTRACT

Cloud Service Providers (CSPs) offer remotely located cloud storage services to business organizations which include cost-effective advantages. From an industrial perspective, Amazon Simple Storage Service (S3) and Google Cloud Storage (GCS) are the leading cloud storage services. These storages are secured using the latest data security approaches such as cryptography algorithms, data auditing processes, and strict access control policies. However, organizations where confidentiality of information is a significant act, they are not assertive to adopt these services due to emerging data confidentiality and integrity concerns. Malicious attackers have violated the cloud storages to steal, view, manipulate, and tamper clients' data. The researchers have attempted to overcome these shortcomings by designing and developing various security models. These solutions incorporate limitations and require enhancements as well as improvements before they can be widely accepted by CSPs to guarantee secure cloud storage services. In order to solve the stated problem, this research developed an improved security solution namely Secure Cloud Storage Model (SCSM) which consists of Multi-factor authentication and authorization process using Role-Based Access Control (RBAC) with Complex Random Security Code Generator (CRSCG), Partial homomorphic cryptography using Rivest, Shamir and Adleman (RSA) algorithm, Trusted Third Party (TTP) services including Key Management (KM) approach and data auditing process, Implementation of 256-bit Secure Socket Layer (SSL), and Service Level Agreement (SLA). SCSM was implemented using Java Enterprise Edition with glassfish server and deployed on a cloud computing infrastructure. The model was evaluated using extended euclidean algorithm, system security analysis, key management recommendations, web-based testing tool, security scanner, and survey. The survey results presented that 83.33% of the respondents agreed for SCSM to be widely accepted by CSPs to offer secured cloud storage services. The aggregate evaluation results proved that SCSM is successful in preserving data confidentiality and integrity at remotely located cloud storages.

ABSTRAK

Penyedia perkhidmatan awan (CSP) menawarkan servis storan awan secara jauh yang memberi kelebihan kos yang efektif. Mengikut perspektif industri, *Amazon Simple Storage Service* (S3) dan *Google Cloud Storage* (GCS) merupakan peneraju utama servis storan awan. Storan ini adalah selamat kerana mereka menggunakan pendekatan keselamatan data yang terkini seperti algoritma kriptografi, proses pengauditan data serta polisi kawalan capaian yang ketat. Walau bagaimanapun, bagi organisasi yang mengutamakan kerahsiaan maklumat, mereka tidak tertarik untuk menggunakan servis tersebut kerana bimbang akan kerahsiaan dan integriti data. Penyerang yang berniat jahat telah mencabuli storan awan dengan mencuri, melihat, memanipulasi dan mengganggu data pelanggan. Para penyelidik telah mencuba menangani masalah-masalah ini dengan mereka bentuk dan membangunkan pelbagai model keselamatan. Penyelesaian yang telah dibangunkan ini masih mempunyai had tertentu dan memerlukan penambahbaikan sebelum ianya diterima secara meluas oleh CSP demi menjamin keselamatan servis tersebut. Untuk menyelesaikan masalah yang dinyatakan, penyelidikan ini telah membangunkan penyelesaian keselamatan yang telah ditambahbaik dan ianya dinamakan *Secure Cloud Storage Model* (SCSM). Model ini terdiri daripada pengesahan pelbagai-faktor, proses kebenaran menggunakan *Role-Based Access Control* (RBAC) dengan *Complex Random Security Code Generator* (CRSCG), kriptografi *homomorphic* separa menggunakan algoritma *Rivest, Shamir and Adleman* (RSA), servis-servis *Trusted Third Party* (TTP) iaitu pendekatan pengurusan kunci (KM) dan proses pengauditan data, perlaksanaan *Secure Socket Layer* (SSL) 256-bit, dan *Service Level Agreement* (SLA). SCSM dibangunkan menggunakan *Java Enterprise Edition* dengan pelayan *Glassfish* dan dilaksanakan pada infrastruktur pengkomputeran awan. Model ini kemudiannya dinilai menggunakan algoritma *Extended Euclidean*, analisis keselamatan sistem, cadangan-cadangan pengurusan kunci, alatan ujian berasaskan sesawang, pengimbas keselamatan serta kajian. Hasil kajian menunjukkan 83.33% responden bersetuju SCSM boleh diterima secara meluas oleh CSP yang menawarkan servis storan awan yang selamat. Keputusan penilaian membuktikan SCSM berjaya dalam memelihara kerahsiaan data dan integriti pada storan awan jarak jauh.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

ACL	-	Access Control List
ACM	-	Access Control Mechanism
ACP	-	Access Control Policy
AES	-	Advanced Encryption Standard
API	-	Application Programming Interface
AWS	-	Amazon Web Services
CA	-	Client's Admin
CAT	-	Computer Associates Technologies
CentOS	-	Community Enterprise Operating System
CRC	-	Cyclic Redundancy Check
CRSCG	-	Complex Random Security Code Generator
CSA	-	Cloud Security Alliance
CSP	-	Cloud Service Provider
CSPA	-	Cloud Service Provider's Admin
CSSP	-	Cloud Storage Service Provider
DAC	-	Discretionary Access Control
DBAN	-	Darik's Boot and Nuke
DSA	-	Digital Signature Algorithm
ECC	-	Elliptic Curve Cryptography
EJBs	-	Enterprise Java Beans
FHE	-	Fully Homomorphic Encryption
GCS	-	Google Cloud Storage
GFIS	-	German Federal Office of Information Security
HIPAA	-	Health Insurance Portability and Accountability Act
HMAC	-	Keyed-Hash Message Authentication Code
HTML	-	Hypertext Markup Language
HTTPS	-	Hypertext Transfer Protocol Secure

IaaS	-	Infrastructure as a Service
IM	-	Integrity Management
JSF	-	Java Server Faces
JSP	-	Java Server Pages
KM	-	Key Management
MAC	-	Mandatory Access Control
MITM	-	Man-in-the-Middle
NAS	-	Network Attached Storage
NIST	-	National Institute of Standards and Technology
NSA	-	National Security Agency
OS	-	Operating System
PaaS	-	Platform as a Service
PCI	-	Payment Card Industry
PCIDSS	-	Payment Card Industry Data Security Standard
RBAC	-	Role-based Access Control
RSA	-	Rivest, Shamir and Adleman
S3	-	Simple Storage Service
SaaS	-	Software as a Service
SCSM	-	Secure Cloud Storage Model
SDK	-	Software Development Kit
SDLC	-	Software Development Life Cycle
SE	-	Software Engineering
SHA	-	Secure Hash Algorithm
SLA	-	Service Level Agreement
SMBs	-	Small and Medium Businesses
SMS	-	Short Message Service
SQL	-	Structured Query Language
SSE	-	Server Side Encryption
SSE-C	-	Server Side Encryption with Customer-Provided Key
SSL	-	Secure Socket Layer
SSO	-	Single Sign-On
TCG	-	Trusted Computing Group
TDEA	-	Triple Data Encryption Algorithm

TED	-	Trusted Extension Device
TLS	-	Transport Layer Security
TPM	-	Trusted Platform Module
TTP	-	Trusted Third Party
TTPA	-	Trusted Third Party’s Admin
TVD	-	Trusted Virtual Domain
UML	-	Unified Modelling Language
VF	-	Virtual Firewall
VM	-	Virtual Machine
VMD	-	Verification Metadata
VPC	-	Virtual Private Cloud
VPS	-	Virtual Private Server
vTPM	-	Virtual Trusted Platform Module
XHTML	-	Extensible Hypertext Markup Language
XML	-	Extensible Markup Language
XSS	-	Cross-site Scripting

LIST OF SYMBOLS

$\mid$	-	Such That
d	-	Private Key Exponent
e	-	Public Key Exponent
n	-	Modulus for Private and Public Key
$\varpi(n)$	-	Phi Euler’s Function
R	-	Random Factor

LIST OF APPENDICES

CHAPTER 1

INTRODUCTION

1.1 Overview

Cloud computing is an innovative method of delivering computing resources (Tripathi and Mishra, 2011). It facilitates the clients to execute their enterprise applications and store data at third party owned servers. The cloud offers various service delivery models such as Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS), which are acquired by the clients according to their requirements (Bouayad *et al.*, 2012). IaaS is further categorized in three major facilities which include compute, network, and storage.

