TRUSTED CLOUD COMPUTING FRAMEWORK IN CRITICAL INDUSTRIAL APPLICATION

MERVAT ADIB BAMIAH

UNIVERSITI TEKNOLOGI MALAYSIA

TRUSTED CLOUD COMPUTING FRAMEWORK IN CRITICAL INDUSTRIAL APPLICATION

MERVAT ADIB BAMIAH

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

This research is dedicated to my beloved family and
Dr. Mohammad Imran Bamiah.

ACKNOWLEDGEMENT

I would like to express my utmost gratitude to ALLAH (SWT), the God Almighty, for granting me health, knowledge, strength, ability, and patience to accomplish this research. I wish to express my sincere appreciation to my main supervisor, Dr. Suriayati Chuprat for her continuous support and valuable feedbacks that enabled me to achieve the research milestones within the required time-frame. I am thankful also to my external research industry supervisor Dr. Jamalul-lail Ab Manan for his continuous support and valuable feedbacks in reviewing, improving and evaluating my research. I am extremely thankful to Dr. Mohammad Imran Bamiah for his financial and caring support. Also I am grateful to every member of my family who stood by me with kind and love during the PhD journey.

ABSTRACT

Cloud computing facilitates instant online unlimited access to data and computing resources, ubiquitously and pervasively through its various service delivery and deployment models. Despite the significant advantages of cloud computing, still there are concerns regarding Security, Privacy and Trust (SPT) that resulted from consumers' loss of control over their confidential data since they outsource it to cloud with no knowledge of storage location or who is accessing and maintaining it. This raises the risks of insider and outsider threats besides the data breach and misuse. A Trusted Cloud Computing Framework (TCCF) is designed to overcome these SPT concerns. TCCF proposes the use of Trusted Computing Group (TCG) technologies including, Trusted Platform Module (TPM), Virtual Trusted Platform Module (VTPM), Self-Encrypting Drives (SEDs), Trusted Network Connect (TNC) and Trusted Software Stack (TSS) to initiate a trusted cloud computing platform. In addition, a Multi-Factor Authentication Single Sign on Role Base Access Control (MFA-SSO-RBAC) prototype was developed using a strict security controls. Furthermore, an additional context for cloud Service Level Agreement (SLA) was proposed to support the framework and to ensure the trustworthiness of the cloud computing services to be adopted in critical information industries specifically healthcare sector. TCCF was evaluated by developing a prototype, comprehensive comparison with previous work, compliance with standards and a survey from cloud computing, healthcare and IT security experts. Feedbacks of experts were satisfactory and they agreed with 94% on the overall security techniques used to secure the TCCF three layers. The evaluation proves that TCCF assists in optimizing the trust on cloud computing to be adopted in healthcare sector for best practices.

ABSTRAK

Pengkomputeran awan memudahkan akses dalam talian segera tanpa had terhadap data dan sumber pengkomputeran secara merata dan merebak melalui pelbagai tawaran penyampaian perkhidmatan dan model penempatan. Walaupun pengkomputeran awan mempunyai kelebihan yang signifikan, masih terdapat beberapa isu berkaitan Keselamatan, Kerahsiaan dan Kepercayaan (SPT) disebabkan oleh kehilangan kawalan terhadap data sulit pengguna itu sendiri. Keadaan ini berlaku kerana mereka menggunakan khidmat penyumberan luar awan tanpa mengetahui sebarang maklumat tentang lokasi sebenar data dan juga siapa yang mencapai dan menguruskan maklumat tersebut. Ini akan meningkatkan risiko ancaman dalaman dan luaran selain kebocoran dan penyalahgunaan data. Rangka Kerja Pengkomputeran Awan Dipercayai (TCCF) direka bentuk untuk mengatasi kebimbangan SPT. TCCF mencadangkan penggunaan Teknologi Pengkomputeran Kumpulan Dipercayai (TCG) termasuk Modul Platform Dipercayai (TPM), Modul Platform Dipercayai Maya (VTPM), Pemacu Penyulitan Diri (SEDs), Rangkaian Sambung Dipercayai (TNC) dan Perisian Timbunan Dipercayai (TSS) untuk memulakan platform pengkomputeran awan yang dipercayai. Di samping itu, prototaip Pengesahan Tandatangan Tunggal Pelbagai-Faktor pada Kawalan Akses Berasaskan Peranan (MFA-SSO-RBAC) dibangunkan menggunakan kawalan keselamatan yang ketat. Seterusnya, konteks tambalan untuk Perjanjian Tahap Perkhidmatan (SLA) awan dicadangkan untuk menyokong rangka kerja dan memastikan kebolehpercayaan perkhidmatan awan yang akan diterima pakai dalam industri maklumat kritikal khususnya sektor penjagaan kesihatan. TCCF telah dinilai dengan membangunkan prototaip, perbandingan komprehensif dengan kerja sebelumnya, kepatuhan kepada standard dan kaji selidik daripada pakar-pakar pengkomputeran awan, penjagaan kesihatan, dan keselamatan IT. Maklum balas daripada pakar adalah memuaskan hati dan setuju secara purata 94% daripada keseluruhan teknik keselamatan yang digunakan untuk memelihara tiga lapisan TCCF. Penilaian tersebut membuktikan bahawa TCCF dapat membantu meningkatkan keyakinan terhadap amalan terbaik dalam pengkomputeran awan untuk digunakan dalam sektor penjagaan kesihatan.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

AAs	-	Attribute Authorities
ABE	-	Attribute Based Encryption
AES	-	Advanced Encryption Standard
AIK	-	Attestation Identity Key
API	-	Application Programming Interface
BIOS	-	Basic Input Output System
BYOD	-	Bring Your Own Device
CA	-	Certificate Authority
CASE	-	Cloud Aided Software Engineering
CRTM	-	Core Root of Trust for Measurement
CSA	-	Cloud Service Administrator, Cloud Security Alliance
CSCC	-	Cloud Standards Customer Council
CSP	-	Cloud Service Provider
CSU	-	Cloud Service User
DDOS	-	Distributed Denial of Service
DLC	-	Data Life Cycle
DOS	-	Denial of Service
EAL4+	-	Evaluation Assurance Level 4+
E-Health	-	Electronic Health
EHRs	-	Electronic Health Records
EK	-	Endorsement Key
EMRs	-	Electronic Medical Records
FISMA	-	Federal Information Security and Management Act
HHS	-	Health and Human Services
HIPAA	-	Health Insurance Portability and Accountability Act
HIT	-	Health Information Technology

HITECH	-	Health Information Technology for Economic and Clinical Health
HSP	-	Healthcare Service Provider
HTCCF	-	Healthcare Trusted Cloud Computing Framework
HTTPS	-	Hypertext Transfer Protocol Secure
IaaS	-	Infrastructure as a Service
IAM	-	Identity and Access Management
IDPS	-	Intrusion Detection and Prevention Systems
IDS	-	Intrusion Detection systems
IEC	-	International Electro-technical Commission
IF-MAP	-	Interface for Metadata Access Points
IOT	-	Internet of Things
IPS	-	Intrusion Prevention Systems
IPSec	-	Internet Protocol Security
ISO	-	International Organization for Standardization
IT	-	Information Technology
ITSG-33	-	Information Technology Security Guidance
KVM	-	Kernel-based Virtual Machines
MA-ABE	-	Multi Authority Attribute Based Encryption
MFA	-	Multi-Factor Authentication
ML	-	Measurement List
NAC	-	Network Access Control
NGFW	-	Next Generation Firewalls
NIST	-	National Institute of Standards and Technology
OCR	-	Office for Civil Rights
ONC	-	Office of National Coordinator
OS	-	Operating System
OTP	-	One-Time PIN
P1-MFA	-	Policy (1) Multi-Factor Authentication
PaaS	-	Platform as a Service
PCI	-	Payment Card Industry
PCM	-	Platform Configuration Measurements
PCRs	-	Platform Configuration Registers
PDA	-	Personal Digital Assistant
PHI	-	Personal Health Information

PHRs	-	Personal Health Records
PKI	-	Public Key Infrastructure
PVI	-	Private Virtual Infrastructure
QoS	-	Quality of Service
RBAC	-	Role Base Access Control
RFID	-	Radio Frequency Identification
RNG	-	Random Number Generator
RSA	-	Rivest, Shamir, and Adelman
RTM	-	Root of Trust for Measurement
RTR	-	Root of Trust for Reporting
RTS	-	Root of Trust for Storage
SaaS	-	Software as a Service
SAML	-	Security Assertion Markup Language
SDLC	-	Software Development Life Cycle
SED	-	Self-Encrypting Drives
SFTP	-	Secure File Transfer Protocol
SHA	-	Secure Hash Algorithm
SLA	-	Service Level Agreement
SLR	-	Systematic Literature Review
SML	-	Stored Measurement Log
SOA	-	Service Oriented Architecture
SoD	-	Security on Demand
SPT	-	Security, Privacy and Trust
SRK	-	Storage Root Key
SSH	-	Secure Shell
SSO	-	Single Sign On
SSL	-	Secure Sockets Layer
TC	-	Trusted Computing/Trusted Coordinator
TCB	-	Trusted Computing Base
TCCF	-	Trusted Cloud Computing Framework
TCCP	-	Trusted Cloud Computing Platform
TCCI	-	Trusted Cloud Computing Infrastructure
TCG	-	Trusted Computing Group
TCP	-	Trusted Computing Platform

TEE	-	Trusted Execution Environment
TLS	-	Transport Layer Security
TNC	-	Trusted Network Connect
TOS	-	Trusted Operating System
TP	-	Trusted Platform
TPM	-	Trusted Platform Module
TM	-	Trust Monitor
TSS	-	Trusted Software Stack
TVCCE	-	Trusted Virtual Cloud Computing Environment
TVD	-	Trusted Virtual Domain
TVDc	-	Trusted Virtual Data Center
TVEM	-	Trusted Virtual Environment Module
TVMM	-	Trusted Virtual Machine Monitor
US	-	United States
USD	-	United States Dollar
UTE	-	User Trusted Entity
VDc	-	Virtual Data Center
VF	-	Virtual Firewall
VLAN	-	Virtual Local Area Network
VM	-	Virtual Machine
VMM	-	Virtual Machine Monitor
VPN	-	Virtual Private Network
VTN	-	Virtual Trust Network
vTPM	-	Virtual Trusted Platform Module

LIST OF APPENDICES

CHAPTER 1

INTRODUCTION

1.1 Overview

Cloud computing has emerged as a business IT solution that provides a new way to manage and deliver automated computing services to consumers via the Internet (Shawish and Salama, 2014). It has evolved from various technologies such as Distributed, Grid, Utility computing and Service Oriented Architecture (SOA), by combining pool of abstracted, dynamic scalable, managed computing IT resources (Chen and Hoang, 2011). Cloud computing reduces capital expenditure and provides availability of real time services on pay-per-use basis (Mahmood and Saeed, 2013). Businesses including government, banking and healthcare require industry specific cloud computing structure to fulfill their IT needs. Each industry has its own rules and regulations. For example, healthcare sector is regulated by the Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH) that are not encountered in standard public cloud frameworks. Healthcare as one of the critical information industries requires a trusted cloud computing solution which provides increased information security, flexibility and accessibility (Smith, 2013**)**. This conducted research focuses on designing a Trusted Cloud Computing Framework (TCCF) to be adopted in critical information industries mainly healthcare sector for improving its Quality of Services (QoSs), just-in-time, in a cost effective manner.

1.2 Problem Background

Despite the numerous benefits of cloud computing in terms of scalability, resilience, adaptability, connectivity, virtualization and high performance, still there are several Security, Privacy and Trust (SPT) concerns that made critical information industries reluctant to deploy cloud computing for best business practices (Thilakanathan *et al.*, 2013; Hsing, 2012; Servos, 2012; Shini *et al*., 2012; Khatua *et al*., 2011; Pearson and Benameur, 2010; Takabi *et al*., 2010). These SPT concerns resulted from the loss of' consumers direct control on their confidential data and computing resources when they outsource them to a remote third Cloud Service Provider (CSP) who facilitates the IT infrastructure, applications and management as services per demands. Since consumers' data are at cloud storage, they do not know who is managing or accessing their data and where their storage locations are, which may cause a threat of data breach or misuse (Taeho *et al*., 2013; Ermakova and Fabian, 2013). Figure 1.1 demonstrates that data privacy and security are consumers' top concerns with 41% which necessitate a trusted cloud solution that overcomes these concerns over deploying cloud computing.