This research mainly focuses on storage sub-offering of IaaS, which is provided to clients by well-known Cloud Service Providers (CSPs) such as Amazon, and Google (Ghosh and Ghosh, 2012). This service facilitates the organizations to obtain dynamic, redundant and scalable, remotely located data storage services that can be easily scaled-up or down to avoid costly burdens of an under or over-utilized storage capacity (Jiang *et al.*, 2013). Cloud storage services have been very useful for Small and Medium Businesses (SMBs) that lack capital budget to implement and maintain personalized storage infrastructure (Sun and Sha-sha, 2011; Deyan and Hong, 2012).

However, nowadays cloud storage is becoming a business interest for all size organizations that are requiring resilient data availability, business continuity, and disaster recovery solutions. For cloud storage clients, critical data are maintained and backed-up by the CSP at multiple geographically distributed locations (Zhang and Zhang, 2011).

The remainder of this chapter is organized in eight sections. Section 1.2, describes the problem background. Section 1.3, represents the problem statement. The objectives, scopes, significance, and contribution of research are described in Sections 1.4, 1.5, 1.6 and 1.7, respectively. Section 1.8, illustrates and describes anatomy of the entire thesis. Section 1.9, represents the summary of this chapter.

1.2 Problem Background

The organizations that are required to follow well-defined data security standards such as the Health Insurance Portability and Accountability Act (HIPAA) and Payment Card Industry Data Security Standard (PCIDSS), do not trust the existing security techniques as well as policies offered by the CSPs (Hofmann and Woods, 2010; Bamiah *et al.*, 2012; Shucheng *et al*., 2010). Due to lack of control on their confidential data while it is stored at cloud storages, clients are concerned that malicious users might gain illegal access to their sensitive records (Taeho *et al*., 2013).

This research focuses on solving two major issues which are emerging concerns for organizations dealing with confidential data not to adopt cloud storage services, these include data confidentiality and integrity breaches (Syam and Subramanian, 2011; Gansen *et al*., 2010). The term data confidentiality refers to the concept that only authorized parties or systems have the ability to access protected information. The threat of data compromise increases in the cloud environment due to augmented number of parties, devices and applications involved, which leads to an increase in the amount of access points.

Data integrity means data can only be modified by the authorized parties. The concept of data integrity refers to protection of data from unauthorized deletion, modification or fabrication (Zissis and Lekkas, 2012). In order to further analyze the research problem, this research also conducted a survey from industry and academia based information security analysts, data auditors, cloud computing researchers, developers, architects and security specialists. The detailed structure of the survey is described in Chapter 6. The following question was mentioned in the survey to determine the validity and impact of the problem background of this research.

Question: Organizations dealing with confidential data are reluctant to use remotely located third party cloud storage services due to emerging data confidentiality and integrity concerns.

The response scale was based on three options, i.e. Agree, Neutral and Disagree. The survey response obtained for the research problem area, as shown in Table 1.1 and Figure 1.1, justifies the necessity of formulating a solution for the research problem, whereby 83.33% of respondents agreed that the organizations are reluctant to adopt cloud storage services due to emerging data confidentiality and integrity concerns.

Table 1.1: Analysis of Research Problem Area

Answer Choices	Response Rate	Academia	Industry	Total
Agree	83.33%	14	11	25
Neutral	16.67%	2	3	5
Disagree	0%	0	0	0

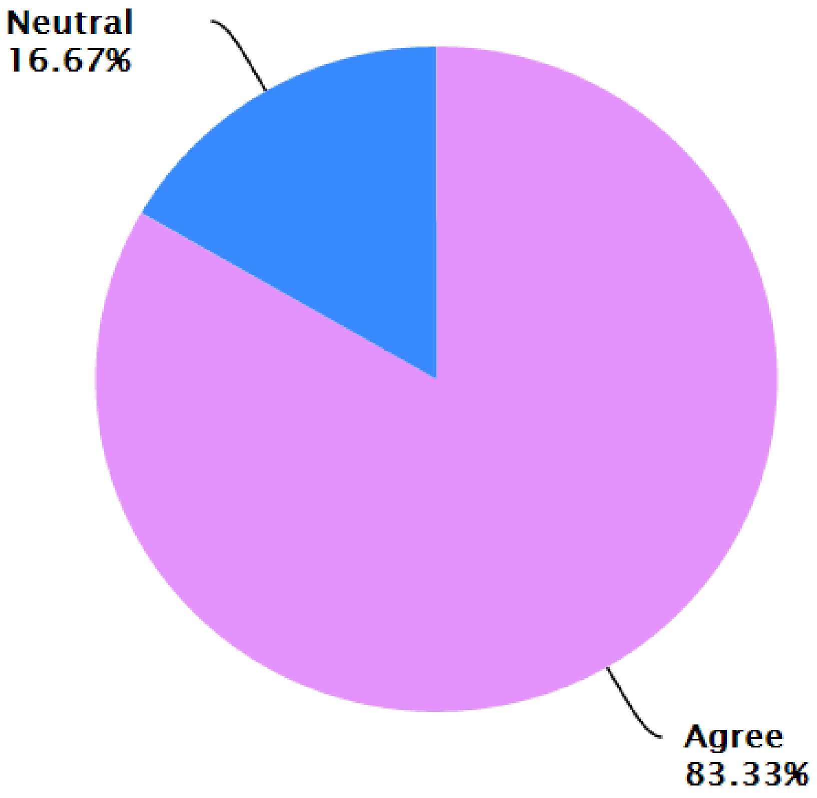

Figure 1.1: Survey for Research Problem Area

Past studies proved that confidentiality and integrity of data stored at cloud computing storage is breached by external or internal attacks (Ling *et al.*, 2011). External attacks are issued by outside hackers who steal clients' confidential records. These attacks may take place by wicked IT personnel from the competitors of CSP or the client. The intention of these attacks is to damage the brand reputation of CSP or to violate the clients' files. In order to defend against these attacks, CSPs normally secure their physical and virtual infrastructure using various tools and techniques for protecting clients' data and their systems. However, existing solutions are not adequate enough to achieve the desired target (Rocha and Correia, 2011). It is also identified that internal employees of CSP may become malicious as well (Catteddu and Hogben, 2009).

Internal attacks are placed by malicious insiders such as disgruntled employees of a CSP. They intentionally exceed their privileged accesses in a negative manner to affect the data confidentiality and integrity (Duncan *et al.*, 2012). In contrast to an external hacker, malicious insiders can attack the computing infrastructure with relatively easy manner and less knowledge of hacking, since they have a detailed description of the underlying infrastructure. Without using a complete trustworthy solution for defending against insider attacks, malicious insiders can easily obtain the passwords, cryptographic keys, files and gain access to clients' records (Rocha *et al.*, 2011). When clients' data confidentiality has been breached, they would never have knowledge of the unauthorized access mostly due to lack of control over their data and lack of transparency in the CSP's security practices as well as policies.

The breach of data confidentiality and integrity creates a barrier of trust among clients and CSPs. Clients need to ensure that CSP will always provide the agreed level of service and security to protect their confidential data. Trust is impacted when CSPs do not meet the negotiated agreements, for example, implementing insufficient security techniques, storing data at invalid locations which are not permitted by the legal law or not complying with the standards such as HIPAA or PCIDSS (Khan and Malluhi, 2010). The trust issues are normally mitigated by signing a legal Service Level Agreement (SLA) and granting adequate control to the clients on their confidential data (Xiaoyong and Junping, 2013). However, the existing SLAs are non-negotiable and fixed from the CSPs for every client which may be either an ordinary home user or a banking sector. These SLAs are not able to accommodate specific requirements of the organizations who are seeking to leverage cloud storage services for storing confidential data (Asha, 2012).

1.3 Problem Statement

As discussed in the problem background that cloud storages are vulnerable to external and internal attacks which have impacted the clients' trust towards CSPs for shifting their confidential data at third party cloud storages. Existing network security solutions are not able to overcome cloud storage data confidentiality and integrity violating threats (Nirmala *et al.*, 2013). Considering these issues, the problem statement of research is mentioned as follows:

How to develop a secure cloud storage model that preserves data confidentiality and integrity as well as ensures the delivery of trusted services to the clients by considering their data security policies?

Several research questions can be extracted from the problem statement, which are mentioned as follows:

i. What are the existing security models that have been designed, developed or proposed by the industry and academia researchers to overcome data confidentiality and integrity concerns for using cloud storage services?

ii. What are the limitations of existing industry and academia implemented cloud storage models that raise confidentiality and integrity issues which prevent organizations dealing with sensitive data from adopting cloud storage services?

iii. How to design a model that preserves data confidentiality and integrity at cloud storages as well as ensures the delivery of trusted services to the clients?

iv. How to develop a model that enables the clients to store and process their data at cloud storages with consistent data integrity, confidentiality and trust?

v. How to verify that the implemented cloud storage model is successful in preserving the confidentiality and integrity of sensitive data, and ensuring the delivery of trusted services to the clients?

1.4 Research Objectives

The aim of this research is to develop a security model that overcomes the data confidentiality and integrity concerns for using cloud storage services as well as for ensuring the delivery of trusted services to the clients by considering their data security policies. The targeted aim will be achieved by completing the following research objectives:

i. To investigate and obtain in-depth understanding of existing security models that have been proposed by the industry and academia researchers to overcome data confidentiality and integrity concerns for using cloud storage services.

ii. To critically analyze as well as explain the limitations or gaps which have been identified in the existing industry and academia implemented secure cloud storage models.

iii. To design an improved and enhanced secure cloud storage model which preserves data confidentiality and integrity, as well as ensures the delivery of trusted services to the clients by considering their data security policies.

iv. To implement and deploy a web-based prototype on a cloud computing infrastructure which facilitates the clients to store and process their data at cloud storages with consistent data confidentiality, integrity and trust assurance.

v. To evaluate the developed cloud storage model in order to ensure that it overcomes or mitigates the data confidentiality and integrity concerns, and gains the trust of organizations dealing with sensitive data to adopt cloud storage services.

1.5 Scope of Research

Cloud reference architecture consists of three service delivery (SaaS, PaaS, and IaaS) and four deployment models (Public, Private, Hybrid, and Community) (Mell and Grance, 2011). Since cloud computing is a vast area of research, this study only focuses on IaaS. Furthermore, IaaS providers offer compute, network and storage services to the clients. This research considers security of a cloud storage that resides at data center of a CSP. Security has several perspectives when it comes to research and development. This research considers confidentiality and integrity parameters of security as the major problems to be solved. This research assumed that breach of data confidentiality and integrity will impact the clients' trust for using cloud storage services. In order to achieve clients' trust, data confidentiality and integrity must be protected, and CSP must always ensure the delivery of trusted cloud storage services to the clients. Therefore, in this thesis, trust do not refers to the concept of trusted computing.

However, this research assumed that users may be required to use trusted platforms for using cloud storage services. For example, Trusted Extension Device (TED) and Trusted Platform Module (TPM) can be used by the clients to protect their devices. In a cloud computing environment, system performance is also considered as a significant factor, but SCSM was designed and developed mainly by considering the security requirements of the organizations dealing with highly confidential data. We believe that the identified research problem was not possible to be solved just by providing encryption and data auditing approaches. Therefore, our research scope focuses on providing a complete secure process that is comprised of a set of five components which include Multi-factor authentication and authorization process using Role-Based Access Control (RBAC) with Complex Random Security Code Generator (CRSCG), Partial homomorphic cryptography, Trusted Third Party (TTP) services including Key Management (KM) approach and data auditing process, implementation of 256-bit Secure Socket Layer (SSL) and SLA. This research also focuses on the deployment of the research contribution

Secure Cloud Storage Model (SCSM) on a cloud computing infrastructure in order to obtain authentic evaluation results.

1.6 Significance of Research

When objectives of the research are successfully accomplished, the development of SCSM can be considered as one of the valuable contributions in the field of cloud computing security, since it will overcome the existing data confidentiality and integrity concerns by providing trusted and secure cloud storage services to the clients. Contribution of this research will be beneficial for both, client organizations and CSPs. Clients will adopt cost-effective storage solutions in order to store their confidential data for high availability, accessibility, secure backup and recovery. Alternatively, CSPs will adopt this solution to overcome the limitations of their existing cloud storage services and to gain clients' trust. This research expects that adoption of cloud storage service will rapidly increase with the successful implementation and deployment of SCSM at the industry level.

1.7 Contribution of Research

The advent of cloud computing brought up enormous challenges for the software engineers to design as well as develop secure cloud applications, platforms, and infrastructures that deal with the storage of mission critical data. In the domain of Software Engineering (SE), information security engineers apply security principles at each stage of the Software Development Life Cycle (SDLC) from requirements analysis until development and deployment phases. They are also responsible to analyze and test the security of their developed cloud based solutions

(Zingham and Saqib, 2013). This research adopted a SE approach by designing, developing, deploying and analyzing the requirements of secure cloud storages. Therefore, this research contributed in the field of SE by completing those requirements which actually fall under the responsibilities of information security engineers for developing secure cloud storage services. The final contribution produced by this research as software will introduce a novel SE approach to develop complex confidentiality and integrity preserved cloud storage systems.

1.8 Thesis Organization

This thesis explores an emerging area of cloud security research focusing on data confidentiality and integrity concerns for using cloud storage services. The complete research is organized in seven chapters. Figure 1.2, shows the flow of thesis organization. Chapter 1 represents the significance of this research mainly by clarifying the research problem area, scope, contributions and objectives. An in-depth analysis of existing literature is provided in Chapter 2, which covers cloud security techniques and models provided by various researchers to solve the existing cloud storage security problems. Chapter 2 also covers the critical analysis on the limitations and strengths of industry and academia implemented contributions. Chapter 3 describes the entire research methodology used systematically for accomplishing each research objective. Description and design of the SCSM are provided in Chapter 4. Each component of SCSM is discussed with technical as well as theoretical details. SCSM is designed using architecture, use-case and sequence diagram, in-addition to the construction of an effective SLA. Chapter 5 describes the development details of SCSM implementation as a web-based prototype. Entire system workflow is described using user interface snapshots. System deployment details at the real cloud computing infrastructure are also described in Chapter 5. The evaluation process and results for the entire process as well as the each component of SCSM are described in Chapter 6. The applications of SCSM, overall research conclusion, limitations and future direction, are critically discussed and justified in Chapter 7.