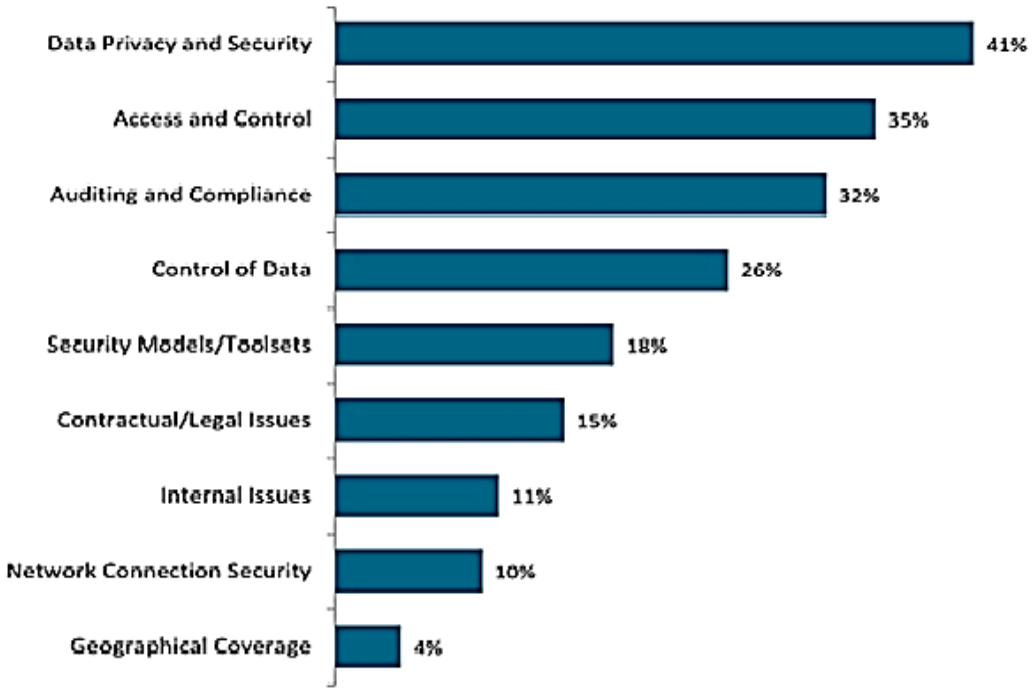

Figure 1.1: Top Cloud Computing Concerns (ffoulkes, 2014)

1.3 Problem Statement

Consumers need to be assured that their privacy is preserved and their data are secured besides complying with rules and regulations. The problem statement that needs to be addressed is as follows

How to design a TCCF that maintains the security and privacy of consumers' confidential data as well as complies with rules and regulations in order to be trusted and deployed in critical information industries such as healthcare sector?

Designing a trusted cloud solution and solving the research problem statement will be achieved by answering the following research questions:

i. What are the current cloud computing security and privacy concerns that prevent critical information industries from trusting and adopting cloud computing?

ii. How to design a cloud computing framework that can fulfill the security and privacy concerns as well as assist in increasing the trust on cloud computing to be adopted in critical information industries?

iii. How to evaluate and ensure that the designed cloud computing framework will assist in overcoming the security and privacy concerns as well as increases the trust on cloud computing to be adopted critical information industries?

1.4 Research Aims and Objectives

According to Trusted Computing Group (TCG) (Donovan and Visnyak 2011), "*There is no comprehensive framework exists to describe the business/mission needs and validate compliance of the entire solution set in compliance with open standards*". The aim of this study is to design a TCCF that overcomes the SPT concerns to be implemented in critical information industries specifically healthcare sector for best

business practices. In order to achieve the research aim, the following objectives should be accomplished.

i. To identify and critically analyze the current cloud computing security and privacy concerns that prevent critical information industries from trusting and adopting cloud computing.

ii. To design a cloud computing framework that can fulfill the security and privacy concerns as well as assist in increasing the trust on cloud computing to be adopted in critical information industries.

iii. To evaluate and ensure that the designed cloud computing framework will assist in overcoming the security and privacy concerns as well as increases the trust on cloud computing to be adopted critical information industries.

1.5 Scope of Research

The scope of this research focuses on designing TCCF for critical information industries specifically healthcare sector as a case study. It proposes secures cloud computing infrastructure based on TCG international standards technologies including Trusted Platform Module (TPM), Trusted Software Stack (TSS), virtual Trusted Platform Module (vTPM), Trusted Network Connect (TNC) and Self Encrypting Drives (SEDs) to initiate a trusted cloud computing platform taking into consideration HIPAA security and privacy rules and regulations as well as the National Institute of Standards and Technology (NIST) Special Publication 800-144 Guidelines (Jansen and Grance, 2011). Moreover, this study proposes a customized cloud Service level Agreement (SLA) by including additional context to it regarding healthcare requirements to support the framework and to make it more trustworthy. However, due to resource and time limitations, TCCF was designed and only the authentication part was implemented.

1.6 Significance of Research

This research contributes to software engineering, public and scientific fields as well as to the body of knowledge as follows:

i. In software engineering field, this research contributes in understanding the cloud computing critical industries requirements. The TCCF contributes in overcoming the SPT concerns and providing trusted cloud services based on secure by design hardware and software execution environment as per experts expectations. Taking into consideration the trust aspects (security, privacy, accountability, and availability) (Muppala *et al*., 2012). Furthermore, by using cloud computing platform, software developers and programmers will be provided with the latest IT tools as a service on-demand that will accelerate the innovation of next generation smart devices, beside facilitating software development and delivery which enables software engineering researchers to study distributed multilateral software development (Østerlie, 2009).

ii. In public field, this research proposes a TCCF that overcomes the SPT concerns to be deployed in critical information industries specifically healthcare sector by providing secure cloud services on demand just-in-time in a cost effective manner that will enhance the QoSs provided to public.

iii. This research adds to science and technology fields as it is based on the usage of the software engineering methodology in gathering user requirements, designing, developing, implementing and testing the systems beside documentation (Bourque and Fairley, 2014). Moreover, providing an agile way of sharing the information in secure and trusted manner ubiquitously and pervasively through the use of cloud computing. In addition, also to addressing the challenge in designing a secure and trusted cloud computing framework for critical information industries including healthcare sector.

iv. This study adds to the body of knowledge through publications in journals and conferences for global recognition. Also, the thesis documentation will assist other researchers in both fields' software engineering and IT.

1.7 Research Contributions

Cloud computing facilitates consumers, users and software engineers the use of computing, storage and other resources over the network. It accelerates real time communication in software development projects that are scattered across the globe in cost effective manner (Munch, 2013). Cloud computing dynamic virtualized multi-tenant nature has raised enormous challenges for software engineers to design and develop trusted cloud applications, platforms, and infrastructures that provide secure services to critical information industries focusing on healthcare sector. In the domain of software engineering, a new term has emerged specifically to cloud computing which is named Cloud Aided Software Engineering (CASE 2.0) that applies the Software Development Life Cycle (SDLC) according to cloud specification's starting with requirements gathering and analysis until development and deployment phases (Zingham and Saqib, 2013).

The Healthcare Trusted Cloud Computing Framework Multi Factor Authentication Single Sign on Role Base Access Control (HTCCF-MFA-SSO-RBAC) prototype is conducted based on the CASE 2.0. software engineering development process Therefore, this research contributes in the field of software engineering by providing a TCCF which secure the overall cloud infrastructure, data, communication and access, bounded by a customized SLA and complies with standards. This research has several contributions to overcome the SPT concerns in order to optimize the trust of consumers to adopt cloud computing as follows:

Contribution 1: TCCF proposes security by design multi-layered, defense-in-depth approach that covers all cloud layers in addition to access and data. It utilizes the latest security standards and mechanisms for virtual, physical and application layers, as well as TCCF considers robust security controls such as firewalls, anti-malware, anti-virus and Intrusion Detection and Prevention Systems (IDPSs).

Contribution 2: TCCF proposes the integration of TCG technologies for enhanced security, privacy and interoperability. TCG's Trusted Computing Platform (TCP) will be used to perform authentication, also to ensure confidentiality and integrity in cloud computing environment.

Contribution 3: TCCF proposes an additional context to be added to SLA according to healthcare requirements as a critical information industry which has its own requirements, rules and regulations that need to be guaranteed in the SLA.

Contribution 4: TCCF proposes the compliance with HIPAA data security and privacy rules and regulations.

Contribution 5: TCCF enforces data encryption in SLA at rest, while in the process and in transmit with the latest efficient encryption mechanisms in order to provide optimized level of data confidentiality besides complying with rules and regulations. Furthermore, TCCF also includes data backup in SLA and in the design as a separate phase for securing data availability and disaster recovery.

Contribution 6: TCCF proposes a robust password policy for usage and storage.

Contribution 7: TCCF offers a Multi-Factor Authentication Single Sign on Role Base Access Control (MFA-SSO-RBAC) prototype for critical information industries specifically healthcare sector that will secure the access against illegal and malicious threats and complies with Healthcare Insurance Portability and Accountability Act (HIPAA) for various types of users' access based on their roles and organizations' policy with least privileges.

1.8 Thesis Organization

This thesis focuses on maintaining SPT in the TCCF to be used in healthcare sector. Complete research is organized into six chapters as follows:

Chapter 1 Introduction: This chapter explores the background of the problem which is about consumers' lack of trust in cloud computing. Research questions, aims, and objectives were formulated as a guide for further studies in the following chapters in order to design and evaluate TCCF. The scope of the research has been identified as to conduct the research within the resources and time frame available. The rest of the chapter discusses the significance and contributions of the study.

Chapter 2 Literature Review: This chapter discusses cloud computing definition and concerns as well as the cloud current standards which the research will be based on. It provides an overview literature review of the research topic in relation to the existing cloud implementations in healthcare sector as a case study with more justification on the problems related to these projects. In addition to discussing cloud computing and TCG technologies that are going to be implemented in the research framework, beside the identification of the cloud SLA current status, in order to customize it regarding healthcare specifications. Moreover, HIPAA will also be discussed for designing the framework compliance requirements.

Chapter 3 Research Methodology: This chapter discusses the research activities and outcomes, research methodology guidelines, study population sampling methods, data collection methods, research limitation as well as planning and schedule.

Chapter 4 Trusted Cloud Computing Framework Design: This chapter introduces the components and designing stages of TCCF for critical information industries. The multi-layered security by design TCCF integrates TCG technologies and other security controls for overcoming the SPT concerns of cloud computing. Cloud Data Life Cycle security is also discussed in this chapter.

Chapter 5 Development of the Multi-Factor Authentication SSO Role Based Access Control Prototype: This chapter discusses the development process of the TCCF evaluation MFA prototype based on the CASE 2.0 approach.

Chapter 6 Evaluation of Trusted Cloud Computing Framework: This chapter introduces the evaluation methods of TCCF that include literature review comparison, a questionnaire survey based on experts' feedbacks, and the compliance with HIPAA and CSA standards. The rest of the chapter presents a critical analysis of the survey and other evaluation methods results.

Chapter 7 Conclusion and Future Work: This chapter summarizes the whole study based on data analysis and interpretation. It discusses detailed research contributions, limitations, and future work directions.

1.9 Summary

The increasing demands of industries for enhanced technology solutions including healthcare sector as a case study for critical information industries, and the increasing advent of advanced smart technologies with limited healthcare resources raised the need to balance the limited healthcare resources and unlimited growth of the healthcare needs. Cloud computing improves the delivery of healthcare services and enables effective and efficient achievement of coordination of healthcare medication services in agile cost effective way. In spite of cloud benefits, still there are some issues related to security and privacy that acts as a barrier against trusting and deploying cloud computing in healthcare sector for best business practices. Throughout this chapter, critical discussion on problem background, research questions, objectives, scope and significance have been conducted.