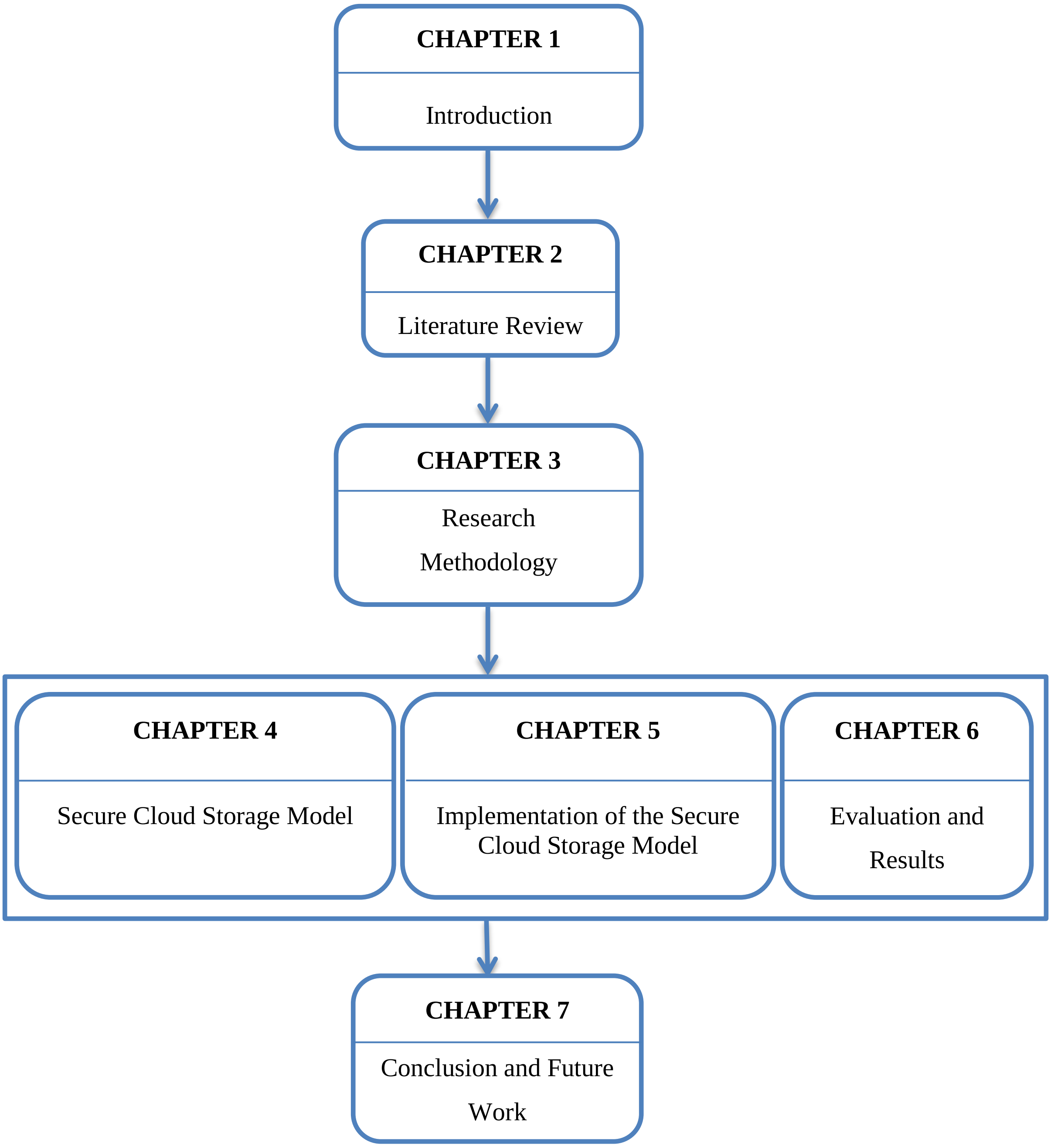

Figure 1.2: Thesis Organization

1.9 Summary

Cloud storage service is sub-category of IaaS which is provided to organizations for storing large amounts of data with unlimited capacity, broad accessibility, resilient availability, disaster recovery, and cost-effectiveness features. However, organizations dealing with confidential data are reluctant to adopt remotely located cloud storage services due to emerging data confidentiality and integrity concerns which have created a barrier of trust among the CSPs and clients. In order to overcome the mentioned problem, this research aims to provide an improved as well as enhanced solution for designing as well as developing confidentiality and integrity preserved secure model to use cloud storage services by accomplishing the research objectives. The successful implementation as well as deployment of SCSM at the industry level will assist CSPs to adopt this solution for offering secure and trusted cloud storage services to the business organizations.

REFERENCES

Achemlal, M., Gharout, S. and Gaber, C. (2011). Trusted Platform Module as an Enabler for Security in Cloud Computing. *Proceedings of 2011 International Conference on Network and Information Systems Security (SAR-SSI),* 18-21 May. La Rochelle, 1-6.

Adebiyi, A., Johnnes, A. and Chris, I. (2012). Security Assessment of Software Design using Neural Network, *International Journal of Advanced Research in Artificial Intelligence,* 1 (4), 1 – 7. SAI Publications.

Afoulki, Z., Bousquet, A., Briffaut, J., Rouzaud, J. and Toinard, C. (2012). MAC Protection of the Open Nebula Cloud Environment, *Proceedings of 2012 International Conference on High Performance Computing and Simulation (HPCS),* 2-6 July. Madrid, 85-90.

Ahmed, A. (2012). Meeting PCI DSS When Using a Cloud Service Provider. *Journal of Information Systems Audit and Control Association (JISACA),* 5, 24 – 30. ISACA Publications.

Ahmed, S. and Raja, M. (2010). Tackling Cloud Security Issues and Forensics Model. *Proceedings of 2010 High-Capacity Optical Networks and Enabling Technologies (HONET),* 19-21 December. Cairo, 190-195.

Amazon, (2011). Amazon Web Services: Overview of Security Processes. Amazon Web Services, Inc.

Amazon, (2013). Amazon Simple Storage Service SLA. Amazon Web Services. Retrieved July 2, 2013, from http://aws.amazon.com/s3/sla.

Amazon, (2014). Amazon Simple Storage Service: Developer Guide. API Version 2006-03-01. Amazon Web Services, Inc.

Ang, L., Yang, X., Srikanth, K. and Ming, Z. (2011). Comparing Public-Cloud Providers. *Internet Computing,* 15 (2), 50 – 53. IEEE Computer Society.

Asghar, M., Russello, G., Bruno, C. and Ion, M. (2013). Supporting Complex Queries and Access Policies for Multi-user Encrypted Databases. *Proceedings of the 2013*

ACM Workshop on Cloud Computing Security. 4-8 November. New York, 77-88.

Asha, M. (2012). Security and Privacy Issues of Cloud Computing: Solutions and Secure Framework. *International Journal of Multidisciplinary Research,* 2 (4), 182 – 193. Zenith International Research and Academic Foundation.

Astrova, I., Stella, G., Marc, S., Koschel, A., Jan, B., Kellermeier, M., Stefan, N., Francisco, C. and Michael, H. (2012). Security of a Public Cloud. *Proceedings of 2012 6th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS),* 4-6 July. Palermo, 564-569.

Ayushi. (2010). A Symmetric Key Cryptographic Algorithm. *International Journal of Computer Applications, 1 (15),* 1 – 4. Foundation of Computer Science.

Bamiah, M. and Brohi, S. (2011). Exploring the Cloud Deployment and Service Delivery Models. *International Journal of Research and Reviews in Information Sciences (IJRRIS),* 1 (3), 77 – 80. Science Academy Publisher.

Bamiah, M. and Brohi, S. (2011a). Seven Deadly Threats and Vulnerabilities in Cloud Computing. *International Journal of Advanced Engineering Sciences and Technologies (IJAEST),* 9 (1), 87 – 90. International Scientific Engineering and Research Publications.

Bamiah, M., Brohi, S. and Chuprat, S. (2012b). Using Virtual Machine Monitors to Overcome the Challenges of Monitoring and Managing Virtualized Cloud Infrastructures. *Proceedings of 2012 4th International Conference on Machine Vision (ICMV 2011)*. 9-10 December. Singapore, 187-192.

Bamiah, M., Brohi, S., Chuprat, S. and Brohi, M. (2012a). Cloud Implementation Security Challenges. *Proceedings of 2012 International Conference on Cloud Computing Technologies, Applications and Management (ICCCTAM)*. 8-10 December. Dubai, 174–178.

Bamiah, M., Brohi, S., Chuprat, S. and Jamalul-lail, A. (2012). A Study on Significance of Adopting Cloud Computing Paradigm in Healthcare Sector. *Proceedings of 2012 International Conference on Cloud Computing Technologies, Applications and Management (ICCCTAM)*. 8-10 December. Dubai, 65–68.

Bamiah, M., Brohi, S., Chuprat, S. and Jamalul-lail, A. (2013). Trusted Cloud Computing Framework for Healthcare Sector, *Journal of Computer Science,* 10 (2), 240 – 250. Science Publications.

Baun, C. and Kunze, M. (2009). Building a Private Cloud with Eucalyptus.

Proceedings of 2009 5th IEEE International Conference on E-Science Workshops. 9-11 December. Oxford, 33-38.

Bouayad, A., Bilalat, A., Mejhed, N. and Ghazi, M. (2012). Cloud Computing: Security Challenges. *Proceedings of 2012 Colloquium in Information Science and Technology (CIST)*. 22-24 October. Fez, 26-31.

Bourque, P. and Fairley, R. (2014). Guide to the Software Engineering Body of Knowledge (SWEBOK). (Version 3.0). IEEE Computer Society. Los Alamitos, CA, USA.

Brohi, S. (2011). A Trusted Virtual Private Space Model for Enhancing the Level of Trust in Cloud Computing Technology. *International Journal of Research and Reviews in Information Sciences (IJRRIS)*, 1 (3), 74 – 76. Science Academy Publisher.

Brohi, S. and Bamiah, M. (2011). Challenges and Benefits for Adopting the Paradigm of Cloud Computing. *International Journal of Advanced Engineering Sciences and Technologies (IJAEST)*, 8 (2), 286 – 290. International Scientific Engineering and Research Publications.

Brohi, S. and Bamiah, M. (2011a). Exploit of Open Source Hypervisors for Managing the Virtual Machines on Cloud. *International Journal of Advanced Engineering Sciences and Technologies (IJAEST)*, 9 (1), 55 – 60. International Scientific Engineering and Research Publications.

Brohi, S., Bamiah, M., Brohi, M. and Kamran, R. (2012). Identifying and Analysing Security Threats to Virtualized Cloud Computing Infrastructures. *Proceedings of 2012 International Conference on Cloud Computing Technologies, Applications and Management (ICCCTAM)*. 8-10 December. Dubai, 151–155.

Brohi, S., Bamiah, M., Chuprat, S. and Jamalul-lail, A. (2012a). Towards an Efficient and Secure Educational Platform on Cloud Infrastructure. *Proceedings of 2012 International Conference on Cloud Computing Technologies, Applications and Management (ICCCTAM)*. 8-10 December. Dubai, 145–150.

Brohi, S., Bamiah, M., Chuprat, S. and Jamalul-lail, A. (2013), Design and Implementation of Privacy Preserved Off-Premises Cloud Storage. *Journal of Computer Science*, 10 (2), 210 – 223. Science Publications.

Catteddu, D. and Hogben, G. (2009). Benefits, Risks and Recommendations for Information Security. *European Network of Information Security Agency (ENISA).*

Retrieved June 25, 2013, from http://www.enisa.europa.eu/activities/ risk-management/files/deliverables/cloud-computing-risk-assessment.

Chan, J., Nepal, S., Moreland, D., Hwang, H., Chen, S. and Zic, J. (2007). User-Controlled Collaborations in the Context of Trust Extended Environments. *Proceedings of 2007 16th IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE)*. 18-20 June. Evry, 389-394.

Chirag, F., Shrikanth, V. and Trivedi, H. (2012). Cloud Security Using Authentication and File Base Encryption. International *Journal of Engineering Research and Technology (IJERT)*, 1 (10), 8 – 12. Engineering and Science Research Support Academy Publications.

Cohen, B. (2013). PaaS: New Opportunities for Cloud Application Development. *Transactions on Computers,* 46 (9), 97 – 100. IEEE Computer Society.

Cong, W., Chow, S., Qiang, W., Kui, R. and Lou, W. (2013). Privacy-Preserving Public Auditing for Secure Cloud Storage. *Transactions on Computers*, 62 (2), 362 – 375. IEEE Computer Society.

Cong, W., Kui, R., Lou, W. and Jin, Li. (2010). Toward Publicly Auditable Secure Cloud Data Storage Services. *Network*, 24 (4), 19 – 24. IEEE Communications Society.

Cong, W., Qiang, W., Kui, R., Ning, C. and Lou, W. (2012). Toward Secure and Dependable Storage Services in Cloud Computing. *Transactions on Services Computing*, 5 (2), 220 – 232. IEEE Computer Society.

CSA. (2011). Security Guidance for Critical Areas of Focus in Cloud Computing V-3.0, *Cloud Security Alliance (CSA).* Retrieved July 5, 2013, from https://cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf.

Deyan, C. and Hong, H. (2012). Data Security and Privacy Protection Issues in Cloud Computing. *Proceedings of 2012 International Conference on Computer Science and Electronics Engineering (ICCSEE).* 23-25 March. Hangzhou, 647-651.

Dillon, T., Chen, W. and Chang, E. (2010). Cloud Computing: Issues and Challenges. Proceedings of 2010 24th IEEE *International Conference on Advanced Information Networking and Applications (AINA).* 20-23 April. Perth, 27-33.

Dongxi, L., Lee, J., Jang, J., Nepal, S. and Zic, J. (2010). A Cloud Architecture of Virtual Trusted Platform Modules. *Proceedings of 2010 8th IEEE/IFIP*

International Conference on Embedded and Ubiquitous Computing (EUC). 11-13 December. Hong Kong, 804-811.

Duncan, A., Creese, S. and Goldsmith, M. (2012). Insider Attacks in Cloud Computing. *Proceedings of 2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*. 25-27 June. Liverpool, 857-862.

eApps, (2014). Custom Virtual Server Hosting in a True Cloud Platform. Retrieved 15 August, 201, from http://www.eapps.com/cloud-solutions/virtual-machine-hosting.php.

Eric, B. (2013). The Top Cloud Companies: Here's What Customers Think of Them: Retrieved July 19, 2014, from http://venturebeat.com/2013/09/09/top-cloud-companies-amazon-google-microsoft/.

Fadadu, C., Shrikanth, V. and Trivedi, H. (2012). Cloud Security Using Authentication and File Base Encryption. *International Journal of Engineering Research and Technology (IJERT)*, 1 (10), 15 – 18. Engineering and Science Research Support Academy Publications.

Ferreira, A. (2013). Google Encrypts All Data In Cloud Storage. Retrieved July 28, 2014, from http://www.securitybistro.com/?p=7931.

Forrester. (2012). IT Purchasing Goes Social. *Forrester Consulting and Research Now*. Retrieved October 23, 2013, from http://www.iab.net/media/file/IT _Purchasing_Goes_Social-Best_Practices_Final.pdf.

Franke, J., Boehm, M., Bahar, F. and Kleinjung, T. (2005). Factoring 640-bit RSA. Crypto World. Retrieved October 9, 2013, from http://www.crypto-world.com/announcements/rsa640.txt.

Friedman, E. and Savio, C. (2013). Influencing the Mass Affluent: Building Relationship on Social Media. *LinkedIn Corporation*. Retrieved October 23, 2013, from http://marketing.linkedin.com/sites/default/files/attachment /MassAffluentWhitepaper.pdf.

Gall, M., Schneider, A. and Fallenbeck, N. (2013). An Architecture for Community Clouds Using Concepts of the Intercloud. *Proceedings of 2013 IEEE 27th International Conference on Advanced Information Networking and Applications (AINA)*. 25-28 March. Barcelona, 1634-1639.

Gansen, Z., Rong, C., Jin, L., Feng, Z. and Yong, T. (2010). Trusted Data Sharing over

Untrusted Cloud Storage Providers. *Proceedings of 2010 IEEE 2nd International Conference on Cloud Computing Technology and Science (CloudCom)*. 30 November – 3 December. Indianapolis, 97-103.

Gentry, C. (2009). Fully Homomorphic Encryption using Ideal Lattices. *Proceedings of the 2009 41st Annual ACM Symposium on Theory of Computing*. 30 May – 2 June. New York, 169-178.

Ghosh, N. and Ghosh, K. (2012). An Approach to Identify and Monitor SLA Parameters for Storage-as-a-Service Cloud Delivery Model. *Proceedings of 2012 IEEE Globecom Workshops (GC Wkshps)*. 3-7 December. Anaheim, 724-729.

Gibson, J., Rondeau, R., Eveleigh, D. and Qing, T. (2012). Benefits and Challenges of Three Cloud Computing Service Models. *Proceedings of 2012 4th International Conference on Computational Aspects of Social Networks (CASoN)*. 21-23 November. Sao Carlos, 198-205.