REFERENCES

Abbadi, I., Deng, M., Nalin, M., Martin, A., Petkovic, A. and Baroni, I. (2011). Trustworthy Middleware Services in the Cloud. *In Proceedings of the 2011 third international workshop on Cloud data management (CloudDB '11)*. ACM, 33-40. DOI: 10.1145/2064085.2064094.

Abbadi, I. (2011a). Middleware Services at Cloud Application Layer. *Proceedings of the 2011 Second International Workshop on Trust Management in P2P Systems (IWTMP2PS '11)*. Lecture Notes in Computer Science. Springer-Verlag, Berlin, 557-571. DOI: 10.1007/978-3-642-22726-4_58.

Achemlal, M., Gharout S., and Gaber, C. (2011). Trusted Platform Module as an Enabler for Security in Cloud Computing. *Proceedings of the 2011 Network and Information Systems Security (SAR-SSI)*. 18-21 May 2011. La Rochelle: IEEE, 1–6. DOI: 10.1109/SAR-SSI.2011.5931361.

Adebiyi, A., Arreymbi, J. and Imafidon, C. (2012). Security Assessment of Software Design using Neural Network, *International Journal of Advanced Research in Artificial Intelligence*, 1 (4: 1-7. SAI Publications.

Ahmad, B. and Mohamed, S. (2011). Implementation of Trusted Computing Technologies in Cloud Computing. *International Journal of Research and Reviews in Information Sciences (IJRIS)*. 1(1):1-3. Science Academy Publisher.

Ahmed, A. (2012). Meeting PCI DSS When Using a Cloud Service Provider. *ISACA Journal* 5:1-30.

Alley, D., Ahmed, T., Androvich, J., Archibald, S., Andrew S., Fultz, N., Heusser, S., Keahey, R., Krogue, K., Menon, R., Morgenthal, J., Rice, A., Roberts, D., Ryan, C., Ulmer, S., Wheeler, H. and Wilson, K. (2012). The Cloud Computing Guide for Healthcare. *Focus Research*. Microsoft, 1-22.

Almorsy, M., Grundy, J. and Ibrahim, S. (2011). Collaboration-Based Cloud Computing Security Management Framework. *Proceedings of the 2011 Cloud Computing (CLOUD)*. 4-9 July 2011. Washington, DC. IEEE, 364-371. DOI: 10.1109/CLOUD.2011.9.

Almutairi, A., Sarfraz, M., Basalamah, S., Aref, W. and Ghafoor, A. (2012). A Distributed Access Control Architecture for Cloud Computing. *Proceedings of the 2012 Software*. 20 February 2012. IEEE Computer Society. 29(2): 36 – 44. DOI: 10.1109/MS.2011.153.

Alshehri, S., Radziszowski, S. and Raj, R. (2012). Secure Access for Healthcare Data in the Cloud Using Ciphertext-Policy Attribute-Based Encryption. *Proceedings of the 2012 Data Engineering Workshops (ICDEW), 2012 IEEE 28th International Conference on.* 1-5 April 2012. Arlington, VA. IEEE, 143-146. DOI: 10.1109/ICDEW.2012.68.

AlZain, M., Pardede, E., Soh, B. and Thom, J. (2012). Cloud Computing Security: From Single to Multi-clouds. *Proceedings of the 2012 45th Hawaii International Conference on. System Science (HICSS)*. 4-7 January. 2012. Maui, HI. IEEE, 5490–5499. DOI: 10.1109/HICSS.2012.153.

Anderson, J. (2011). The Top 10 Strategic Considerations to Address in a Government Solicitation for Cloud Computing Services. Retrieved on January 13, 2014, from http://safegov.org/2011/12/12/the-top-10-strategic-considerations-to-address-in-a-government-solicitation-for-cloud-computing-services

Angelov, S., Trienekens, J. and Kusters, R. (2014). A survey on design and usage of Software Reference Architectures. Retrieved October 23, 2014, from http://purl.tue.nl/24821036841001.pdf

Arora, P., Wadhawan, R. and Ahuja, S. (2012). Cloud Computing Security Issues in Infrastructure as a Service. *International Journal of Advanced Research in Computer Science and Software Engineering (IJARCSSE)*. 2 (1), January 2012. ISSN: 2277 128X.

Ashford (2011). Self-encrypting drives: SED the best-kept secret in hard drive encryption security. *Computer Weekly* Retrieved on November 18, 2013, from http://www.computerweekly.com/feature/Self-encrypting-drives-SED-the-best-kept-secret-in-hard-drive-encryption-security

Ayad, M., Rodriguez, H. and Squire, J. (2012). Addressing HIPAA Security and Privacy Requirements in the Microsoft Cloud. Retrieved on December 23, 2013, fromhttp://smb.blob.core.windows.net/smbstaging/Content/Microsoft_Cloud_Healthcare_HIPAA_Security_Privacy.pdf

Baaskar, R. and Gomathi, A. (2012). A Framework for Security Based Cloud by using Trusted Computing. *International Journal of Advanced Research in Computer Science and Software Engineering (IJARCSSE)*. 2:36-40. December – 2012. ISSN: 2277 128X.

Badger, L., Grance, T., Patt-Corner, R. and Voas, J. (2012). Cloud Computing Synopsis and Recommendations. *National Institute of Standards and Technology (NIST).* Special Publication 800-146, Computer Security Division, 1-81.

Bamiah, M., Brohi, S., Chuprat, S. and Ab Manan, J. (2013). Trusted Cloud Computing Framework for Healthcare Sector. *Journal of Computer Science*. 10 (2):240-250. DOI: 10.3844/jcssp.2014.240.250. Science Publications.

Bamiah, M. (2013a) Evaluating Trusted Cloud Computing Framework for Healthcare. LinkedIn. Retrieved on October 8, 2014, from https://www.linkedin.com/nhome/updates?topic=5810666560951848960.

Bamiah, M., Brohi, S., Chuprat, S., and Brohi, M. (2012). Cloud Implementation Security Challenges. *Proceedings of the 2012 Cloud Computing Technologies, Applications and Management (ICCCTAM)*. 8-10 December. 2012. Dubai. IEEE, 174–178. DOI:10.1109/ICCCTAM.2012.6488093.

Bamiah, M., Brohi, S., Chuprat, S. and Ab Manan, J. (2012a). A Study on Significance of Adopting Cloud Computing Paradigm in Healthcare Sector. *Proceedings of the 2012 Cloud Computing Technologies, Applications and Management (ICCCTAM)*. 8-10 December, 2012. Dubai. IEEE, 65–68. DOI:10.1109/ICCCTAM.2012.6488073.

Bamiah, M., Brohi, S. and Chuprat, S. (2012b). Using Virtual Machine Monitors To Overcome The Challenges Of Monitoring And Managing Virtualized Cloud Infrastructures. Proc. SPIE 8349, *Proceedings of the 2012 Fourth International Conference on Machine Vision (ICMV 2011).* Machine Vision; Image Processing, and Pattern Analysis, 83491M. 11 January, 2012. DOI:10.1117/12.920880.

Bamiah, M. and Brohi, S. (2011a). Exploring the Cloud Deployment and Service Delivery Models. *International Journal of Research and Reviews in Information Sciences (IJRRIS)*. 1 (3):77- 80. September 2011, Science Academy Publisher. ISSN: 2046-6439.

Banirostam, H., Hedayati, A., Zadeh, A. and Shamsinezhad, E. (2013). A Trust Based Approach for Increasing Security in Cloud Computing Infrastructure. *Proceedings of the 2013 Computer Modelling and Simulation (UKSim)*. 10-12 April 2013. Cambridge. IEEE, 717 – 721. DOI:10.1109/UKSim.2013.39.

Barua, M., Liang, X., Lu, R. and Shen, X. (2011). ESPAC: Enabling Security and Patient-centric Access Control for e-Health in Cloud Computing. *International Journal of Security and Networks (IJSN).* 6 (2/3):67–76. Inderscience Publishers.

Basit, A. (2009). *Guide To Trusted Computing*. *Approaches for Attesting Virtualized Environments*. Master Thesis. Royal Institute of Technology, Sweden.

Batchu, S., Chaitanya, J., Sagar. N. and Patnala, E. (2013). A study on Security Issues Associated with Public Clouds in Cloud Computing. *International Journal of Advanced Computer Technology (IJACT)*. 2(2):28-38. ISSN: 2319-7900.

Baudoin, C., Flynn, J., McDonald, J., Meegan, J., Salsburg, M. and Woodward, S. (2013). Public Cloud Service Agreements: What to Expect and What to Negotiate. *Cloud Standards Customer Council*.

Begum, R., Kumar, R. and Kishore, V. (2012). Data Confidentiality Scalability and Accountability (DCSA). *International Journal of Advanced Research in Computer Science and Software Engineering (IJARCSSE)*.2(11):200-206, November 2012. ISSN: 2277 128X.

Behl, k. and Behl, A. (2012). An Analysis of Cloud Computing Security Issues. *Proceedings of the 2012 Information and Communication Technologies (WICT), 2012 World Congress on*. October. 30 2012-November. 2 2012. Trivandrum. IEEE, 109 – 114. DOI: 10.1109/WICT.2012.6409059.

Benkhelifa, E. and Dayan, F. (2014). On a Real World Implementation of Advanced Authentication Mechanism in a Multi-Tenant Cloud Service Delivery Platform. *Proceeding of the* 2014 *5th International Conference on Information and Communication Systems (ICICS)*. 1-3 April 2014. Irbid. IEEE, 1-6. DOI:10.1109/IACS.2014.6841944.

Berger, S., C´aceres, R., Goldman, K., Perez, R., Sailer, R. and Doorn, L. (2006). VTPM: Virtualizing The Trusted Platform Module. *In Proceedings of the 15th conference on USENIX Security Symposium (USENIX-SS'06)*, 15(21):187- 196. USENIX Association, ACM.

Botero, D. (2013). *Pwnetizer: Improving Availability in Cloud Computing through Fast Cloning and I/O Randomization*. Master Thesis. Princeton University.

Bourque, P. and Fairley, R.E (2014). Guide to the Software Engineering Body of Knowledge, Version 3.0, IEEE Computer Society, 2014; www.swebok.org.

Bowman, D. (2013). Cloud adoption slower in healthcare than in other industries. Health Information Technology *Fierce Health IT*. Retrieved on December 2, 2013, from http://www.fiercehealthit.com/story/cloud-adoption-slower-healthcare-other-industries/2013-02-15

Brink, D. (2012). End Point Security. Hardware Root of Trust. *Aberdeen Group, Inc*. Retrieved on November 15, 2013, from http://www.trustedcomputinggroup.org/files/static_page_files/E8B61748-1A4B-B294-D0BD6A4ACA7E04FC/0331-7080-RB-HWRoT-DB-02-NSP.pdf

Brohi, S., Bamiah, A., Chuprat, S. and Ab Manan, J. (2013), Design And Implementation of Privacy Preserved Off-Premises Cloud Storage. *Journal of Computer Science*. 10 (2): 210-223. DOI: 10.3844/jcssp.2014.210.223.

Brohi, S.; Bamiah, M.; Brohi, M. and Kamran, R. (2012). Identifying and Analysing Security Threats to Virtualized Cloud Computing Infrastructures. *Proceedings of the 2012 Cloud Computing Technologies, Applications and Management (ICCCTAM)*. 8-10 December. 2012. Dubai. IEEE, 151–155. DOI:10.1109/ICCCTAM.2012.6488089.

Brohi, S. Bamiah, M.; Chuprat, S. and Ab Manan, J. (2012a). Towards an Efficient and Secure Educational Platform on Cloud Infrastructure. *Proceedings of the 2012 Cloud Computing Technologies, Applications and Management (ICCCTAM)*. 8-10 December. 2012. Dubai. IEEE, 145–150. DOI:10.1109/ICCCTAM.2012.6488088.

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'11)*. 8 (2): 286 – 290. 2011. ISSN: 2230-7818.

Bromium (2013). Understanding Bromium® Micro-virtualization for Security Architects. Retrieved on November 30, 2013, from http://www.bromium.com/sites/default/files/Bromium%20Microvirtualization%20for%20the%20Security%20Architect_0.pdf

Buecker, A., Costa, F., Davidson, R., Matteotti, E., North, G., Sherwood, D. and Zaccak, S. (2013). *Managing Security and Compliance in Cloud or Virtualized Data Centers Using IBM PowerSC*. International Technical Support Organization. IBM. Red Books. (January 2013), 1-319.

Butler, B. (2012). Nine security controls to look for in cloud contracts. *Network World*. Retrieved on November 17, 2013, from http://www.networkworld.com/news/2012/111412-gartner-cloud-contracts-264270.html?page=1

Butler, J. (2010). Adding Enterprise Access Management to Identity Management. SANS Institute. Retrieved on November 17, 2013, from http://www.sans.org/reading-room/whitepapers/analyst/adding-enterprise-access-management-identity-management-35075

Celesti, A., Salici, A., Villar, M. and Puliafito, A. (2011). A Remote Attestation Approach for a Secure Virtual Machine Migration in Federated Cloud Environments. *Proceedings of the 2011 Network Cloud Computing and Applications (NCCA)*, 2011 First International Symposium on. 21-23 November. 2011. Toulouse. IEEE, 99–106. DOI: 10.1109/NCCA.2011.23.

Chen, D. and Zhao, H. (2012). Data Security and Privacy Protection Issues in Cloud Computing. *Proceedings of the 2012 International Conference on Computer Science and Electronics Engineering (CSEE)*. 23-25 March 2012. Hangzhou. IEEE, 647-651. DOI:10.1109/ICCSEE.2012.193.

Chen, L. and Hoang, D. (2011). Novel Data Protection Model in Healthcare Cloud. *Proceedings of the 2011 High Performance Computing and Communications (HPCC), 2011 IEEE 13th International Conference on*. 2-4 September 2011. Banff, AB. IEEE, 550–555. DOI: 10.1109/HPCC.2011.148.

Chen, L. and Hoang, D. (2011a). Towards Scalable, Fine-Grained, Intrusion-Tolerant Data Protection Models for Healthcare Cloud. *Proceedings of the 2011 Trust, Security and Privacy in Computing and Communications (TrustCom)*. 16-18 November. 2011. Changsha. IEEE, 126–133. DOI: 10.1109/TrustCom.2011.19.

Chen, L., Franklin, J. and Regenscheid, A. (2012). Guidelines on Hardware-Rooted Security in Mobile Devices: *Recommendations of the National Institute of Standards and Technology (NIST)*. NIST Special Publication 800-164 (Draft), 26.

Chi, Y., Moon, H. and Hacigümüş, H. (2011). ICBS: Incremental Cost-Based Scheduling under Piecewise Linear SLAs. *Journal Proceedings of the VLDB Endowment*. In VLDB Endowment Homepage archive. ACM. 4 (9):563-574.

Choudhury, A., Kumar, P., Sain, M., Lim, H. and Jae-Lee, H. (2011). A Strong User Authentication Framework for Cloud Computing. *Proceedings of the 2011 Services Computing Conference (APSCC), 2011 IEEE Asia-Pacific on*. 12-15 Dec. 2011. Jeju Island. IEEE, 110–115. DOI:10.1109/APSCC.2011.14.

CIO.gov (2012). Creating Effective Cloud Computing Contracts for the Federal Government. Best Practices for Acquiring IT as a Service. *A joint publication of the* Chief *Acquisition Officers Council and Federal Cloud Compliance Committee.*

CMS (2007). HIPAA Security Series. Security Standards: Technical Safeguards. *Department of Health and Human Services USA.* Centers for Medicare and Medicaid Services (CMS). 2(4):1-17.

Cohen, L., Manion, L. and Morrison, K. (2011). Research Methods in Education. Routledge, 7th Ed. Routledge 2011 -762.

Cooper, D., Polk, W., Regenscheid, A. and Souppaya, M. (2011). BIOS Protection Guidelines. *NIST Special Publication 800-147*. Retrieved on November 15, 2013, from http://csrc.nist.gov/publications/nistpubs/800-147/NIST-SP800-147-April2011.pdf

Creative Research Systems (2012). The Survey System. Retrieved on October, 2014, from http://www.surveysystem.com/sscalc.htm#one

Cryptomathic (2014). Industry Standards. Retrieved on September 23, 2014, from http://www.cryptomathic.com/company/industry-standards

CSA (2013). The Notorious Nine Cloud Computing Top Threats in 2013. *Cloud Security Alliance (CSA).* Retrieved on November 28, 2013, from https://downloads.cloudsecurityalliance.org/initiatives/top_threats/The_Notorious_Nine_Cloud_Computing_Top_Threats_in_2013.pdf

CSA (2012). Top Ten Big Data Security and Privacy Challenges. *Cloud Security Alliance (CSA)* Retrieved on May 28, 2013, from https://cloudsecurityalliance.org/download/top-ten-big-data-security-and-privacy-challenges/

CSA (2011). Security Guidance For Critical Areas Of Focus In Cloud Computing V3.0. *Cloud Security Alliance.* Retrieved on May 28, 2013, from https://downloads.cloudsecurityalliance.org/initiatives/guidance/csaguide.v3.0.pdf

CSA (2010). Domain 12: Guidance for Identity and Access Management V2.1. *2010 Cloud Security Alliance (CSA).* Retrieved on November 15, 2013, from https://cloudsecurityalliance.org/guidance/csaguide-dom12-v2.10.pdf

Danev, B., Masti, R., Karame, G. and Capkun, S. (2011). Enabling Secure VM-vTPM Migration in private clouds. *Proceedings of the 2011 Annual computer Security Applications conference (ACSAC).* New York, USA. ACM, 187-196.DOI:10.1145/2076732.2076759.

Decat, M., Lagaisse, B. and Joosen, W. (2012). Federated Authorization for SaaS Applications. *In International Symposium on Engineering Secure Software and Systems*, 2012 ESSoS Doctoral Symposium 2012. First Doctoral Symposium on Engineering Secure Software and Systems. ESSoS-DS'12, 53-59.

Demirkan, H. (2013). A Smart Healthcare Systems Framework. *Proceedings of the 2013 IT Professional*. 10 October 2013. IEEE Computer Society. 15(5): 38-45. DOI: 10.1109/MITP.2013.35.

Department Of Health And Human Services (2013). Modifications to the HIPAA Privacy, Security, Enforcement, and Breach; Notification Rules under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Non-discrimination Act; Other Modifications to the HIPAA Rules. *Office for Civil Rights, Department of Health and Human Services,* 1-534. RIN: 0945-AA03.

Diaz, A. (2012). Cloud SLAs: What You Don't Know Can Hurt You. *IBM*. Thoughts. IBM_THOUGHTSONCLOUD. Retrieved on November 17, 2013, from http://www.wired.com/insights/2012/05/cloud-slas/

Dinh, T. and Ryan, M. (2006). Trusted Computing: TCG proposals. *Trusted Computing Group (TCG)* Retrieved on November 15, 2013, from http://www.cs.bham.ac.uk/~mdr/teaching/modules/security/lectures/TrustedComputingTCG.html

Doddavula, S. and Saxena, V. (2011). Implementation of a Secure Genome Sequence Search Platform on Public Cloud: Leveraging Open Source Solutions. *Proceedings of the 2011 Cloud Computing Technology and Science (CloudCom)*. July 2012. Springer-Verlag, 205–212. DOI:10.1109/CloudCom.2011.36.

Donovan, M. and Visnyak, E. (2011). The Case for a Reference Framework for Trusted Multi-Tenant Infrastructure Retrieved on April 30, 2013, from https://www.ncsi.com/nsatc11/presentations/tuesday/research/donovan_visnyak.pdf

Doyle, K. (2013). KVM Security in The Cloud: A Choice That Matters. Retrieved on January 30, 2014, from http://www.globalknowledge.co.uk/content/files/documents/640774/640819/kvm-security

Du, Z., Li, X. and Shen, K. (2011). Ensemble of Trusted Firmware Services based on TPM. *International Journal of Digital Content Technology and its Applications (JDCTA)*. 5(3): 175-184.

El Emam, K., Moreau, K. and Jonker, E. (2011). How strong are passwords used to protect personal health information in clinical trials? Multimedia Appendix 1: Background. *Journal Med Internet Res 2011*; 13 (1):e18 DOI: doi:10.2196/jmir.1335. http://www.jmir.org/2011/1/e18/

Ermakova, T. and Fabian, B. (2013). Secret Sharing for Health Data in Multi Provider Clouds. *Proceedings of the Business Informatics (CBI), 2013 IEEE 15th Conference on. 2013 IEEE International Conference on Business Informatics*. 15-18 July 2013. Vienna. IEEE, 93–100. DOI:10.1109/CBI.2013.22.

European CIO Association (2012). Users Recommendations From *The European CIO Association For The Success Of The Cloud Computing In Europe*. Retrieved on January 13, 2014, from http://ec.europa.eu/information_society/activities/cloudcomputing/docs/consolidated_list_of_recommendations_users_%20perspective.pdf%5B1%5D.pdf

Fan, W., Yang, S., Pei, J. and Luo, H. (2012). Building trust into cloud. *International Journal of Cloud Computing and Services Science (IJ-CLOSER)*. 1(3):115-122. DOI: 10.11591/closer.v1i3.742.

Fan, Y. and Wu, J. (2012). Middleware Software for Embedded Systems. *Proceedings of the 2012 26th Advanced Information Networking and Applications Workshops (WAINA)*. 26-29 March 2012. Fukuoka. IEEE, 61-65. DOI: 10.1109/WAINA.2012.88.

Ffoulkes, P. (2014). Securing the cloud: What are the top concerns? *451 Research LLC*. Retrieved on July 30, 2014, from https://451research.com/biography?eid=581

FIDIS (2009). Chain of Trust. FIDIS Deliverables: Privacy and legal-social content. *D14.3: Study on the Suitability of Trusted Computing to support Privacy in Business Processes*. Retrieved on November 17, 2013, from http://www.fidis.net/resources/deliverables/privacy-and-legal-social-content/d143-study-on-the-suitability-of-trusted-computing-to-support-privacy-in-business-processes/doc/19/

FireEye, Inc, 2013. FireEye Advanced Threat Report. Retrieved September 25 , 2014, from http://www2.fireeye.com/rs/fireye/images/fireeye-advanced-threat-report-2013.pdf

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

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

Galav, D. and Ghosh, S. (2014). An Identification of Framework for Secure Cloud Computing. *International Journal of Science and Research (IJSR)*. 3(5): 269-272 ISSN (Online): 2319-7064. Impact Factor (2012): 3.358.

Gartner (2013). Identity and Access Management (IAM). Retrieved on November 17, 2013, from http://www.gartner.com/it-glossary/identity-and-access-management-iam/

Ghatage, S. and Rewadkar, D. (2013). Secure Cloud Storage System Incorporating Privacy-Preserving Third Party Audit. *International Journal of Advanced Research in Computer Science and Software Engineering (IJARCSSE).* 3(11):126-129. November 2013. ISSN: 2277 128X.

Gilmer, E. (2013). Privacy And Security Of Patient Data In The Cloud. IBM. Developer Works Retrieved on January 9, 2014, from http://www.ibm.com/developerworks/library/cl-hipaa/

Gonzalez, N., Miers, C., Redígolo, F., Carvalho, T., Simplicio, M., Näslund, M. and Pourzandi, M. (2011). A quantitative analysis of current security concerns and solutions for cloud computing. *Proceedings of the 2011 Cloud Computing Technology and Science (CloudCom)*. November.29-December.1 2011. Athens. IEEE, 231-238. DOI: 10.1109/CloudCom.2011.39.

Govpub (2013). Healthcare 2030: The road to wellness – Draft. *Western Cape Government*. Retrieved on January 2, 2014, from http://www.westerncape.gov.za/text/2013/October/health-care-2030-9-oct-2013.pdf

Grozev, N. and Buyya, R. (2012). Inter-Cloud Architectures and Application Brokering: Taxonomy and Survey. *Software Practice And Experience.* Wiley InterScience, 1-22. DOI: 10.1002/spe.