Goluch, S. (2011). *The Development of Homomorphic Cryptography from RSA to Gentry's Privacy Homomorphism*. Vienna University of Technology, Vienna.

Google, (2012). Google Cloud Storage: A Simple Way to Store, Protect, and Share Data. Google Inc., USA.

Google, (2012a). Google’s Approach to IT Security: A Google White Paper. Google Inc., USA.

Google, (2013). Just Develop IT Migrates Petabytes of Data to Google Cloud Storage. Retrieved July 27, 2014, from http://googlecloudplatform.blogspot.com /2013/11/justdevelopit-migrates-petabytes-of-data-to-google-cloud-storage.html.

Google, (2014). Google Cloud Storage: Authentication: Retrieved July 27, 2014, from https://cloud.google.com/storage/docs/authentication.

Gupta, S., Horrow, S. and Sardana, A. (2012). IDS Based Defense for Cloud Based Mobile Infrastructure as a Service. *Proceedings of 2012 IEEE 8th World Congress on Services (SERVICES)*. 24-29 June. Honolulu, 199-202.

Harris, C. (2011). IT Downtime Costs $26.5 Billion In Lost Revenue. Retrieved August 7, 2014, from http://www.informationweek.com/it-downtime-costs-$265-billion-in-lost-revenue/d/d-id/1097919.

Hibo, H., Jianliang, X., Chushi, R. and Byron, C. (2011). Processing Private Queries over Untrusted Data Cloud through Privacy Homomorphism. *Proceedings of 2011 27th International Conference on Data Engineering*. 11-16 April. Hannover, 601-

61.

Hofmann, P. and Woods, D. (2010). Cloud Computing: The Limits of Public Clouds for Business Applications. *Internet Computing*, 14 (6), 90 – 93. IEEE Computer Society.

Huaqun, W. (2013). Proxy Provable Data Possession in Public Clouds. *Transactions on Services Computing*, 6 (4), 551 – 559. IEEE Computer Society.

Hunsinger, S. and Corley, J. (2013). What Influences Students to Use Dropbox? *Journal of Information Systems Applied Research (JISAR)*, 6 (3), 18 – 25. Education Special Interest Group (EDSIG).

Ivan, R., Christian, B., Christian, F., Robert, H., Shezaf, O. and Colin Watson. (2013). SSL Server Rating Guide. *Qualys SSL Labs*. Retrieved October 3, 2013, from https://www.ssllabs.com/projects/rating-guide/.

Jadeja, Y. and Modi, K. (2012). Cloud Computing-Concepts, Architecture and Challenges. *Proceedings of 2012 International Conference on Computing, Electronics and Electrical Technologies (ICCEET)*. 21-22 March. Kumaracoil, 877-880.

Jang-Jaccard, J., Manraj, A. and Nepal, S. (2012). Portable Key Management Service for Cloud Storage. *Proceedings of 2012 8th International Conference on Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom)*. 14-17 October. Pittsburgh, 147-156.

Jansen, W. and Grance, I. (2011). Guidelines on Security and Privacy in Public Cloud Computing. *National Institute of Standards and Technology (NIST)*. Special Publication. NIST Special Publication 800-14.

Janssen, C. (2010). Key Escrow. Retrieved August 20, 2014, from http://www.techopedia.com/definition/3997/key-escrow.

Javaraiah, V. (2011). Backup for Cloud and Disaster Recovery for Consumers and SMBs. *Proceedings of 2011 IEEE 5th International Conference on Advanced Networks and Telecommunication Systems (ANTS)*. 18-21 December. Bangalore, 1-3.

Jeff, B. (2011). New - Amazon S3 Server Side Encryption for Data at Rest. Retrieved July 20, 2014, from http://aws.amazon.com/blogs/aws/new-amazon-s3-server-side-encryption/.

Jeff, B. (2011a). Client-Side Data Encryption for Amazon S3 Using the AWS SDK for

Java. Retrieved July 22, 2014, from http://aws.amazon.com/blogs/aws/client-side-data-encryption-using-the-aws-sdk-for-java/.

Jeff, B. (2014). Use Your Own Encryption Keys with S3's Server-Side Encryption. Retrieved July 22, 2014, from http://aws.amazon.com/blogs/aws/s3-encryption-with-your-keys/.

Jiang, W., Zhiming, Z. and Laat, C. (2013). An Autonomous Security Storage Solution for Data-Intensive Cooperative Cloud Computing, *Proceedings of 2013 IEEE 9th International Conference on eScience (eScience)*. 22-25 October. Beijing, 369-372.

Jing-Jang, H., Chuang, H., Yi-Chang, H. and Chien-Hsing, W. (2011). A Business Model for Cloud Computing Based on a Separate Encryption and Decryption Service, *Proceedings of 2011 International Conference on Information Science and Applications (ICISA)*. 26-29 April. Jeju Island, 1-7.

Junjie, P., Xuejun, Z., Zhou, L., Bofeng, Z., Wu, Z. and Qing, L. (2009). Comparison of Several Cloud Computing Platforms. Proceedings of 2009 2nd *International Symposium on Information Science and Engineering (ISISE)*. 26-28 December. Shanghai, 23-27.

Kalpana, P. and Sudha, S. (2012). Data Security in Cloud Computing using RSA Algorithm. *International Journal of Research in Computer and Communication Technology (IJRCCT)*, 1 (4), 143 – 146.

Kandukuri, R., Paturi, R. and Rakshit, A. (2009). Cloud Security Issues. *Proceedings of 2009 IEEE International Conference on Services Computing (SCC)*, 21-25 September. Bangalore, 517-520.

Karumanchi, S. (2010). *A Trusted Storage System for the Cloud*. Masters of Science in College of Engineering, University of Kentucky, USA.

Keung, J. and Kwok, F. (2012). Cloud Deployment Model Selection Assessment for SMEs: Renting or Buying a Cloud. *Proceedings of 2012 IEEE 5th International Conference on Utility and Cloud Computing (UCC)*. 5-9 November. Chicago, 21-28.

Kevin, B. and Hanf, D. (2010). Cloud SLA Consideration for the Government Consumers. *The MITRE Corporation.* Case Number 10-2902.

Khan, A. (2012). Access Control in Cloud Computing Environment, *Journal of Engineering and Applied Sciences (JEAS)*, 7 (5), 613 – 615. ARPN Publications.

Khan, K. and Malluhi, Q. (2010). Establishing Trust in Cloud Computing. *IT*

Professional, 12 (5), 20 – 27. IEEE Computer Society.

Kui, R., Cong, W. and Qian, W. (2012). Security Challenges for the Public Cloud. *Internet Computing*, 16 (1), 69 – 73. IEEE Computer Society.

Kumar, S. and Dubey, N. (2013). Cloud Computing (A Survey on Cloud Computing Security Issues and Attacks in Private Clouds). *International Journal of Emerging Trends in Engineering and Development (IJETED)*, 1 (2), 416 – 427. RS Publications.

Le, X., Li, L., Nagarajan, V., Dijiang Huang. and Wei-Tek, T. (2013). Secure Web Referral Services for Mobile Cloud Computing. *Proceedings of 2013 IEEE 7th International Symposium on Service Oriented System Engineering (SOSE)*. 25-28 March. Redwood City, 584-593.

Lin, Y., Hongli, Z., Jiantao, S. and Xiaojiang, D. (2012). Verifying Cloud Service Level Agreement. *Proceedings of 2012 IEEE Global Communications Conference (GLOBECOM)*. 3-7 December. Anaheim, 777-782.

Ling, L., Lin, X., Jing, L. and Changchun, Z. (2011). Study on the Third-party Audit in Cloud Storage Service. *Proceedings of 2011 International Conference on Cloud and Service Computing (CSC)*. 12-14 December. Hong Kong, 220-227.

Loewen, G., Galloway, M. and Vrbsky, S. (2013). Designing a Middleware API for Building Private IaaS Cloud Architectures. *Proceedings of 2013 IEEE 33rd International Conference on Distributed Computing Systems Workshops (ICDCSW)*. 8-11 July. Philadelphia, 103-107.