Guilloteau, S. and Mauree, V. (2012). Privacy in Cloud Computing. *ITU-T Technology Watch Report March 2012*. Retrieved on January 8, 2014, from http://www.itu.int/dms_pub/itu-t/oth/23/01/T23010000160001PDFE.pdf

Hall, J., Rapanotti, L. and Jackson, M. (2007). Problem Oriented Software Engineering: A design-theoretic framework for software engineering. *Proceedings of Fifth IEEE International Conference on Software Engineering and Formal Methods*. 10-14 September. 2007. London, IEEE, 15-24. DOI:10.1109/SEFM.2007.29.

Hall, M. and Nachbar, R. (2010). Cloud Security Alliance Announces Collaboration with HITRUST. *Proceedings of the 2010 Infosecurity Europe Conference*, London, UK 27 April, 2010. London, UK.

Hao, F., Lakshman, T., Mukherjee, S. and Song, H. (2010). Secure cloud computing with a virtualized network infrastructure. *Proceedings of the 2010 HotCloud'10 Proceedings of the 2nd USENIX conference on Hot topics in cloud computing (HotCloud'10)*. USENIX Association, ACM, 1-7.

Harmana, M., Lakhotiaa, K., Singerb, J., Whiteb, D. and Yooa, S. (2013). Cloud Engineering is Search Based Software Engineering too. *Journal of Systems and Software*, September 2013, 86(9): 2225-2241. DOI: 10.1016/j.jss.2012.10.027

Harris, J. and Hill, R. (2011). StaticTrust: A Practical Framework for Trusted Networked Devices. *Proceedings of the 44th Hawaii International Conference on System Sciences (HICSS)*. 4-7 January. 2011. Kauai, HI. IEEE, 1-10. DOI: 10.1109/HICSS.2011.384.

Hashizume, K., Rosado, D., Medina, E. and Fernandez, E. (2013). An analysis of security issues for cloud computing. *Journal of Internet Services and Applications (JISA)*.4(1):1-13. DOI: 10.1186/1869-0238-4-5.

HealthIT.gov (2012). Guide to Privacy and Security of Health Information Retrieved December 28, 2013, from http://www.healthit.gov/sites/default/files/pdf/privacy/priv and-security-guide.pdf

HHS.gov (2014). Data breach results in $4.8 million HIPAA settlements. *U.S. Department of Health and Human* Services. Retrieved on September 23, 2014, from http://www.hhs.gov/news/press/2014pres/05/20140507b.html

HHS.gov (2013). New rule protects patient privacy, secures health information. *U.S. Department of Health and Human* Services. Retrieved on November 19, 2013, from http://www.hhs.gov/news/press/2013pres/01/20130117b.html

HHS.gov (2013a). Cyber Security. Retrieved on December 28, 2013, from http://www.healthit.gov/providers-professionals/cybersecurity

Holtzman, D., Koenig, J. and LeSueur, T. (2013). HITECH and The Cloud: Control and Accessibility of Data Downstream. *Proceedings of the 2013 NIST/OCR HIPAA Security Assurance Conference*. 21 May, 2013.

Hon, W., Millard, C. and Walden, I. (2012). Negotiating Cloud Contracts: Looking At Clouds From Both Sides Now. *Stanford Technology Law Review*. 16 (1):80-125. 16 Stan. Tech. L. Rev. 79 (2012).

Honan, B. (2011). Layered Security Protecting Your Data In Today's Threat Landscape. Tripwire Take Control. IT Security And Compliance Automation Solutions. Retrieved on November 30, 2013, from http://www.tripwire.com/linkservid/28A1C99D-DCBC-A339-0115D05A9EAB543E/showMeta/2/

Hsing, K. (2012). A Healthcare Cloud Computing Strategic Planning Model. *Computer Science and Convergence*. Lecture Notes in Electrical Engineering 114:769-775. DOI: 10.1007/978-94-007-2792-2_76.

Hwang, K. and Li, D. (2010). Trusted Cloud Computing with Secure Resources and Data Colouring. *Proceedings of the 2010 Internet Computing*. September.-October. 2010. IEEE Computer Society. 14(5): 14–22. DOI: 10.1109/MIC.2010.86.

Indiana University (2013). Secure File Transfer Alternatives. Retrieved on October 14, 2013, from http://protect.iu.edu/cybersecurity/secure-file-transfer-alternatives

ISO (2009). ISO/IEC 11889-1:2009 Information technology-Trusted Platform Module-Part 1: Overview. Retrieved on November 16, 2013, from http://www.iso.org/iso/catalogue_detail.htm?csnumber=50970

Ivanov, V., Yu, P. and Baras, J. (2010). Securing the communication of medical information using local biometric authentication and commercial wireless links. *Health Informatics Journal*. 16(3):211–223. DOI: 10.1177/1460458210377482.

Jamkhedkar, P., Szefer, J., Botero, D., Zhang, T., Triolo, G. and Lee, R.B. (2013). A Framework for Realizing Security on Demand in Cloud Computing. *Proceedings of the 2013 Cloud Computing Technology and Science (CloudCom),* 2013 IEEE 5th International Conference on, 2-5 Dec. 2013. Bristol. IEEE. 1: 371-378. DOI:10.1109/CloudCom.2013.55.

Jansen, W. and Grance, T. (2011). Guidelines on Security and Privacy in Public Cloud Computing. *National Institute of Standards and Technology (NIST)*, Special Publication 800-144. COMPUTER SECURITY. Gaithersburg, MD 20899-8930, 1-70.

Jones, A., DeKeyrel, M., Lobbes, M. and Ling, J. (2012). SmartCloud tip: Build multiple VPNs and VLANs VPN and VLAN features and capabilities in IBM SmartCloud Enterprise 2.0. *IBM. DeveloperWorks*. Retrieved on December 6, 2013, from http://www.ibm.com/developerworks/cloud/library/cl-multiplevlans/

Khan, M. and Malluhi, Q. (2010). Establishing Trust in Cloud Computing. *Proceedings of the 2010 IT Professional*. September.-October. 2010. IEEE Computer Society, 12(5):20–27. DOI:10.1109/MITP.2010.128.

Khatua, S., Mukherjee, N. and Chaki, N. (2011). A New Agent Based Security Framework For Collaborative Cloud Environment. *In Proceedings of the Seventh Annual Workshop on Cyber Security and Information Intelligence Research (CSIIRW '11)*, ACM, 76:1-4. DOI: 10.1145/2179298.2179385.

Kim, M., Ju, H., Kim, Y., Park, J. and Park, Y. (2010). Design And Implementation of Mobile Trusted Module for Trusted Mobile Computing. *Proceedings of the 2010 Consumer Electronics*. 9-13 January. 2010. Las Vegas, NV. IEEE Consumer Electronics Society, 56(1):134 -140. DOI: 10.1109/TCE.2010.5439136.

Kim, T., Adeli, H., Fang, W., Villalba, J., Arnett, K. and Khan, M. (2011). Security Technology. *Proceedings of the 2011 International Conference, SecTech 2011, Held as Part of the Future Generation Information Technology Conference, FGIT 2011, in Conjunction with GDC 201*. 8-10 Dec. 2011. Jeju Island, Korea. Springer, 11–20.

Kissel, R., Scholl, M., Skolochenko, S. and Li, X. (2012). Guidelines for Media Sanitization Revision 1. *National Institute of Standards and Technology (NIST).* Retrieved on July 2, 2014, from http://www.disa.mil/Services/DoD-Cloud-Broker/~/media/Files/DISA/Services/Cloud-Broker/sp800_88_r1_draft.pdf

Ko, R., Jagadpramana, P., Mowbray, M., Pearson, S., Kirchberg, M., Liang, Q. and Lee, B. (2011). TrustCloud: A Framework for Accountability and Trust in Cloud Computing. *Proceedings of the 2011 Services (SERVICES). 2011 IEEE World Congress on*. 4-9 July 2011. Washington, DC. IEEE, 584–588. DOI: 10.1109/SERVICES.2011.91.

Krautheim, F., Phatak, D. and Sherman, A. (2010). Introducing the trusted virtual environment module: a new mechanism for rooting trust in cloud computing. *Proceedings of the 3rd international conference on Trust and trustworthy computing (TRUST'10)*. Springer-Verlag, Berlin, Heidelberg, 211-227. DOI: 10.1007/978-3-642-13869-0_14.

Kulkarni, G., Gambhir, J., Patil, T. and Dongare, A. (2012). A security aspects in cloud computing. *Proceedings of the 2012 Software Engineering and Service Science (ICSESS), 2012 IEEE 3rd International Conference on.* 22-24 June 2012. Beijing, 547 – 550. DOI: 10.1109/ICSESS.2012.6269525.

Le, X., Sankar, R. and Khalid. M. (2010). Public Key Cryptography-Based Security Scheme For Wireless Sensor Networks In Healthcare. *Proceedings of the 2010 4th International Conference on Ubiquitous Information Management and Communication (ICUIMC '10)*. ACM, 5-7. DOI=10.1145/2108616.2108623.

Lehman, T., and Vajpayee, S. (2011). We've Looked at Clouds from Both Sides Now. *Proceedings of the 2011 SRII Global Conference (SRII), 2011 Annual on*. March 29 2011-April 2 2011. San Jose, CA. IEEE, 342–348. DOI: 10.1109/SRII.2011.46.

Leyva, C. (2013). HIPAA Omnibus Rule. Retrieved on December 25, 2013, from http://www.hipaasurvivalguide.com/hipaa-omnibus-rule.php

Li, J., Tan, X., Chen, X. and Wong, D. (2013). An Efficient Proof of Retrieve-ability with Public Auditing in *Cloud Computing. Proceedings of the 2013 Intelligent Networking and Collaborative Systems (INCoS), 2013 5th International Conference on.* 9-11 September. 2013. Xi'an. IEEE, 93-98. DOI: 10.1109/INCoS.2013.185.

Li, Z, Chang, C., Huang, K. and Lai, F. (2011). A secure electronic medical record sharing mechanism in the cloud computing platform. *Proceedings of the 2011 Consumer Electronics (ISCE), 2011 IEEE 15th International Symposium on*. 14-17 June 2011. Singapore. IEEE, 98–103. DOI: 10.1109/ISCE.2011.5973792.

Liu, F., Tong, J., Mao, J., Bohn, R., Messina, J., Badger, L. and Leaf, D. (2011). NIST Cloud Computing Reference Architecture. Cloud Computing Program Information Technology Laboratory. *National Institute of Standards and Technology (NIST)*. Gaithersburg, MD 20899-8930. NIST Special Publication 500-292, 1-28.

Lofgren, A. (2013). What's the healthcare industry doing about BYOD? *Health Management Technology*. Retrieved on January 2, 2014, from http://www.healthmgttech.com/online-only/whats-the-healthcare-industry-doing-about-byod.php

Lohr, H., Sadeghi, A. and Winandy, M. (2010). Securing the e-health cloud. *In Proceedings of the 2010 1st ACM International Health Informatics Symposium (IHI '10)*, Tiffany Veinot (Ed.). ACM, 220-229. DOI:10.1145/1882992.1883024.

Lynn, J. (2013). The HIPAA Final Rule and Staying Compliant in the Cloud. Retrieved on January 4, 2014, from http://www.porticor.com/2013/09/hipaa-compliant-checklist/

Mackey, R. (2012). HIPAA cloud computing advice: Ensuring cloud computing compliance. Retrieved on December 27, 2013, from http://searchcloudsecurity.techtarget.com/tutorial/HIPAA-cloud-computing-advice-Ensuring-cloud-computing-compliance

Mahmood, Z. and Saeed, S. (2013). Software Engineering Frameworks for the Cloud Computing Paradigm. *Computer Communications and Networks*. Springer London Heidelberg New York Dordrecht (2013).1-361. DOI: 10.1007/978-1-4471-5031-2

Markets and Markets (2011). World Healthcare IT (Provider and Payor) Market - Clinical (EMR, PACS, RIS, CPOE, LIS) and Non-Clinical (RCM, Billing, Claims). Retrieved on October 16, 2013, from http://www.marketsandmarkets.com/Market-Reports/healthcare-information-technology-market-136.html

McGee, M. (2013). Medical Device Vulnerability Alert Issued. Homeland Security Warns of Password Problems. Healthcare Info Security. *Information Security Media Group (ISMG)* Retrieved on November 24, 2013, from http://www.databreachtoday.com/medical-device-vulnerability-alert-issued-a-5847

McGee, M. (2013a). HIPAA Omnibus: Impact on Breach Notices. Experts Assess What the Final Rule Means. Data Breach Today.com. *Information Security Media Group, Corp (ISMG)*. Retrieved on November 19, 2013, from http://www.databreachtoday.com/hipaa-omnibus-impact-on-breach-notices-a-5436

McGee, M. (2013b). Patient Information Exposed on Google Business Associate Blamed for Security Lapse. *Healthcare Info Security*. Retrieved on December 21, 2013, from http://www.healthcareinfosecurity.com/patient-information-exposed-on-google-a-6303

Mell, P. and Grance, T. (Eds) (2011). The NIST Definition of Cloud Computing. *National Institute of Standards and Technology (NIST), Special Publication 800-145.* COMPUTER SECURITY. Gaithersburg, MD 20899-8930, 1-3.

Mell, P. and Scarfone, K. (2012). Guide to Intrusion Detection and Prevention Systems (IDPS). *Recommendations of the National Institute of Standards and Technology (NIST). Special Publication 800-94 Revision 1 (Draft).* COMPUTER SECURITY. Gaithersburg, MD, 1-99.

Messmer, E. (2013). IBM earns patent for 'encrypted blobs' IBM researchers invented 'fully homomorphic encryption' that allows for processing of encrypted data without having to decrypt it first. *Network World*. Retrieved on December 31, 2013, from http://www.networkworld.com/news/2013/121913-ibm-patent-277118.html

Messmer, E. (2012). Gartner: Network virtualization will lead to security control changes. Network World. Retrieved on November 30, 2013, from http://www.cio.com/article/708302/Gartner_Network_Virtualization_Will_Lead_to_Security_Control_Changes?taxonomyId=3112

Metri, P. and Sarote, G. (2011). Privacy Issues and Challenges in Cloud computing. *International Journal of Advanced Engineering Sciences and Technologies (IJAEST)*. 5(1):1-6. ISSN: 2230-7818.

Mo, Z., Zhou, Y. and Chen, S. (2012). A Dynamic Proof of Irretrievability (PoR) Scheme with O (logn) Complexity. *Proceedings of the 2012 Communications (ICC), 2012 IEEE International Conference on.* 10-15 June 2012. Ottawa, ON. IEEE, 912 – 916. DOI: 10.1109/ICC.2012.6364056.

Modi, C., Patel, D., Borisaniya, B., Patel, A and Rajarajan, M. (2012). A survey on security issues and solutions at different layers of Cloud computing. *The Journal of Supercomputing*. Springer US. 63(2):561-592. DOI: 10.1007/s11227-012-0831-5.

Moffa, T. (2012). IT Security Risk Management: A Lifecycle Approach (ITSG-33) Overview. *Communications Security Establishment Canada*, Security Control Catalogue ITSG-33 – Annex 3, 1-16.

Mohammed, S., Servos, D. and Fiaidhi, J. (2010). HCX: A Distributed OSGi Based Web Interaction System for Sharing Health Records in the Cloud. *Web Intelligence and Intelligent Agent Technology (WI-IAT)*, 2010 IEEE/WIC/ACM. International Conference on. August. 31 2010-September. 3 2010. Toronto, ON. IEEE, 3:102–107. DOI: 10.1109/WI-IAT.2010.26.

Monticello, K. (2012). The $1.7 Million Flash drive Alaska Medicaid Settles HIPAA Violations. *Attorneys at Oscislawski llc*. Retrieved on November 19, 2013, from http://www.legalhie.com/security-breaches/the-17-million-flashdrivealaska-medicaid-settles-hipaa-violations/

Mu-Hsing, K. (2012). A Healthcare Cloud Computing Strategic Planning Model. *Computer Science and Convergence*. CSA 2011 and WCC 2011 Proceedings, 2012, Lecture Notes in Electrical Engineering. 1l4(6):769-775. DOI: 10.1007/978-94-007-2792-2_76.

Munch, J. (2013). Cloud-Based Software Engineering. Proceedings Of The Seminar No. 58312107. Retrieved on October 12, 2014, from https://tuhat.halvi.helsinki.fi/portal/files/28513674/cbse13_proceedings.pdf

Muppala, J., Shukla1, D., Mondal, S. and Patil, P. (2012). Establishing Trust in Public Clouds. *Information Technology and Software Engineering*. 2(4):1-3. DOI:10.4172/2165-7866.1000e107.

Myerson, J. (2013). Best practices to develop SLAs for cloud computing. Develop a standard way to create service level agreements that multiple partners can use. *IBM. Developer Works*. Retrieved on November 17, 2013, from http://www.ibm.com/developerworks/cloud/library/cl-slastandards/

Narayan, S., Gagné, M. and Naini, R. (2010). Privacy preserving EHR system using attribute-based infrastructure. *Proceedings of the 2010 ACM workshop on Cloud computing security workshop (CCSW '10)*. ACM, 47-52. DOI:10.1145/1866835.1866845.

Narayanan, H. and Gunes, M. (2011). Ensuring access control in cloud provisioned healthcare systems. *Proceedings of the 2011 Consumer Communications and Networking Conference (CCNC)*. 9-12 Jan. 2011. Las Vegas, NV. IEEE, 247–251. DOI:10.1109/CCNC.2011.5766466.

Naruchitparames, J. (2011). Enhancing the Privacy of Data Communications within Information Sensitive Systems. ProQuest LLC1-91. UMI Number: 1494258.

Nemati, H. (2011). Pervasive Information Security and Privacy Developments. *IGI Global Snippet*, 2011, 1- 428. ISBN: 9781616920012.

Nissany, G. (2013). HIPAA and the Cloud: Securing Patient Data. Retrieved on April 4, 2013, from http://www.thesecurityadvocate.com/2013/09/17/hipaa-and-the-cloud-securing-patient-data/

NIST (2012). Special Publication 800-12: An Introduction To Computer Security: The NIST Handbook Section I: Introduction and Overview. Chapter 1. *National Institute of Standards and Technology (NIST)*. Retrieved on August 3, 2014, from http://www.davidsalomon.name/CompSec/auxiliary/handbook.pdf

Olden, E. (2011). Architecting a Cloud-Scale Identity Fabric. *Proceedings of the 2011 Computer*. 17 March 2011. IEEE Computer Society. 44(3):52–59. DOI: 10.1109/MC.2011.60.

Olzak, T. (2011). UEFI and the TPM: Building a foundation for platform trust. *InfoSec Institute Resources. Management, Compliance, and Auditing*. Chapter 8, 2011.

Østerlie, T. (2009). Cloud computing: Impact on Software Engineering Research and Practice. *Norwegian University of Science and Technology (NTNU)*. Retrieved on August 3, 2014, from http://www.idi.ntnu.no/grupper/su/publ/phd/osterlie-triallecture09.pdf

Ouellette, P. (2013). Reviewing the HIPAA omnibus four data breach risk factors. Retrieved on January 9, 2014, from http://healthitsecurity.com/2013/09/05/reviewing-the-hipaa-omnibus-four-data-breach-risk-factors/

Padhy, R., Patra, M. and Satapathy, S. (2011). Cloud Computing: Security Issues and Research Challenges. *IRACST - International Journal of Computer Science and Information Technology and Security (IJCSITS)*. 1(2):136-146. ISSN: 2249-9555.

Palmer, D. (2012). Understanding Trusted Computing From The Ground Up. *Electronic Design Magazine*. Retrieved on November 25, 2013, from http://electronicdesign.com/microprocessors/understanding-trusted-computing-ground

Pan, L. (2011). Towards a framework for automated service negotiation in cloud computing. *Proceedings of the 2011 Cloud Computing and Intelligence Systems (CCIS), 2011 IEEE International Conference on*. 15-17 September. 2011. Beijing. IEEE, 364–36. DOI: 10.1109/CCIS.2011.6045091.

Parakala, K. and Udhas, P. (2011). The Cloud Changing the Business Ecosystem. KPMG. Retrieved on December 12, 2013, from http://www.kpmg.com/IN/en/IssuesAndInsights/ThoughtLeadership/The_Cloud_Changing_the_Business_Ecosystem.pdf

Patel, A. and Kumar, M. (2013). A Proposed Model for Data Security of Cloud Storage Using Trusted Platform Module. *International Journal of Advanced Research in Computer Science and Software Engineering (IJARCSSE)*. 3(4):862-866. April 2013. ISSN: 2277 128X.

Patidar, K., Gupta, R., Singh, G., Jain, M. and Shrivastava, P. (2012). Integrating the Trusted Computing Platform into the Security of Cloud Computing System. *International Journal of Advanced Research in Computer Science and Software Engineering (IJARCSSE).* 2(2):1-5. February 2012.

Pearson, S. and Benameur, A. (2010). Privacy, Security and Trust Issues Arising from Cloud Computing. *Proceedings of the 2010 2nd IEEE International Conference on Cloud Computing Technology and Science (CloudCom), 2010 IEEE Second International Conference on*. Nov. 30 - Dec. 3 2010. Indianapolis, IN. IEEE, 693 – 702. DOI: 10.1109/CloudCom.2010.66.

Popovic, K. and Hocenski, Z. (2010). Cloud Computing Security Issues And Challenges. *In MIPRO, 2010 Proceedings of the 33rd International Convention,* 24-28 May 2010. Opatija, Croatia. IEEE. 344 - 349. ISBN: 978-1-4244-7763-0.

PR Newswire Association (2014). Retrieved on September 22, 2014, from http://www.prnewswire.com/news-releases/linkedin-study-cnp-credential-key-to-nonprofit-career-advancement-276385931.html

Proofpoint (2012). Meeting the Challenges of HIPAA Compliance, Phishing Attacks, and Mobile Security. Retrieved on November 19, 2013, from http://healthsystemcio.com/whitepapers/proofpoint-hippa-compliance.pdf

Proofpoint (2013). Experts urge healthcare to be proactive for security and compliance. Retrieved on November 11, 2013, from http://www.proofpoint.com/about-us/security-compliance-and-cloud-news/articles/experts-urge-healthcare-to-be-proactive-for-security-and-compliance-440291

Purcell, J. (2013). Security Control Types and Operational Security. Retrieved on November 29, 2013, from http://www.giac.org/cissp-papers/207.pdf

Radwan, A., Abdel-Hamid, A. and Hanafy, Y. (2012). Cloud-based Service for Secure Electronic Medical Record Exchange. *Proceedings of the 2012 Computer Theory and Applications (ICCTA), 2012 22nd International Conference on*. 13-15 October. 2012. Alexandria. IEEE, 94-103. DOI: 10.1109/ICCTA.2012.6523553.

Rak, M., Liccardo, L. and Aversa, R. (2011). A SLA-Based Interface for Security Management in Cloud and GRID Integrations. *Proceedings of the 2011 Information Assurance and Security (IAS), 2011 7th International Conference on*. 5-8 December. 2011. Melaka. IEEE, 378–38. DOI: 10.1109/ISIAS.2011.6122783.

Rani, P., Sangeeta, V. and Babu, P. (2013). Achieving Information Accountability In Cloud Computing Environment. *International Journal of Computer and Electronics Research (IJCER)*. 2(2):169-172. April 2013.

Ratnam, K. and Dominic, P. (2012). Cloud services - Enhancing the Malaysian healthcare sector. *Proceedings of the 2012 Computer and Information Science (ICCIS), 2012 International Conference on.* 12-14 June 2012. Kuala Lumpur. IEEE, 2: 604-608. DOI:10.1109/ICCISci.2012.6297101.

Redd, B. (2011). Implement secure SSH access to IBM Cloud. *Learn the basics of secure cloud access.* Retrieved on December 9, 2013, from http://www.ibm.com/developerworks/cloud/library/cl-sshaccessibmcloud/

Regenscheid, A. and Scarfone, K. (2011). BIOS Integrity Measurement Guidelines (Draft). Recommendations of the National Institute of Standards and Technology. *National Institute of Standards and Technology (NIST)* .Special Publication 800-155. Gaithersburg, MD 20899-8930.