Marshal, S. (2013). Secure Audit Service by Using TPA for Data Integrity in Cloud System. *International Journal of Innovative Technology and Exploring Engineering (IJITEE)*, 3 (4), 49 – 52.

Marston, S., Zhi, L., Bandyopadhyay, S. and Ghalsasi, A. (2011). Cloud Computing - The Business Perspective. *Decision Support Systems (DSS)*, 51 (1), 176 – 189. Elsevier.

Mazhelis, O., Fazekas, G. and Tyrvainen, P. (2012). Impact of Storage Acquisition Intervals on the Cost-Efficiency of the Private vs. Public Storage. *Proceedings of 2012 IEEE 5th International Conference on Cloud Computing (CLOUD)*. Honolulu, 646-653.

McRee, R. (2010). Web Security Tools: Skipfish and iScanner. *Journal of Information Systems Security Association (JISSA)*, 35 – 37. ISSA Publications.

Mell, P. and Grance, T. (2011). The NIST Definition of Cloud Computing, *National Institute of Standards and Technology (NIST)*. Retrieved June 2, 2013, from http://csrc.nist.gov/publications/nistpubs/800145/SP800-145.pdf.

Michael, H. (2011). Security Recommendations for Cloud Computing Providers. *German Federal Office of Information Security (GFIS)*. Retrieved October 15, 2013, from https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/ Publications/Minimum_information/SecurityRecommendationsCloudComputingProviders.pdf?__blob=publicationFile.

Milanov, E. (2009). The RSA Algorithm, University of Washington: Department of Mathematics. Retrieved October 8, 2013, from http://www.math.washington.edu /~morrow/336_09/papers/Yevgeny.pdf.

Mishra, N., Kanchan, K., Ritu, C. and Abhishek, C. (2013). Technologies of Cloud Computing-Architecture Concepts based on Security and its Challenges. *International Journal of Advanced Research in Computer Engineering & Technology (IJARCET),* 2 (3), 1143 – 1149.

Murali, M., Kinnari, S. and Gunda, M. (2013). Enabling Secure Database as a Service using Fully Homomorphic Encryption: Challenges and Opportunities. Cornell University Computer Science Database. Arxiv: 1302.2654. 1-5.

Nepal, S., Friedrich, C., Henry, L. and Shiping, C. (2011). A Secure Storage Service in the Hybrid Cloud. *Proceedings of 2011 IEEE 4th International Conference on Utility and Cloud Computing (UCC)*. 5-8 December. Victoria, 334-338.

Nepal, S., John, Z., Hon, H. and Moreland, D. (2007). Trust Extension Device: Providing Mobility and Portability of Trust in Cooperative Information Systems. *In. International Conference on On the Move to Meaningful Internet Systems 2007: CoopIS,* DOA, ODBASE, GADA (pp. 253 – 271). Berlin Heidelberg: Springer.

Nirmala, V., Sivanandhan, R. and Lakshmi, R. (2013). Data Confidentiality and Integrity Verification using User Authenticator Scheme in Cloud. *Proceedings of 2013 IEEE International Conference on Green High Performance Computing (ICGHPC).* 14-15 March. Tamilnadu, 1-5.

Nithiavathy, R. (2013). Data Integrity and Data Dynamics with Secure Storage Service in Cloud. *Proceedings of 2013 International Conference on Pattern Recognition, Informatics and Mobile Engineering (PRIME).* 21-22 February. Salem, 125-130.

Nkosi, L., Tarwireyi, P. and Adigun, M. (2013). Insider Threat Detection Model for the

Cloud. *Information Security for South Africa (ISSA),* 1 – 8.

Omar M., Asif, K., Mahaboob, S. and Ramana, M. (2012). Secure Communication using Symmetric and Asymmetric Cryptographic Techniques. *International Journal of Information Engineering and Electronic Business (IJEEB),* 2 (6), 36 – 42. MECS Publisher.

Oracle, (2013). GlassFish Server Open Source Edition Application Deployment Guide. Release 4.0. Oracle America, Inc., 500 Oracle Parkway, Redwood City, CA.

Pang Xiong, W. and Li, D. (2013). Quality Model for Evaluating SaaS Service. *Proceedings of 2013 4th International Conference on Emerging Intelligent Data and Web Technologies (EIDWT).* 9-11 September. Xian, 83-87.

Paul, R. and Shanmugapriyaa, S. (2012). Evolution of Cloud Storage as Cloud Computing *Infrastructure Service. Journal of Computer Engineering (JCE),* 1 (1), 38 – 45. International Organization of Scientific Research.

Prerna, M. and Abhishek, S. (2013). A Study of Encryption Algorithms AES, DES and RSA for Security. Global Journal of Computer Science and Technology Network, Web & Security. 13(15). 14 – 22.

Pressman, R. (2010). Software Engineering: A Practitioner’s Approach. (Edition 7th). McGraw-Hill. Avenue of the Americas, New York, USA.

Puttaswamy, N., Christopher, K. and Ben, Z. (2011). Silverline: Toward Data Confidentiality in Storage-intensive Cloud Applications. *Proceedings of the 2nd ACM Symposium on Cloud Computing*. 26-28 October. Cascais, 1-13.

Raj, P., Venkatesh, V. and Rengarajan, A. (2013). Software Engineering Frameworks for Cloud Computing Paradigm. (1st Edition). Springer-Verlag. Springer London Heidelberg New York Dordrecht.

Rajasekar, N. and Chris, I. (2010). Exploitation of Vulnerabilities in Cloud Storage. *Proceedings of The 1st International Conference on Cloud Computing, GRIDs, and Virtualization*. 21-26 November. Lisbon, 122-127.

Ranchal, R., Bharat, B., Lotfi, B. and Lilien, L. (2010). Protection of Identity Information in Cloud Computing without Trusted Third Party. *Proceedings of 2010 IEEE 29th Symposium on Reliable Distributed Systems*. 31 October – 3 November. New Delhi, 368-372.

Rivest, R., Shamir, A. and Adleman, L. (1978). A Method for Obtaining Digital Signatures and Public-Key Cryptosystems, *Communications of the ACM,* 21, 120 –

126. ACM.

Rocha, F. and Correia, M. (2011). Lucy in the Sky without Diamonds: Stealing Confidential Data in the Cloud. *Proceedings of 2011 IEEE/IFIP 41st International Conference on Dependable Systems and Networks Workshops (DSN-W)*. 27-30 June. Hong Kong, 129-134.

Rocha, F., Abreu, S. and Correia, M. (2011). The Final Frontier: Confidentiality and Privacy in the Cloud. *Computer*, 44 (9), 44 – 50. IEEE Computer Society.

Roshan, R., Rahul, D., Vaishali, S. and Saurabh, R. (2014). Assurance of Data Integrity in Multi-cloud Using CPDP Scheme. International Journal of Engineering Research and Applications, 4 (2), 262 – 267.

Salim, N., Mariyam, S., Safaai, D., Rose, A., Subariah, I., Roselina, S., Siti, Z., Azizah, R., Dayang, J., Nor, Z. and Juhana, S. (2010). *Handbook of Research Methods in Computing*. (1st Edition). Faculty of Computer Science and Information System. Universiti Teknologi Malaysia, Johor Malaysia.

Sathiyapriya, K., Malathi, D., Vijaya, K. and Nagadevi, S. (2013). A Study on Security Challenges and Issues in Cloud Computing. *International Journal of Engineering and Innovative Technology (IJEIT)*, 2 (7), 256 – 261.

Sattiraju, G., Mohan, S. and Mishra, S. (2013). IDRBT Community Cloud for Indian Banks. Proceedings of 2013 *International Conference on Advances in Computing, Communications and Informatics (ICACCI)*. 22-25 August. Mysore, 74-81.

Savu, L. (2011). Cloud Computing: Deployment Models, Delivery Models, Risks and Research Challenges. *Proceedings of 2011 International Conference on Computer and Management (CAMAN)*. 10-12 March. Wuhan, 1-4.