Renda, S., Goodrich, M., Stanton, A., Cantor, J., Cramer, J. and the Federal Cloud Compliance Committee (2012). Creating Effective Cloud Computing Contracts for the Federal Government Best Practices for Acquiring IT as a Service. *A joint publication of the Chief Acquisition Officers Council In coordination with Federal Cloud Compliance Committee.* Retrieved on January 14, 2014, from http://www.gsa.gov/portal/mediaId/164011/fileName/cloudbestpractices.action

Revar, A. and Bhavsar, M. (2011). Securing User Authentication using Single Sign-On in Cloud Computing. *Proceedings of the 2011 Engineering (NUiCONE), 2011 Nirma University International Conference on.* 8-10 Dec. 2011. Ahmedabad, Gujarat. IEEE, 1-4. DOI: 10.1109/NUiConE.2011.6153227.

Rokosz, V. (2011). Extend your corporate network with the IBM Cloud See how the IBM Cloud can become a seamless extension of your network. *IBM Developer Works* Retrieved on December 5, 2013, from http:// http://www.ibm.com/developerworks/cloud/library/cl-extendnetworkcloud/

Rong, C., Nguyen, S. and Jaatun, M. (2013). Beyond lightning: A survey on security challenges in cloud computing. *Computers and Electrical Engineering*. 39(1):47-54, January 2013, ISSN 0045-7906.

Ruan, A. and Martin, A. (2011). RepCloud: achieving fine-grained cloud TCB attestation with reputation systems. *In Proceedings of the sixth ACM workshop on Scalable trusted computing (STC '11)*. ACM, 3-14. DOI: 10.1145/2046582.2046586.

Rutkowski, M. and Mahmud, S. (2012).Security for Cloud Computing 10 Steps to Ensure Success. Cloud Standards Customer Council. Retrieved on January 13, 2014, from http://www.cloudstandardscustomercouncil.org/Security_for_Cloud_Computing-Final_080912.pdf

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.

Samson, T. (2013). 9 top threats to cloud computing security. Data breaches and cloud service abuse rank among the greatest cloud security threats, according to Cloud Security Alliance. *InfoWorld*. Retrieved on November 23, 2013, fromhttp://www.infoworld.com/t/cloud-security/9-top-threats-cloud-computing-security-213428

Santos, O. (2007). End-to-End Network Security Defence-in-Depth. Best practices for assessing and improving network defences and responding to security incidents. Cisco Press; ISBN-13: 978-1587053320 | Edition: 1(September 3, 2007).

Sarwar, A., Naeem, M. and Khan, A. (2013). A Review of Trust Aspects in Cloud Computing Security. *International Journal of Cloud Computing and Services Science (IJ-CLOSER)*. 2(2):116-122. April 2013. ISSN: 2089-3337.

Savu, L. (2011). Cloud Computing: Deployment Models, Delivery Models, Risks and Research Challenges. *Proceedings of the 2011 Computer and Management (CAMAN), 2011 International Conference on*. 19-21 May 2011. Wuhan. IEEE, 1-4. DOI: 10.1109/CAMAN.2011.5778816.

Scarfone, K., Souppaya, M. and Hoffman, P. (2011). Guide to Security for Full Virtualization. Recommendations of the National Institute of Standards and Technology (NIST). *NIST Special Publication 800-125 Technologies.*

Schellekens, D. (2012). *Design and Analysis of Trusted Computing Platforms*. PhD Thesis, Katholieke Universiteit Leuven, Faculty of Engineering Science Kasteelpark Arenberg 10, B-3001 Heverlee.

Schiffman, J., Moyer, T., Vijayakumar, H., Jaeger, T. and McDaniel, P. (2010). Seeding clouds with trust anchors. *In Proceedings of the 2010 ACM workshop*, on Cloud computing security workshop (CCSW '10). ACM, New York, NY, USA, 43-46. DOI:10.1145/1866835.1866843.

Schnjakin, M., Alnemr, R. and Meinel, C. (2010). Contract-based cloud architecture. *Proceedings of the 2010 second international workshop on Cloud data management (CloudDB '10)*. ACM, 33-40. DOI:10.1145/1871929.1871936.

Seddon, J. and Currie, W. (2013). Cloud Computing And Trans-Border Health Data: Unpacking U.S. And EU Healthcare Regulation And Compliance. *Health Policy and Technology (2013).* Elsevier. 2(4):229-241. DOI: doi:10.1016/j.hlpt.2013.09.003.

Servos, D. (2012). A Role and Attribute Based Encryption Approach to Privacy and Security in Cloud Based Health Services. *Master of Science in Computer Science*. Lakehead University, 1-223.

Shawish, A. and Salama M. (2014). Cloud Computing: Paradigms and Technologies *Inter-cooperative Collective Intelligence: Techniques and Applications Studies in Computational Intelligence* 495: 39-67. DOI: 10.1007/978-3-642-35016-0_2

Shen, Z., Li, L., Yan, F. and Wu, X. (2010). Cloud Computing System Based on Trusted Computing Platform. *Proceedings of the 2010 Intelligent Computation Technology and Automation (ICICTA), 2010 International Conference on*. 11-12 May 2010. Changsha. IEEE, 1: 942-945. DOI: 10.1109/ICICTA.2010.724.

Shini, S., Thomas, T. and Chithraranjan, K. (2012). Cloud Based Medical Image Exchange-Security Challenges. Procedia Engineering 38, Elsevier Ltd, 3454 – 1877-7058. DOI: 10.1016/j.proeng.2012.06.399.

Singh, A. and Shrivastava, M. (2012). Overview of Attacks on Cloud Computing. *International Journal of Engineering and Innovative Technology (IJEIT)*. 1(4):321-323. April 2012, ISSN: 2277-3754.

Smith, D. (2013). Cloud computing and HIPAA: Achieving compliance. Retrieved on July 30, 2014, from http://techpageone.dell.com/technology/cloud-computing-hipaa-achieving-compliance/#.U9lZIuPoRHW

Somorovsky, J., Heiderich, M., Jensen, M., Schwenk, J., Gruschka, N. and Iacono, L. (2011). All Your Clouds are Belong to us – Security Analysis of Cloud Management Interfaces. *In Proceedings of the 3rd ACM workshop on Cloud computing security workshop (CCSW 2011)*.ACM, 3-13. DOI:10.1145/2046660.2046664.

Subashini, S. and Kavitha, V. (2011). A Survey On Security Issues In Service Delivery Models Of Cloud Computing. *Journal of Network and Computer Applications*, ACM. 34(1):1-11. DOI:10.1016/j.jnca.2010.07.006.

Sulayman, M. (2007). *A Systematic Literature Review of Software Process Improvement for Small and Medium Web Companies*. PhD Thesis. Department of Computer Science. The University of Auckland

Sun, X., Chang, G. and Li, F. (2011). A Trust Management Model to Enhance Security of Cloud Computing Environments. *Proceedings of the 2011 Networking and Distributed Computing (ICNDC), 2011 Second International Conference on*. 21-24 September. 2011. Beijing. IEEE, 244–248. DOI: 10.1109/ICNDC.2011.56.

Sundareswaran S. and Squicciarini, A. (2012). Ensuring Distributed Accountability for Data Sharing in the Cloud. *IEEE Transactions on Dependable and Secure Computing*, IEEE Computer Society. 9(4):1-13. DOI: 10.1109/TDSC.2012.26.

Survey Software Reviews (2012). Top 10 promising online survey tools. Retrieved on July 30, 2014, from http://www.survey-reviews.net/index.php/2012/02/top-10-promising-online-survey-tools/

Taeho, J., Li, X., Wan, Z. and Wan, M. (2013). Privacy Preserving Cloud Data Access with Multi-Authorities. *Proceedings of 2013 IEEE INFOCOM*. 14-19 April 2013. Turin, 2625-2633.

Takabi, H., Joshi, D. and Ahn G. (2010a). SecureCloud: To-wards a Comprehensive Security Framework for Cloud Computing Environments. *Proceedings of the 2010 34th Annual IEEE Computer Software and Applications Conference Workshops (COMPSACW)*. 19-23 July 2010. Seoul. IEEE, 393-398. DOI: 10.1109/COMPSACW.2010.74.

Takabi, H., Joshi, D. and Ahn, G. (2010). Security and Privacy Challenges in Cloud Computing Environments. *Security and Privacy*, IEEE Computer Society. 8(6):24–31. DOI: 10.1109/MSP.2010.186.

Takahashi, T., Blancy, G., Kadobayashiy, Y., Fally, D., Hazeyamay, H. and Matsuo, S. (2012). Enabling Secure Multi-Tenancy In Cloud Computing: Challenges And Approaches. *Future Internet Communications (BCFIC)*, 2012 2nd Baltic Congress on, 72–79.

TCG (2007). TCG Specification Architecture Overview. *Trusted Computing Group (TCG) Specification Revision1.4*, August 2007.

TCG (2011). Mobile Trusted Module 2.0 Use Cases. *Trusted Computing Group (TCG)*. Specification Version 1.0. Retrieved on January 12, 2014, from http://www.trustedcomputinggroup.org/resources/tpm_mobile_with_trusted_execution_environment_for_comprehensive_mobile_device_security.

TCG (2011a). Network Security Automation Standards: TNC and SCAP. *Trusted Computing Group (TCG)* Retrieved on November 17, 2013, from http://scap.nist.gov/events/2011/saddsp/presentations/TCG-TNC_and_SCAP.pdf

TCG (2011b). Trusted Computing Group's Trusted Network Connect Technology Standards Development for Network Security Interoperability. *Trusted Computing Group (TCG)* Retrieved on December 5, 2013, from http://www.nist.gov/standardsgov/upload/TCG.pdf

TCG (2011c). Trusted Network Connect (TNC) Open Standards for Integrity-based Network Access Control and Coordinated Network Security. *Trusted Computing Group (TCG)* Retrieved on December 5, 2013, from http://www.trustedcomputinggroup.org/files/resource_files/758321DC-1A4B-B294-D07BB912754041F8/TNC_OpenStandards_April2011.pdf

TCG (2012). Trusted Network Connect. Trusted Computing Group (TCG) Retrieved on November 17, 2013, from http://www.trustedcomputinggroup.org/files/resource_files/2884F884-1A4B-B294-D001FAE2E17EA3EB/TNC_Architecture_v1_5_r3-1.pdf

TCG (2013). Trusted Network Connect Standards for Network Security Retrieved on November 17, 2013, from http://www.trustedcomputinggroup.org/files/resource_files/DEDFD151-1A4B-B294-D0D0358910297C19/TNC%20Briefing%202013-12-10.pdf

TCG (2013a). About TCG. *Trusted Computing Group (TCG)* Retrieved on November 15, 2013, from http://www.trustedcomputinggroup.org/about_tcg

TCG (2013b). Architect's Guide: Cyber Security. *Trusted Computing Group (TCG)* Retrieved on December 6, 2013, from http://www.trustedcomputinggroup.org/resources/architects_guide_ics_security_using_tnc_technology

TCG (2013c). Architect's Guide: Data Security Using TCG Self-Encrypting Drive Technology. *Trusted Computing Group (TCG)* Retrieved on November 16, 2013, from http://www.trustedcomputinggroup.org/.

TCG (2013d). Architect's Guide: ICS Security Using TNC Technology. Trusted Computing Group (TCG) Retrieved on December 6, 2013, from http://www.trustedcomputinggroup.org/resources/architects_guide_ics_security_using_tnc_technology

Teo, J. (2009). Features and benefits of trusted computing. *Proceedings of the 2009 Information Security Curriculum Development Conference (InfoSecCD '09)*. ACM, 67-71. DOI: 10.1145/1940976.1940990.

Thilakanathan, D., Chen, S., Nepal, S., Calvo, R., Alem, L. (2013). A platform for secure monitoring and sharing of generic health data in the Cloud. *Future Generation Computer Systems (2013),* 35: 102-113. DOI: 10.1016/j.future.2013.09.011.