Seiger, R., Stephan, G. and Alexander, S. (2011). SecCSIE: A Secure Cloud Storage Integrator for Enterprises. *Proceedings of 2011 IEEE 13th Conference on Commerce and Enterprise Computing (CEC)*. 5-7 September. Luxembourg, 252-255.

Shucheng, Y., Cong, W., Kui, R. and Wenjing, L. (2010). Achieving Secure, Scalable and Fine-grained Data Access Control in Cloud Computing. *Proceedings of The 2010 30th International Conference on Computer Communications*. 14-19 March. San Diego, 1-9.

Somani, U., Lakhani, K. and Mundra, M. (2010). Implementing Digital Signature with RSA Encryption Algorithm to Enhance the Data Security of Cloud in Cloud

Computing. *Proceedings of 2010 1st Parallel Distributed and Grid Computing (PDGC)*. 28-30 October. Solan, 211-216.

Soni, M., Namjoshi, J. and Pillai, S. (2013). Robustness and Opportuneness based Approach for Cloud Deployment Model Selection. *Proceedings of 2013 International Conference on Advances in Computing, Communications and Informatics (ICACCI),* 207-212 August. Mysore, 207-212.

Soni, S. and Soni, A. (2013). Brief Analysis of Methods for Cloud Computing Key Management. *Journal of Information Engineering and Applications (JIEA),* 3 (6), 42 – 45. IISTE Publications.

Stamou, K., Jean-Henry, M., Benjamin, G. and Jocalyn, A. (2012). Service Level Agreement as a Service: Towards Security Risk Aware SLA Management. *Proceedings of 2012 2nd International Conference on Cloud Computing and Services Sciences (CLOSER)*. 18-21 April. Parto, 663-669.

Stefania, D., Alecsandru, P. and Emil, S. (2012). Homomorphic Encryption Schemes and Applications for a Secure Digital World. *Journal of Mobile, Embedded and Distributed Systems. (JMEDS),* 4 (4), 224 – 232.

Stipic, A. and Bronzin, T. (2012). How Cloud Computing is (not) Changing the Way We do BI. *Proceedings of the 2012 35th International Convention on MIPRO*. 21-25 May. Opatija, 1574-1582.

Sun, J. and Sha-sha, Y. (2011). The Application of Cloud Storage Technology in SMEs. *Proceedings of 2011 International Conference on E-Business and E-Government (ICEE),* 6-8 May. Shanghai, 1-5.

Sun, L., Zishan, D. and Guo, J. (2010). Research on Key Management Infrastructure in Cloud Computing Environment. *Proceedings of 2010 9th International Conference on Grid and Cooperative Computing (GCC)*. 1-5 November. Nanjing, 404-407.

Syam, P. and R. Subramanian. (2011). An Efficient and Secure Protocol for Ensuring Data Storage Security in Cloud Computing. *International Journal of Computer Science Issues (IJCSI),* 8 (6), 261 – 274.

Taeho, J., Xiang-Yang, L., Zhiguo, W. and Meng, W. (2013). Privacy Preserving Cloud Data Access with Multi-Authorities. *Proceedings of 2013 IEEE INFOCOM*. 14-19 April. Turin, 2625-2633.

Tripathi, A. and Mishra, A. (2011). Cloud Computing Security Considerations. *Proceedings of 2011 IEEE International Conference on Signal Processing,* *Communications and Computing (ICSPCC)*. 14-16 September. Xian, 1-5.

Ullrich, M., Hagen, K. and Lassig, J. (2012). Public Cloud Extension for Desktop Applications-Case Study of a Data Mining Solution. *Proceedings of 2012 2nd Symposium on Network Cloud Computing and Applications (NCCA)*. 3-4 December. London, 53-64.

Ushadevi, R. and Rajamani, V. (2012). A Modified Trusted Cloud Computing Architecture based on Third Party Auditor (TPA) Private Key Mechanism. *International Journal of Computer Applications*, 58 (22), 1 – 9. IJCA Publications.

Vahid, A., Seyed, T. and Kamran, Z. (2012). A Survey on Cloud Computing and Current Solution Providers. *International Journal of Application or Innovation in Engineering and Management (IJAIEM),* 1 (2), 226 – 233.

Varalakshmi, P. and Deventhiran, H. (2012). Integrity Checking for Cloud Environment using Encryption Algorithm. *Proceedings of 2012 International Conference on Recent Trends In Information Technology (ICRTIT)*. 19-21 April. Chennai, 228-232.

Victor, M., Peter, M., Aida, O. and Gunka, A. (2013). Eliciting Risk, Quality and Cost Aspects in Multi-cloud Environments. *Proceedings of 2013 The 4th International Conference on Cloud Computing, GRIDs, and Virtualization*. 27 May – 1 June. Valencia, 238-243.

Wang, B., Baochun, L., Hui, L. and Fenghua, L. (2013). Certificateless Public Auditing for Data Integrity in the Cloud. *Proceedings of 2013 IEEE Conference on Communications and Network Security (CNS)*. 14-16 October. National Harbor, 136-144.

Wang, W., Yin, H., Chen, L., Huang, X. and Sunar, B. (2013). Exploring the Feasibility of Fully Homomorphic Encryption. *Transactions on Computers,* 8 (99), 1 – 10. IEEE Computer Society.

Wei, L., Haishan, W., Xunyi, R. and Sheng, L. (2012). A Refined RBAC Model for Cloud Computing. *Proceedings of 2012 IEEE/ACIS 11th International Conference on Computer and Information Science (ICIS)*. 30 May-1 June, Shanghai, 43-48.

Xiaoyong, L. and Junping, D. (2013). Adaptive and Attribute-based Trust Model for Service Level Agreement Guarantee in Cloud Computing. *Information Security,* 7 (1), 39 – 50. Institute of Engineering and Technology.

Xing, W., Ming, W., Zhang, W. and Yike, G. (2012). Cloud Program with a Pricing

Strategy for IaaS in Cloud Computing. *Proceedings of 2012 IEEE 26th International Parallel and Distributed Processing Symposium Workshops & PhD Forum (IPDPSW)*. 21-25 May. Shanghai, 2316-2319.

Yen-Hung, K., Yu-Lin, J. and Juei-Nan, C. (2013). A Hybrid Cloud Storage Architecture for Service Operational High Availability. *Proceedings of 2013 IEEE 37th Annual Computer Software and Applications Conference Workshops (COMPSACW)*. 22-26 July. Japan, 487-492.

Yogesh, K., Rajiv, M. and Harsh, S. (2011). Comparison of Symmetric and Asymmetric Cryptography with Existing Vulnerabilities and Countermeasures. *International Journal of Computer Science and Management Studies (IJCSMS)*, 11 (2), 60 – 63.

Yu-Hui, W. (2011). The Role of SaaS Privacy and Security Compliance for Continued SaaS Use. *Proceedings of 2011 7th International Conference on Networked Computing and Advanced Information Management (NCM).* 21-23 June. Gyeongju, 303-306.

Zeng, S. and Xu, J. (2010). The Improvement of PaaS Platform. *Proceedings of 2010 1st International Conference on Networking and Distributed Computing (ICNDC)*. 21-24 October. Hangzhou, 156-159.

Zhang, J. and Zhang, N. (2011). Cloud Computing-based Data Storage and Disaster Recovery. *Proceedings of 2011 International Conference on Future Computer Science and Education (ICFCSE)*. 20-21 August. Xian, 629-632.

Zingham, M. and Saqib, S. (2013). Software Engineering Frameworks for Cloud Computing Paradigm. (1st Edition). Springer-Verlag. Springer London Heidelberg New York Dordrecht.

Zissis, D. and Lekkas, D. (2012). Addressing Cloud Computing Security Issues. *Future Generation Computer Systems (FGCS)*, 28 (3), 583 – 592. Elsevier.

Zlatko, S., Eva, L., Antonio, C., Marcos, O. and Vjeran, S. (2012). Performing Systematic Literature Review in Software Engineering. *Proceedings of 2012 Central European Conference on Information and Intelligent Systems*. 19-21 September. Croatia, 441-447.