Tian, L., Lin, C. and Ni, Y. (2010). Evaluation of user behaviour trust in cloud computing. *Proceedings of the 2010 Computer Application and System Modelling (ICCASM)*, 2010 International Conference on. 22-24 October. 2010. Taiyuan. IEEE, 7: 567-572. DOI: 10.1109/ICCASM.2010.5620636.

Tianfield, H. (2012). Security Issues In Cloud Computing. *Proceedings of the 2012 Systems, Man, and Cybernetics (SMC), 2012 IEEE International Conference on*, October. 14-17, 2012, COEX, Seoul, Korea. IEEE, 108-1089. DOI:10.1109/ICSMC.2012.6377874.

Tracy, M., Jansen, W., Scarfone, K, and Winograd, T. (2007). Guidelines on Securing Public Web Servers. Special Publication 800-44 .Version 2 *National Institute of Standards and Technology (NIST).* Retrieved on December 7, 2013, from http://csrc.nist.gov/publications/nistpubs/800-44-ver2/SP800-44v2.pdf

Trend Micro (2010). Cloud Computing Security, Server Security: Making Virtual Machines Cloud-Ready. Retrieved on December 7, 2013, from http://www.securecloud.com/cloud-content/us/pdfs/business/white-papers/wp_cloudsecurity-unlock-opportunities.pdf

Trend Micro (2012). Security Threats To Evolving Data Centres. Virtualization and Cloud Computing. Retrieved on November 23, 2013, from http://la.trendmicro.com/media/report/virtualization-and-cloud-security-report-en.pdf

Trend Micro (2013). Deep Security 9. Comprehensive security platform for physical, virtual, and cloud servers. Retrieved on November 23, 2013, from http://www.trendmicro.com/cloud-content/us/pdfs/business/datasheets/ds_deep-security.pdf

Tripathi, A. and Mishra, A. (2011). Cloud computing security considerations. *Proceedings of the 2011 Signal Processing, Communications and Computing (ICSPCC), 2011 IEEE International Conference on*. 14-16 September. 2011. Xi'an. IEEE, 1–5. DOI: 10.1109/ICSPCC.2011.6061557.

Tupakula, U. and Varadharajan, V. (2011). TVDSEC: Trusted Virtual Domain Security. *Proceedings of the 2011 Fourth IEEE International Conference on Utility and Cloud Computing*. *2011 International conference on*. 5-8 Dec. 2011. Victoria, NSW. IEEE, 57- 64. DOI: 10.1109/UCC.2011.18.

Ubhale, P. and Sahu, A. (2013). Securing Cloud Computing Environment by means of Intrusion Detection and Prevention System (IDPS). *International Journal of Computer Science and Management Research (IJCSMR)*. 2(5):2430-2436. May 2013.

Uppal, H. (2010). *Enabling Trusted Distributed Control with Remote Attestation*. Bachelor Thesis. Computer Science and Engineering University of Washington.

Vernier, D. and Jones, A. (2011). SmartCloud tip: Span virtual local area networks Provision and configure an instance that spans a public and private VLAN. *IBM DeveloperWorks* Retrieved on December 5, 2013, from http: http://www.ibm.com/developerworks/cloud/library/cl-multiplevlans/.

Wang, X. and Tan, Y. (2010). Application of Cloud Computing in the Health Information System. *In Computer Application and System Modelling (ICCASM), 2010 International Conference on*. 22-24 October. Taiyuan. 2010. IEEE, 1:179-182. DOI: 10.1109/ICCASM.2010.5619051.

Wieder, P., Butler, J., Theilmann, W. and Yahyapour, R. (2011). Service Level Agreements for Cloud Computing. Springer New York Dordrecht Heidelberg London, 2011. ISBN: 978-1-4614-1613-5 (Print) 978-1-4614-1614-2.

Williams, C. (2007). Research Methods. *Journal of Business and Economic Research*. 5(3):65-71.

Wilson, G, Day, M. and Taylor, B. (2011). KVM: Hypervisor Security You Can Depend On. *IBM Linux Technology Centre*. Retrieved on January 3, 2014, from ftp://public.dhe.ibm.com/linux/pdfs/LXW03004-USEN-00.pdf

Wu, R., Ahn, G. and Hu, H. (2012). Secure Sharing of Electronic Health Records in Clouds. *Proceedings of the 2012 Collaborative Computing: Networking, Applications and Work sharing (CollaborateCom)*, 2012 8th International Conference on, 14-17 October. 2012, Pittsburgh. IEEE, 711-718.

Wu, R., Ahn, G. and Hu, H. (2012a). Towards HIPAA-compliant Healthcare Systems. *Proceedings of the 2012 2nd ACM SIGHIT International Health Informatics Symposium (IHI '12)*. ACM, 593-602. DOI:10.1145/2110363.2110429.

Xiao, Z. and Xiao, Y. (2013). Security and Privacy in Cloud Computing. *Proceedings of the 2013 IEEE Communications Surveys and Tutorials*, 2 May 2013, IEEE Communications Society. 15 (2): 843 – 859. DOI: 10.1109/SURV.2012.060912.00182.

Yadav, P. (2013). Review of Trusted Framework for Cloud Computing. *International Journal of Computational Science, Engineering and Technology (IJCSET).* I (II): 36-38. March 2013.

Yang, J. and Chen, Z (2010). Cloud Computing Research and Security Issues. *Proceedings of the 2010 Computational Intelligence and Software Engineering (CiSE), 2010 International Conference on*. 10-12 Dec. 2010. Wuhan. IEEE, 1-3. DOI: 10.1109/CISE.2010.5677076.

Yau, S. and An, H. (2011). Software Engineering Meets Services and Cloud Computing. *Proceedings of the 2011 Computer*. 44(10):47-53 IEEE Computer Society, DOI:10.1109/MC.2011.267.

Yeluri, R., Castro-Leon, E., Harmon, R. and Greene, J. (2012). Building Trust and Compliance in the Cloud for Services. *Proceedings of the 2012 SRII Global Conference (SRII), 2012 Annual*. 24-27 July 2012. San Jose, CA. IEEE, 379 – 390. DOI: 10.1109/SRII.2012.49.

Youssef, A. (2012). Exploring Cloud Computing Services and Applications. *Journal of Emerging Trends in Computing and Information Sciences.* 3(6, no.3):838-847.

Youssef, A. and Alageel, M. (2012). A Framework for Secure Cloud Computing. *International Journal of Computer Science Issues (IJCSI)*, 9: (4), No 3, July 2012. ISSN (Online): 1694-0814. www.IJCSI.org

Yu, X. and Wen, Q. (2010). A View about Cloud Data Security from Data Life Cycle. *Proceedings of the 2010 Computational Intelligence and Software Engineering (CiSE), 2010 International Conference on*. 10-12 December. 2010. Wuhan. IEEE, 1 – 4. DOI: 10.1109/CISE.2010.5676895.

Zhang, R. and Liu, L. (2010). Security Models and Requirements for Healthcare Application Clouds. *Proceedings of the 2010 Cloud Computing (CLOUD), IEEE 3rd International Conference* on. 5-10 July 2010. Miami, FL. IEEE, 268-275. DOI: 10.1109/CLOUD.2010.62.

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 System*. Elsevier, 583–592. DOI: 10.1016/j.future.2010.12.006.

APPENDIX A

PUBLICATIONS DURING AUTHOR'S CANDIDATURE

Impact Factor Journal

Mervat Adib Bamiah, Sarfraz Nawaz Brohi, Suriayati Chuprat, Jamalul-lail Ab Manan, Trusted cloud computing framework for healthcare sector, 2013, *Journal of Computer Science*. 10(2):240-250. DOI:10.3844/jcssp.2014.240.250.

Sarfraz Nawaz Brohi, Mervat Adib Bamiah, Suriayati Chuprat, Jamalul-lail Ab Manan, Design And Implementation of a Privacy Preserved Off-Premises Cloud Storage, 2013, *Journal of Computer Science*. 10(2):210-223. DOI: 10.3844/jcssp.2014.210.223.

IEEE Xplore

Mervat Bamiah, Sarfraz Brohi, Suriayati Chuprat, and Jamalul-lail Ab Manan. 2012. A Study on Significance of Adopting Cloud Computing Paradigm in Healthcare Sector. *Cloud Computing Technologies, Applications and Management (ICCCTAM), 2012 International Conference on*, 65–68. DOI:10.1109/ICCCTAM.2012.6488073.

Mervat Bamiah, Sarfraz Brohi, Suriayati Chuprat, and Muhammad Nawaz Brohi. 2012. Cloud Implementation Security Challenges. *Cloud Computing Technologies, Applications and Management (ICCCTAM), 2012 International Conference on*, 174–178. DOI:10.1109/ICCCTAM.2012.6488093.

Sarfraz Nawaz Brohi, Mervat Adib Bamiah, Muhammad Nawaz Brohi, and Rukshanda Kamran. 2012. Identifying and Analyzing Security Threats to Virtualized Cloud Computing Infrastructures. *Cloud Computing Technologies, Applications and Management (ICCCTAM), 2012 International Conference on*, 151–155. DOI:10.1109/ICCCTAM.2012.6488089.

Sarfraz Nawaz Brohi, Mervat Adib Bamiah, Suriayati Chuprat, and Jamalul-lail Ab Manan. 2012. Towards an Efficient and Secure Educational Platform on Cloud Infrastructure. *Cloud Computing Technologies, Applications and Management (ICCCTAM), 2012 International Conference on*, 145–150. DOI:10.1109/ICCCTAM.2012.6488088.

Indexed by SPIE

Mervat Adib Bamiah, Sarfraz Nawaz Brohi and Suriayati Chuprat. Using Virtual Machine Monitors to Overcome The Challenges of Monitoring and Managing Virtualized Cloud Infrastructures, Proc. SPIE 8349, *Fourth International Conference on Machine Vision (ICMV 2011)*. Machine Vision, Image Processing, and Pattern Analysis, 83491M (January 11, 2012); DOI:10.1117/12.920880.

Journals

Mervat Adib Bamiah, Sarfraz Nawaz Brohi. Exploring the Cloud Deployment and Service Delivery Models. *International Journal of Research and Reviews in Information Sciences (IJRRIS)*, Vol. 1, no. 03. September 2011, Science Academy Publisher, 77-80. ISSN: 2046-6439.

Mervat Adib Bamiah, Sarfraz Nawaz Brohi. Seven Deadly Threats and Vulnerabilities in Cloud Computing. *International Journal of Advanced Engineering Sciences and Technologies (IJAEST'11)*, Vol. 9. no.1, 2011. 87-90. ISSN: 2230-7818.

Sarfraz Nawaz Brohi, Mervat Adib Bamiah. Challenges and Benefits for Adopting the Paradigm of Cloud Computing. *International Journal of Advanced Engineering Sciences and Technologies (IJAEST'11)*, Vol. 8, no.2. 2011. 286 – 290. ISSN: 2230-7818.

Sarfraz Nawaz Brohi, Mervat Adib Bamiah. Exploit of Open Source Hypervisors for Managing the Virtual Machines. *Cloud International Journal of Advanced Engineering Sciences and Technologies (IJAEST)*, Vol. 9, no.1. 55 – 60. ISSN: 2230-7818.

Postgraduate Annual Research on Informatics Seminar

Mervat Bamiah, Sarfraz Brohi, Suriayati Chuprat, 2012. Emerging Security Concerns for Implementing Cloud Computing in Healthcare Sector. *Postgraduate Annual Research on Informatics Seminar (PARIS 2012-2).*

Mervat Bamiah, Sarfraz Brohi, Suriayati, Chuprat, S., 2011. Cloud Computing: A Key Enabler for Smart Healthcare. *In Postgraduate Annual Research on Informatics Seminar (PARIS).*

Sarfraz Brohi, Mervat Bamiah, Suriayati Chuprat, 2011. Designing a Trustable Security Protocol for Implementing a Smart Educational Platform on Cloud Infrastructure. *In Postgraduate Annual Research on Informatics Seminar (PARIS).*

Sarfraz Nawaz Brohi, Mervat Adib Bamiah, Suriayati Chuprat, Jamalul-lail Ab Manan, 2012. Towards a Secure Cloud Computing Infrastructure. *In Postgraduate Annual Research on Informatics Seminar (PARIS 2012-2*).